პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

N1, 2023

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

№1, 2023

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის პირველი გამოცემა ეძღვნება მონაცემთა დაცვის საერთაშორისო დღეს.

P-ISSN 2720-8753
E-ISSN 2720-8761

სარჩევი

მთავარი რედაქტორისაგან

"Scientia dux vitae certissimus" („მეცნიერება ცხოვრების ყველაზე საიმედო გზამკვლევია") – სენტენციის ჭეშმარიტება ეხმიანება საზოგადოებაში მეცნიერების ყოფიერებისა და ცოდნის გადაცემის ხელშეწყობის მიზანს, რომელიც დემოკრატიული და სამართლებრივი სახელმწიფოს უმნიშვნელოვანეს პრიორიტეტს წარმოადგენს. ამ ამოცანის განხორციელებაში თითოეულ საზოგადოებრივ აქტორს, საგანმანათლებლო დაწესებულებებთან ერთად, ინდივიდუალური როლი მიუძღვის, განსაკუთრებით კი სამართლის პრაქტიკული არსობის თეორიული შემეცნებისა და პირიქით – სამართლის თეორიის პრაქტიკაში განხორციელების თვალსაზრისით. მონაცემთა დაცვის საზედამხედველო ორგანოები ერთობლივი ძალისხმევით ცდილობენ პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის შესახებ საზოგადოების ცნობიერების ამაღლებას და პრაქტიკული გამოწვევების სამართლებრივ გააზრებას. პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები ადამიანის პიროვნული იდენტობის განუყოფელი ნაწილია. მისი ინსტიტუციური დაცვა მონაცემთა დაცვის საზედამხედველო ორგანოთა უპირველესი ამოცანაა. დღესდღეობით ციფრული ტექნოლოგიური პროგრესი, ერთი მხრივ, განვითარების შეუქცევადი და გარდაუვალი პროცესია, ხოლო მეორე მხრივ – დიდი გამოწვევა, განსაკუთრებით კი ინდივიდთა პერსონალური მონაცემების დაცვის თვალსაზრისით. მსგავსად მონაცემთა დაცვის კოლეგა საზედამხედველო ორგანოებისა, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურიც მიისწრაფვის საზოგადოებაში პირადი ცხოვრების პატივისცემის კულტურის დამკვიდრების და საერთო ევროპული ფასეულობების განმტკიცებისკენ. ევროპულ სამართალთან ჰარმონიზაციის თანმხლები და გარდაუვალი პროცესია სამეცნიერო კვლევების განხორციელება, საზღვარგარეთის მონაცემთა დაცვის კოლეგა საზედამხედველო ორგანოებს შორის საუკეთესო პრაქტიკის გაზიარება. ამ მიზნის განსახორციელებლად, საერთაშორისო თანამშრომლობის არაერთი ფორმატი არსებობს. „პერსონალურ მონაცემთა დაცვის სამეცნიერო ჟურნალის" დაარსება ინტერნაციონალური, სამეცნიერო ქსელის ჩამოყალიბებისა და გაძლიერების მიზანს ემსახურება. ჟურნალის კონცეფციაა ინსტიტუციური და ინდივიდუალური თანამშრომლობის სამეცნიერო კონტრიბუცია პერსონალურ მონაცემთა დაცვის სფეროში არსებული პრობლემატიკის განხილვისა და გადაჭრის გზაზე.

„პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი" წარმოადგენს საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის ორენოვან, სრული ღია წვდომის, საერთაშორისო სარედაქციო კოლეგიის მქონე, პერიოდულ სამეცნიერო გამოცემას. ჟურნალის დაარსება ევროკავშირის „მონაცემთა დაცვის ზოგადი რეგულაციის" (GDPR) მიღების მეოთხე საიუბილეო თარიღს უკავშირდება, რომელიც 2018 წლის 25 მაისიდან

ამოქმედდა. იგი პერსონალურ მონაცემთა დაცვის უმაღლეს სტანდარტს წარმოადგენს და ევროინტეგრაციის გზაზე, ეროვნული კანონმდებლობის მასთან ჰარმონიზება საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის უალტერნატივო პრიორიტეტია. ჟურნალის პირველი გამოცემაც სწორედ მონაცემთა დაცვის საერთაშორისო დღეს ეძღვნება, რომელიც ევროპის საბჭოს 2006 წლის 26 აპრილის გადაწყვეტილებით, ყოველწლიურად, 28 იანვარს აღინიშნება და „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს 1981 წლის კონვენციის ხელმოწერისთვის გახსნის თარიღს უკავშირდება. წინამდებარე გამოცემით გვსურს, შევუერთდეთ საერთაშორისო საზოგადოებას, მონაცემთა დაცვის კოლეგა საზედამხედველო ორგანოების მიერ ამ უაღრესად მნიშვნელოვანი თარიღის აღნიშვნაში.

ჟურნალში ქვეყნდება ადამიანის ძირითად უფლებათა და თავისუფლებათა, განსაკუთრებით კი პერსონალურ მონაცემთა დაცვის სამართლის დარგში შესრულებული სამეცნიერო ნაშრომები. მისი ძირითადი ორიენტირია საჯარო სამართლის დარგობრივი მიმართულებით შედარებითსამართლებრივი დისკურსის წარმართვა, აქტუალურ საკითხთა სამართლებრივი ანალიზი, საუკეთესო პრაქტიკის წარმოჩენა და საზოგადოების ფართო წრისათვის გაცნობა. აკადემიური ღირებულებებისა და კულტურის მხარდაჭერა, დარგობრივი მიმართულებით არსებული სამეცნიერო წყაროთა ფონდის გამდიდრება ჟურნალის ერთ-ერთი მიზანია. იგი ხელს შეუწყობს კვლევების ინტერნაციონალიზაციას და მონაცემთა დაცვის საზედამხედველო ორგანოებს, რათა განახორციელონ გამოქვეყნებული კვლევის შედეგების მათ ყოველდღიურ საქმიანობაში ინტეგრაცია.

პერიოდული გამოცემის ცალკეული რუბრიკებისა და კვლევითი თემატიკის განსაზღვრის პროცესში, აღსანიშნავია დარგის მოწინავე მკვლევარ-მეცნიერთა, აკადემიური წრის წარმომადგენელთა და პრაქტიკოს იურისტთა ჟურნალთან თანამშრომლობა. „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ დაფუძნება ასევე აღსანიშნავია იმ თვალსაზრისითაც, რომ საქართველოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს არსებობის ისტორიაში პირველად დაფუძნდა მსგავსი ტიპის ორენოვანი, სამეცნიერო, პერიოდული გამოცემა. ეს ერთგვარად ეხმიანება საზღვარგარეთის მონაცემთა დაცვის კოლეგა საზედამხედველო ორგანების მიერ სამეცნიერო პუბლიკაციების გამოცემის თანამედროვე ტენდენციასა და საკმაოდ გავრცელებულ პრაქტიკას.[1]

[1] ამ თვალსაზრისით აღსანიშნავია ევროპის მონაცემთა დაცვის ზედამხედველი (*European Data Protection Supervisor*), რომლის ოფიციალურ ვებგვერდზე პერიოდულობით ქვეყნდება სტატიები, მოხსენებები, სხვადასხვა ტიპის მასალები; აგრეთვე, თურქეთის მონაცემთა დაცვის საზედამხედველო ორგანოს პერიოდული გამოცემა: “Turkish Journal of Privacy and Data Protection”, რომელიც ასევე ხელმისაწვდომია ოფიციალური ვებგვერდის მეშვეობით.

„პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი“ გამიზნულია როგორც თეორეტიკოსი და პრაქტიკოსი იურისტებისთვის, ისევე პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობით დაინტერესებულ მკითხველთა ფართო წრისათვის. ინტერნაციონალიზაციის კომპონენტის გაძლიერების მიზნით, თითოეული გამოცემა გააერთიანებს ქართველ და უცხოელ ავტორთა ნაშრომებს. უაღრესად მნიშვნელოვანია, რომ ჟურნალს ჰყავს საერთაშორისო სარედაქციო კოლეგია და მის შემადგენლობაში არიან ევროპის მოწინავე უნივერსიტეტების პროფესორები, საჯარო სამართლის მეცნიერ-მკვლევრები, რომელთა წვლილი სამართლის აღნიშნული დარგის განვითარებაში უაღრესად დიდია.

მადლობას ვუხდი „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ რედაქციას, სარედაქციო კოლეგიის თითოეულ წევრს პირველი ნომრის მოსამზადებლად გაწეული შრომისთვის, საერთაშორისო საგამომცემლო სტანდარტებთან ჟურნალის საგამომცემლო პოლიტიკის ჰარმონიზებისა და მის სამომავლო განვითარებაზე ზრუნვისთვის.

მადლიერებას გამოვთქვამ თითოეული ავტორის მიმართ, ჟურნალის პირველ გამოცემაში მათ მიერ განხორციელებული სამეცნიერო წვლილისთვის და უაღრესად აქტუალურ საკითხებზე წარმოდგენილი კვლევებისთვის. მსურს განსაკუთრებული მადლიერებით აღვნიშნო ბერლინის შტაინბეის უნივერსიტეტის რექტორის, ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ***პროფესორის, დოქტ. გიორგი ხუბუას*** მუდმივი მხარდაჭერა. მადლიერებას გამოვთქვამ ევროპის მონაცემთა დაცვის ზედამხედველის (European Data Protection Supervisor) – ***პროფესორ, დოქტ. ვოიჩეკ ვიევიოროვსკის*** მიმართ თანამშრომლობისათვის და ჟურნალის პირველი ნომრის გამოცემისადმი მიძღვნილი მისასალმებელი წერილისთვის. მადლობას ვუხდი საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის პარტნიორ უწყებებს – იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (Garante per la protezione dei dati personali) ***პრეზიდენტს*** – ***პროფესორ, დოქტ. პასკუალე სტანციონესა*** და ხორვატიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (Agencija za zaštitu osobnih podataka) ***პრეზიდენტს*** – ***ზდრავკო ვუკიჩს*** სამსახურთან გაფორმებული ურთიერთთანამშრომლობის მემორანდუმისთვის, აქტიური თანამშრომლობაზე მზაობისთვის და ჟურნალის პირველი გამოცემისადმი მიძღვნილი წერილებისთვის. დიდი მადლობა ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ***პროფესორს, დოქტ. პაატა ტურავას***, გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილ მოსამართლეს, მარბურგის ფილიპეს სახელობის უნივერსიტეტის ***პროფესორს, დოქტ. ნორბერტ ბერნსდორფს***, უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანოს ***პრეზიდენტს*** – ***პროფესორ, დოქტ. ატილა პეტერფალვს*** და ამავე უწყების კოლეგას, ხელოვნური ინტელექტის ექსპერტს – ***დოქტ.***

დანიელ ესტერს უაღრესად მნიშვნელოვანი სამეცნიერო კონტრიბუციისათვის და გამოქვეყნებული სამეცნიერო შრომებისთვის. აგრეთვე მადლობას ვუხდი საქართველოში საერთაშორისო სამართლებრივი თანამშრომლობის გერმანული ფონდის (IRZ) პროექტის კოორდინატორს – ***ასოცირებულ პროფესორ, დოქტ. სულხან გამყრელიძეს*** ჟურნალის პირველი გამოცემისადმი მიძღვნილი მისასალმებელი წერილისათვის.

დაბოლოს, მოლოდინი მაქვს, რომ ჟურნალს მკითხველთა ფართო წრე ეყოლება და სამართალმცოდნეთა გარდა, მომიჯნავე დარგის სპეციალობების წარმომადგენლებიც დაინტერესდებიან მისი სამომავლო გამოცემებით.

ასოც. პროფესორი, დოქტ., დოქტ. ლელა ჯანაშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი

ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

ბარსელონის ავტონომიური უნივერსიტეტის მოწვეული პროფესორი

პროფ., დოქტ. გიორგი ხუბუას მისასალმებელი წერილი

ძვირფასო მკითხველო,

ჩემთვის დიდი პატივია, მოგილოცოთ პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის დაფუძნება!

ჩვენ ვცხოვრობთ ახალი, ციფრული რევოლუციის ეპოქაში. ფინანსური ტრანზაქციების 70 პროცენტი უკვე ალგორითმების მეშვეობით ხორციელდება. მომდევნო 10-20 წლის პერიოდში ალგორითმი დღეს არსებული სამუშაო ადგილების ნახევარზე მეტს ჩაანაცვლებს, ხოლო ციფრული განვითარების გავლენით, მომდევნო ათწლეულის განმავლობაში, მსოფლიოს 500 ტოპ-ფირმის 40 პროცენტი უბრალოდ გაქრება.

კაცობრიობისათვის უცხო არ არის რევოლუციური მნიშვნელობის ცვლილებები. მაგრამ, ციფრული რევოლუცია გამოირჩევა მნიშვნელოვანი თავისებურებით. ადრე ადამიანებს საკმარისი დრო ჰქონდათ იმისათვის, რომ ფეხი აეწყოთ ინდუსტრიული რევოლუციით გამოწვეული ცვლილებებისათვის. თანამედროვე ეპოქაში კი იმდენად დაჩქარდა ყველაფერი, რომ ადამიანს ძალიან ლიმიტირებული დრო აქვს ადაპტაციისათვის. ჟურნალს შეუძლია მნიშვნელოვანი დახმარება გაგვიწიოს, რომ უფრო მომზადებული შევხვდეთ ციფრული რევოლუციის გამოწვევებს.

ციფრული ტრანსფორმაცია და პერსონალური მონაცემების დაცვა ხშირად განიხილება როგორც ორი, ერთმანეთისადმი ანტაგონისტურად დაპირისპირებული კატეგორია. ხშირად საუბრობენ „მონაცემების დიქტატზეც“, როდესაც ინფორმაციის უზარმაზარმა ნაკადმა შეიძლება წაგლეკოს კიდეც. პერსონალურ მონაცემთა დაცვა ესწრაფვის ამ მონაცემების მინიმალიზაციას და მის მიმართ ძალიან მომჭირნე და ეკონომიურ მიდგომას.

პერსონალურ მონაცემთა დაცვის უფლება, ისევე როგორც ნებისმიერი უფლება, მნიშვნელოვნად არის დამოკიდებული მისი სუბიექტური განცდის ინტენსიურობაზე. ჟურნალის ერთ-ერთი მთავარი გამოწვევა იქნება პერსონალურ მონაცემთა დაცვის სფეროში სამოქალაქო ცნობიერების დონის ამაღლება და გაძლიერება.

ციფრული განვითარების პროცესში ადამიანებს ხშირად უყალიბდებათ პასიური, მომხმარებლური დამოკიდებულება და მათ უმრავლესობას ნაკლებად წარმოუდგენია, თუ რა როლი გვეკისრება ჩვენ ციფრული სამყაროს კონსტრუირებაში. დემოკრატიულ საზოგადოებასა და სამართლებრივ სახელმწიფოს სჭირდება არა პასიური მომხმარებელი, არამედ – აქტიური მოქალაქე. ჟურნალმა ხელი უნდა შეუწყოს პასუხისმგებლობის მაღალგანვითარებული უნარის მქონე საზოგადოების ფორმირებას.

ციფრულ სამყაროში პიროვნული თვითგამორკვევა და ინდივიდუალური ავტონომია აუცილებელი წინაპირობაა იმისათვის, რომ განხორციელდეს მაქსიმალურად გამჭვირვალე კონტროლი პერსონალური მონაცემების მიღებასა და გამოყენებაზე.

ინფორმაციული თვითგამორკვევა მოითხოვს ფუნქციონირებადი ქსელების ჩამოყალიბებას სახელმწიფოს, ეკონომიკურ სტრუქტურებს, მეცნიერებასა და სამოქალაქო საზოგადოებას შორის. ჟურნალი უნდა გახდეს ერთგვარი ეროვნული პლატფორმა, რომელიც ხელს შეუწყობს თვითგამორკვევას ციფრული მართვის პირობებში, გაამყარებს ნდობას ციფრული სტრუქტურების მიმართ ეკონომიკასა და საზოგადოების სხვა სექტორებში. ჟურნალმა უნდა უზრუნველყოს სხვა, მათ შორის საერთაშორისო ქსელებში ინტეგრირებაც.

დარწმუნებული ვარ ჟურნალის წარმატებაში! დიდი მადლობა ყველას, ვინც თავისი წვლილი შეიტანა ამ მნიშვნელოვანი წამოწყების განხორციელებაში!

პროფ., დოქტ. გიორგი ხუბუა

ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო
უნივერსიტეტის პროფესორი

ბერლინის შტაინბეის უნივერსიტეტის რექტორი

პროფ., დოქტ. ვოიჩეკ ვიევიოროვსკის
მისასალმებელი წერილი

ძვირფასო მკითხველო,

დიდი პატივით ვწერ ამ წერილს, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის პირველი გამოცემის აღსანიშნავად.

აღნიშნული ჟურნალის დაფუძნების ინიციატივა მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) ამოქმედების მეოთხე წლისთავზე გაჩნდა. ეს ერთი მხრივ, წარმოაჩენს ევროპის კავშირის გავლენას, რომელიც თავისი კანონმდებლობის მეშვეობით ადგენს სტანდარტს, რომელსაც მსოფლიოს მრავალი ქვეყანა მისდევს. GDPR-ი უპირობოდ წარმოადგენს ოქროს სტანდარტს, მაგრამ ამავდროულად იგი ცოცხალი ორგანიზმია — სამართლებრივი აქტი, რომელიც ახალია და ჯერაც დგას მისი სწორად განმარტების, აღსრულების, გასაჩივრების და სასამართლო კონტროლის წინაშე. აქედან გამომდინარე, ძალზე მნიშვნელოვანია, რომ GDPR-ს ყურადღება ეთმობა აკადემიური წრისა და ყველა იმ პირის მხრიდან, ვინც, მაგალითად, საკუთარი პრაქტიკული გამოცდილების მეშვეობით ისურვებს ჩაერთოს დებატებში ინდივიდებისა და მათი ფუნდამენტური უფლებების — პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის შესახებ.

ის ფაქტი, რომ ჟურნალი შეიქმნა GDPR-ის ძალაში შესვლიდან მე-4 საიუბილეო წელს, წარმოაჩენს იმ კონკრეტულ და განსაკუთრებულ როლს, რომელსაც საქართველო ამ დებატებში ასრულებს. მიუხედავად იმისა, რომ ევროპის საბჭოს კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (ე. წ. 108-ე კონვენცია) არის საქართველოსა და ევროკავშირის წევრი სახელმწიფოებისათვის მოქმედი საერთო სამართლებრივი ჩარჩო, საქართველო, როგორც ევროკავშირის არაწევრი ქვეყანა, საკუთარი სამართლებრივი კულტურის სისტემაში ეყრდნობა GDPR-ს და რეგიონის დონეზე უწევს ადვოკატირებას, რაც წარმოადგენს მისი მეზობელი ქვეყნებისათვის გასაზიარებელ მაგალითს. ასეთი გავლენის მნიშვნელობა, როგორც იურიდიულად, ასევე გეოპოლიტიკურად შეუძლებელია, რომ არ დაფასდეს.

მაშასადამე, მადლობას ვუხდი საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურს დისკუსიის ამგვარი პლატფორმის შექმნისათვის, მჯერა, რომ იგი შეძლებს საქართველოში დისკუსიის გამდიდრებას, ასევე, ხელს შეუწყობს საქართველოს ცნობადობის გაზრდას მსოფლიო დონეზე.

საუკეთესო სურვილებით,

პროფ., დოქტ. ვოიჩეკ ვიევიოროვსკი

ევროპის მონაცემთა დაცვის ზედამხედველი (EDPS)

ზდრავკო ვუკიჩის
მისასალმებელი წერილი

ჩვენ ვცხოვრობთ მონაცემებზე ორიენტირებულ სამყაროში, სადაც პერსონალური მონაცემები ვალუტის ახალი ფორმაა.

კაცობრიობის საერთო პროგრესი ეფუძნება ცოდნის შეძენას, შენახვასა და გადაცემას, ხოლო საინფორმაციო და საკომუნიკაციო ტექნოლოგიები ამ პროცესს უფრო სწრაფს, იაფს, ხელმისაწვდომს და ზუსტს ხდის. ციფრული ტრანსფორმაცია არის ქვაკუთხედი, რომელზეც დამოკიდებულია ჩვენი საზოგადოების გადარჩენა. აღნიშნულთან დაკავშირებით არ უნდა დაგვავიწყდეს, რომ თითოეული ინდივიდის მონაცემი მის ხელთ არსებული მნიშვნელოვანი აქტივია. პერსონალური მონაცემების ბოროტად გამოყენება დიდ საფრთხეს უქმნის ნდობას, უსაფრთხოებასა და პირადი ცხოვრების დაცულობას, რომლებიც თითოეული ადამიანის პიროვნების შეუცვლელი შემადგენელი ნაწილია.

ციფრულ ეპოქაში პერსონალურ მონაცემთა დაცვის უფლება უფრო მნიშვნელოვანია, ვიდრე ეს ოდესმე ყოფილა. ერთი შეხედვით, არაერთ ინტერნეტ მომსახურებასა და აპლიკაციას გვთავაზობენ უფასოდ. მაგალითად, ჩვენ შეგვიძლია, გამოვიყენოთ უფასო სოციალური ქსელები, ციფრული პლატფორმები მუსიკისა და ვიდეოების ჩამოსატვირთად, მყისიერი შეტყობინებების ელექტრონული ფოსტის სერვისები, ღრუბლოვანი სერვისები და ა. შ. აღნიშნული მომსახურების მომწოდებლებს მონაცემთა შენახვასა და გადაცემასთან დაკავშირებული მაღალი ხარჯები აქვთ, თუმცა, ამის მიუხედავად, თავიანთ მომსახურებას უფასოდ გვთავაზობენ.

დღესდღეობით, მონაცემთა მონეტიზაცია ნიშნავს მონაცემთა პირდაპირ გაყიდვას ან მონაცემთა ანალიტიკის გამოყენებას შემოსავლის გაზრდის მიზნით. გარდა ამისა, არსებობს საფრთხე, რომ ხელოვნური ინტელექტის სისტემების საშუალებით მონაცემთა დამუშავება შესაძლებელია, ემსახურებოდეს სოციალური ქულების მინიჭების სისტემის შექმნას, მასობრივი მიყურადების განხორციელებას, აზიანებდეს დემოკრატიულ წესრიგს ან მიზნად ისახავდეს საზოგადოების ყველაზე მოწყვლადი ჯგუფების მანიპულირებას. როგორც არასდროს, პირადი ცხოვრების ხელშეუხებლობის ეფექტიანად დაცვა მნიშვნელოვანია, როგორც ადამიანზე ორიენტირებული მიდგომის ნაწილი, ციფრულ ეპოქასა და ხელოვნურ ინტელექტთან დაკავშირებული შესაძლებლობებისა და გამოწვევების გათვალისწინებით.

ერთი შეხედვით, მონაცემების ღირებულება, რომელიც ავლენს, თუ რა მოსწონს ადამიანს სოციალურ ქსელში, თითქოს არ არის განსაკუთრებით მნიშვნელოვანი. თუმცა ფსიქოგრაფიული მოდელირების მეთოდის გამოყენებითა და სხვა მონაცემებთან შესაბამისობის დადგენით, აღნიშნული მონაცემები გამოიყენება მომხმარებლების პროფილირებისა და მაგალითად, პოლიტიკური პრეფერენციების

განსაზღვრის, სამიზნე ჯგუფებისთვის ყალბი ინფორმაციისა და დეზინფორმაციის გავრცელებისა და ინდივიდების აზრებსა და ქმედებებზე ზემოქმედების მიზნებით.

მოდით, უბრალოდ გავიხსენოთ „კემბრიჯ ანალიტიკას“ შემთხვევა, რომელმაც თვალები აგვიხილა და გვაჩვენა, თუ როგორ იყენებენ მსხვილი ტექნოლოგიური კომპანიები ჩვენს მონაცემებს ჩვენი თანხმობის გარეშე და აღნიშნულზე აფუძნებენ საკუთარ მოგებას, რომელიც მილიარდებს ითვლის. როგორც ყოველთვის, კაცობრიობის ისტორიაში, როდესაც არსებობს რესურსების მონეტიზაციის დიდი პოტენციალი, უკონტროლო ექსპერიმენტებისა და უფლებამოსილების ბოროტად გამოყენების პერიოდს მოჰყვება ბაზრის რეგულირებისა და კომპანიების სამართლებრივ ჩარჩოსთან ადაპტაციის ხანგრძლივი პერიოდი.

ევროპის კავშირის მონაცემთა ინდუსტრიის შემთხვევაში, აღნიშნულ სამართლებრივ ჩარჩოს ქმნის მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR), ერთ-ერთი ყველაზე ძლიერი სამართლებრივი მექანიზმი და ყოვლისმომცველი რეგულაცია, რომელიც აწესრიგებს პერსონალური მონაცემების შეგროვებას და გამოყენებას როგორც ხელისუფლების, ისე კერძო სექტორის მიერ. საჭიროა, არსებობდეს დემოკრატიული ქვეყნების საერთო მიდგომა და მოქმედება, რადგან დიდი მოცულობით შეგროვებული მონაცემები, რომლებიც გაანალიზებული და დაჯგუფებულია, შემდეგ კი პროფილების შესაქმნელად და სამიზნე ჯგუფებისთვის პერსონალიზებული შეტყობინებების მიწოდებისთვის გამოყენება, არ ცნობს სახელმწიფოთა საზღვრებს. მონაცემთა დაცვის ორგანოებმა, საარჩევნო ორგანოებმა, მედიის მარეგულირებლებმა და ინფორმაციული უსაფრთხოების ექსპერტებმა — ჩვენ ყველამ, უნდა ვითანამშრომლოთ, რათა მივაღწიოთ სათანადო ბალანსს, რომელიც პატივს სცემს ადამიანის ძირითად უფლებებს და ამავდროულად, უზრუნველყოფს ციფრული ბიზნესმოდელების ზრდას.

თუმცა მონაცემთა დაცვის კანონმდებლობა არ უნდა იყოს დაბრკოლება მონაცემებთან დაკავშირებით ცოდნის მოპოვებისა და მონაცემებზე ორიენტირებული ბიზნეს მოდელების შემუშავებისთვის. GDPR არის პირადი ცხოვრების ხელშეუხებლობის, უსაფრთხოებისა და მონაცემთა მართვის გაუმჯობესების შესაძლებლობა და წარმოადგენს კატალიზატორს ახალი ბიზნეს მოდელებისთვის. როდესაც ვსაუბრობთ GDPR-ზე, მნიშვნელოვანია ხაზგასმით აღვნიშნოთ, რომ ეს ყველაფერი ნდობას ეხება. ბევრმა კომპანიამ აღიარა, რომ GDPR-თან შესაბამისობა დადებითად აისახება მათ იმიჯსა და მომხმარებელთა აზრზე, ბიზნესის კეთების მათ მეთოდებთან დაკავშირებით, რაც საშუალებას აძლევთ, შეიძინონ დიდი რაოდენობით ახალი მომხმარებლები და შეინარჩუნონ არსებულნი.

გარდა ამისა, GDPR წარმოადგენს შესაძლებლობას, ბიზნეს საკითხების ახლებური გადაწყვეტისა და ბაზრის ახალი ნიშების აღმოჩენისთვის, უზრუნველყოფს მონაცემთა თავისუფალ მიმოცვლას ევროპის კავშირის წევრ ქვეყნებს შორის და

ზრდის მომხმარებელთა ნდობასა და უსაფრთხოებას — ორ აუცილებელ წინაპირობას ერთიანი ციფრული ბაზრის ფუნქციონირებისთვის.

მონაცემთა დაცვის ორგანოებს მთელს ევროპაში შეიძლება, ჰქონდეთ არაერთი განმასხვავებელი ნიშანი, მაგრამ ჩვენ ყველას გვაქვს კოლექტიური ევროპული ხმა და ვიზიარებთ ერთსა და იმავე მიზანსა და გამოწვევებს. ეს მიზანი არის ევროპის მოქალაქეების მონაცემთა დაცვასთან დაკავშირებული უფლებებისა და ინტერესების ეფექტიანად განხორციელება ჩვენს მუდმივად ცვალებად სამყაროში, სადაც ქვეყნებს შორის მონაცემთა თავისუფალი მიმოცვლა გადამწყვეტ როლს ასრულებს ევროპის სოციალურ-ეკონომიკური ზრდისთვის.

სწორედ ამიტომ, ევროპის კავშირში მონაცემთა დაცვა ციფრული პოლიტიკისა და სტრატეგიის ცენტრალური კომპონენტია და ნებისმიერი მომავალი საკანონმდებლო ინიციატივა უნდა შეესაბამებოდეს მონაცემთა დაცვის ზოგადი რეგულაციით დადგენილ პერსონალურ მონაცემთა დაცვის სტანდარტებს.

ახალი თაობის ონლაინ მომსახურებების სწრაფი პროგრესის გამო, რომელიც სულ უფრო მეტად აგროვებს, აანალიზებს და იყენებს მომხმარებელთა პერსონალურ მონაცემებს და ხელოვნური ინტელექტის დაჩქარებულ პროგრესს, ევროპის კავშირმა დაიწყო ციფრული სივრცის ამბიციური რეფორმა. ეს არის ახალი წესების ყოვლისმომცველი ერთობლიობა ყველა ციფრული მომსახურებისთვის: ციფრული მომსახურებების აქტი და ციფრული ბაზრების აქტი. აღნიშნული არის ერთ-ერთი მთავარი ევროპული საკანონმდებლო ინიციატივა ონლაინ სივრცეში მოქალაქეთა და მომხმარებელთა ფუნდამენტური უფლებების დასაცავად. მიზნობრივი რეკლამა უნდა იყოს უფრო გამჭვირვალე, მაგალითად, მოქალაქეებს ექნებათ უფლება, მიიღონ გამჭვირვალე ინფორმაცია, თუ როგორ მოხდება მათი მონაცემების მონეტიზაცია და აიკრძალება პლატფორმების მანიპულაციური ქმედებები.

2023 წლის იანვარში მონაცემთა დაცვის ევროპულმა საბჭომ გამოსცა სავალდებულო გადაწყვეტილება, რომელშიც ნათქვამია, რომ “Meta”-ს მიერ პერსონალური მონაცემების უკანონოდ დამუშავება ქცევითი რეკლამისთვის, არ არის აუცილებელი “Facebook”-ისა და “Instagram”-ის მომხმარებლებთან არსებული ხელშეკრულებების შესასრულებლად. მსხვილ ტექნოლოგიურ კომპანიებს, რომლებიც მანიპულაციურად იყენებენ მათი მომხმარებლების პერსონალურ მონაცემებს, ახლა უზარმაზარი ჯარიმები ემუქრებათ. როგორც ხორვატიის პერსონალურ მონაცემთა დაცვის სააგენტოს დირექტორს, პატივი მაქვს, ვიყო მონაცემთა დაცვის ევროპული საბჭოს წევრი, რომელიც ხელს უწყობს მონაცემთა დაცვის წესების თანმიმდევრულ გამოყენებას ევროპის კავშირის მასშტაბით და აერთიანებს მონაცემთა დაცვის ექსპერტებს განსხვავებული პროფესიული გამოცდილებითა და ექსპერტიზის ფართო სპექტრით.

ასევე, მადლიერი ვარ, რომ მაქვს შესაძლებლობა, ვითანამშრომლო კოლეგებთან მონაცემთა დაცვის საზედამხედველო ორგანოებიდან მთელს ევროპაში, მათ შორის

განსაკუთრებით მინდა აღვნიშნო ჩემი კოლეგა პერსონალურ მონაცემთა დაცვის სამსახურიდან — დოქტ., დოქტ. ლელა ჯანაშვილი, რომელსაც მისი მანდატის ცხრა თვის განმავლობაში აქვს რიცხვებში გამოხატული შესანიშნავი შედეგები განხორციელებული საქმიანობის ყველა ასპექტში: ინსპექტირებები, კონსულტაციები, ცნობიერების ამაღლების აქტივობები და ევროპულ დონეზე მონაცემთა დაცვის სფეროს გაღრმავებაში შეტანილი ღირებული წვლილი, რომელიც 2022 წელს, თბილისში „ევროპული საქმისწარმოების სამუშაო შეხვედრის“ მასპინძლობაში გამოიხატა.

მოუთმენლად ველი ჩვენ შორის ცოდნისა და გამოცდილების კიდევ უფრო ინტენსიურ გაცვლას, რომელიც მიზნად ისახავს პერსონალური მონაცემების დაცვის სფეროში ევროპული სტანდარტების დანერგვის მხარდაჭერას და საქართველოს ხელშეწყობას ევროპის კავშირისკენ მიმავალ გზაზე.

ზდრავკო ვუკიჩი

ხორვატიის პერსონალურ მონაცემთა
დაცვის სააგენტოს (AZOP) დირექტორი

პროფ., დოქტ. პასკუალე სტანციონეს
მისასალმებელი წერილი

პერსონალური მონაცემები ჩვენი ყოველდღიური ცხოვრების ნაწილია. ნათქვამია — „ჩვენ მონაცემები ვართ“. ყოველდღიურად ხდება პერსონალური მონაცემების დამუშავდება და გაცვლა — მათ შორის ავტომატურად — მრავალი მიზნით. ციფრული მოწყობილობების გამოყენებით, თამაშის, მუშაობის, კვლევის, მოსაზრების საჯაროდ გაზიარების, პროდუქტის ელექტრონულად შეძენის გზით უმრავლესობა გავცემთ პერსონალურ მონაცემებს, რომლებიც მონაცემთა ანალიზის შედეგად, შეიძლება გამოყენებული იქნეს ჩვენი არჩევანის, პრეფერენციების, აზრებისა და გრძნობების შესასწავლად. ამ მონაცემების ბაზაზე შექმნილი სპეციფიკური ციფრული პროფილები შესაძლოა, გამოყენებული იქნას პერსონალიზებული მომსახურების შეთავაზების და პირის ნების ამოცნობის მიზნებისათვის.

საზოგადოებისა და ინდივიდებისთვის ამ ყოველივეს დადებითი გავლენა სადავო არაა, მაგრამ პერსონალური მონაცემების დამუშავება შესაძლოა საფრთხეებსაც უკავშირდებოდეს. როდესაც დამუშავება მიზნად ისახავს, განსაზღვროს, თუ რა შინაარსის ინფორმაციას გაეცნობა მომხმარებელი, მათ ქცევასა და პოლიტიკურ შეხედულებებზე ზემოქმედების მიზნით, მათ შორის, მათი, როგორც ამომრჩევლების სამიზნე ჯგუფად განსაზღვრით, საფრთხის ქვეშ ექცევა დემოკრატიული ღირებულებები, კონსტიტუციური უფლებები და თავისუფლებები, მათ შორის, პირადი ცხოვრების ხელშეუხებლობა, გამოხატვის თავისუფლება და დისკრიმინაციის აკრძალვა.

პირადი ცხოვრებისა და მონაცემთა დაცვა ჩვენი ცხოვრების თითოეულ ასპექტზე ახდენს გავლენას, ამასთან, ეს უფლებები შეიძლება განხილულ იქნეს სხვა ძირითადი უფლებების დაცვის ხელშემწყობ ფაქტორებად. ახალი სოციალურ-ეკონომიკური და ტექნოლოგიური გამოწვევების გათვალისწინებით, ინტერესი პერსონალური მონაცემების დაცვის მიმართ იზრდება და ეს სასიხარულო მოვლენაა.

შესაბამისად, დიდი სიამოვნებით მივესალმები საქართველოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ეგიდით „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ დაფუძნებას: პერსონალურ მონაცემთა დაცვის საკითხებზე ორიენტირებული, იმედის მომცემ საერთაშორისო ჟურნალს, რომლის გვერდებზე შესაძლებელია, აღიბეჭდოს თეორიის სამართლებრივი ანალიზი და შედარებით ჭრილში საერთაშორისოსამართლებრივი პრაქტიკის მიმოხილვა, ისევე, როგორც იმ პროცესის მნიშვნელოვანი ფრაგმენტი, რომელიც მიმართულია საქართველოს მონაცემთა დაცვის სამართლის ევროპეიზაციისკენ.

პერსონალურ მონაცემთა დაცვასთან დაკავშირებული ღირებულებები სცდება ეროვნულ საზღვრებს და ტრადიციულ სოციალურ და ეკონომიკურ დაყოფას. მასთან დაკავშირებული გარანტიები არის (უნდა იყოს) იმავე ბუნების. პერსონალური მონაცემების დაცვა არ უნდა იქნეს

დანახული, როგორც პრივილეგია ან ელიტური უფლება, პირიქით, მისი კონცეპტუალური განვითარება და სამართლებრივი გაძლიერება, გვეხმარება, რომ იგი აღვიქვათ, როგორც საზოგადოებრივი კეთილდღეობა, რომლის დასაცავად შექმნილი გარანტიები უნდა იყოს ტრანსნაციონალური/საერთაშორისო განზომილების.

პირადი ცხოვრების დაცულობა და შემდგომში მონაცემთა დაცვა, საერთაშორისოსამართლებრივი ინსტრუმენტების ფარგლებში გათვალისწინებულია როგორც ძირითადი უფლება (უფლებები)[1].

ევროპის დონეზე, ევროპის კავშირის ძირითადი უფლებების ქარტიის და ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულება (TFEU) განამტკიცებს, რომ „ყველას აქვს პერსონალური მონაცემების დაცვის უფლება" (მიუხედავად ეროვნებისა თუ საცხოვრებელი ადგილისა). აგრეთვე, ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკაში აღნიშნულია, რომ 2016 წლის მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) „იცავს ფიზიკურ პირთა ძირითად უფლებებსა და თავისუფლებებს და, კერძოდ, მათი პერსონალური მონაცემების დაცვის უფლებას". აღნიშნული რეგულაცია, რომელსაც აქვს პირდაპირი მოქმედების ძალა ევროკავშირის ფარგლებში და რომელიც მიზნად ისახავს მოქალაქეთა უფლებების დაცვას და ამისათვის ევროკავშირის მასშტაბით ერთიანი სტანდარტების დამკვიდრებას და მიზნად ისახავს კომპანიებისთვის და საჯარო უწყებებისთვის ადეკვატური პასუხისმგებლობის დაკისრებას, მიმდინარე წელს აღნიშნავს მისი ძალაში შესვლის 5 წლის იუბილეს. იგი შეიძლება, მიჩნეულ იქნეს მისი წინამორბედის (მონაცემთა დაცვის დირექტივა 95/46) ევოლუციად და არა რევოლუციად. მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) განიხილება ღირებულ ინსტრუმენტად იმისათვის, რომ ტექნოლოგიების განვითარების პარალელურად, დაცული იქნეს დემოკრატიული ღირებულებები. GDPR-ი ხშირად განიხილება, როგორც სამაგალითო დოკუმენტი, რომლის შესაბამისადაც უნდა ვითარდებოდეს მსოფლიოს მასშტაბით მონაცემთა დაცვის კანონმდებლობა.

GDPR-ის მთავარი მიღწევები ეჭვგარეშეა და საჭიროებს შენარჩუნებასა და განმტკიცებას. ადამიანის უფლებებთან დაკავშირებული ახალი გამოწვევები საჭიროებს GDPR-ის პრინციპების უფრო მეტი გულმოდგინებით გამოყენებას, ვიდრე უწინ და ზედამხედველობისა და კონტროლის გაძლიერებას. ახალ ტექნოლოგიებთან დაკავშირებით, აღსანიშნავია, რომ GDPR-ი არ უნდა განიხილებოდეს ინოვაციისა და ტექნოლოგიური განვითარებისთვის (მაგალითად, ხელოვნური ინტელექტისთვის) წინაღობად. პირიქით, იგი უნდა შეფასდეს, როგორც შესაძლებლობა. ტექნოლოგიური განვითარების ეპოქაში მას შეუძლია, შეასრულოს

[1] იხ., კერძოდ, 1948 წლის ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-12 მუხლი; სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტის მე-17 მუხლი; 1950 წლის ადამიანის უფლებათა და ძირითად თავისუფლებათა კონვენციის მე-8 მუხლი; ევროპის საბჭოს 1981 წლის 108-ე კონვენცია (მბოჭავი ხასიათის მქონე პირველი საერთაშორისო ინსტრუმენტი მონაცემთა დაცვის მიმართულებით); და მისი მოდერნიზებული ვერსია (108-ე კონვენციის 2018 წლის დამატებითი ოქმი) - ეს უკანასკნელი კვლავაც არ არის ხელმოწერილი რამდენიმე წევრი სახელმწიფოს მიერ.

მნიშვნელოვანი როლი და მონაცემებზე ორიენტირებული ეკონომიკის პირობებში, წარმოშვას კომპანიებისთვის კონკურენტუნარიანობაზე დაფუძნებული უპირატესობა და შესაძლებლობები. GDPR-ის პირველი მუხლი განამტკიცებს, რომ მისი მიზანია ძირითადი უფლებების დაცვის კვალდაკვალ მონაცემთა თავისუფალი ნაკადის უზრუნველყოფა.

აღსანიშნავია, რომ რეგულაცია დგას ახალი გამოწვევების წინაშე, რომლებიც არამხოლოდ ახალი ტექნოლოგიებიდან გამომდინარეობს, არამედ მონაცემთა დამუშავების მეთოდიდან და იქიდან, რომ მონაცემთა განკარგვაზე უფლებამოსილ სუბიექტებს უზარმაზარი (ხშირ შემთხვევაში, წინასწარ განუსაზღვრელი) ძალაუფლება ენიჭებათ. ეკონომიკური და ტექნოლოგიური კონვერგენციის გათვალისწინებით, არსებობს მზარდი საჭიროება, რომ მონაცემთა დაცვის საკანონმდებლო ჩარჩო შეივსოს სამართლის სხვა დარგებითაც, როგორებიცაა კონკურენციის სამართალი, რომელიც, თავის მხრივ სხვადასხვა მარეგულირებელი ორგანოების მიერ რეგულაციური მიდგომების დაახლოების საკითხს წამოჭრის. გამოწვევები აგრეთვე უკავშირდება აღსრულების საკითხსაც, რაც მნიშვნელოვანწილად განპირობებულია ეროვნული ადმინისტრაციული წარმოების წესების, აგრეთვე, ეკონომიკური და პოლიტიკური არჩევანის სხვადასხვაობით.

აზრი არ აქვს მხოლოდ ეროვნული მიდგომის არსებობას, არამედ საჭიროა ფართო საერთო ხედვის არსებობა. ტექნოლოგიების დაახლოებასთან ერთად, საჭიროა ზესახელმწიფოებრივ დონეზე პოლიტიკისა და მარეგულირებელი ჩარჩოს კონვერგენციის გაზრდა, რათა გარკვეულწილად, თავიდან იქნას არიდებული საზიანო განსხვავებული მიდგომებისა და ფრაგმენტაციის რისკი.

გარდა ამისა, უფლებების დაცვის მულტიდისციპლინურ მიდგომას უაღრესი მნიშვნელობა აქვს ძირითადი უფლებებისა და თავისუფლებების ჰარმონიზებული და ყოვლისმომცველი დაცვისთვის, რათა იურისტებმა, პოლიტიკისა და ეკონომიკის ექსპერტებმა, კომპიუტერისა და მონაცემთა სპეციალისტებმა ისაუბრონ და ერთმანეთისგან ისწავლონ.

ცნობიერების ამაღლებასთან დაკავშირებული ისეთი ინიციატივა, როგორიცაა მაგალითად წინამდებარე ჟურნალი, არის განუსაზღვრელი მნიშვნელობის მქონე იმისათვის, რომ მოქალაქეებს, კანონშემოქმედებს შეახსენოს მონაცემთა დაცვის მნიშვნელობა ჩვენი საზოგადოების დემოკრატიული განვითარებისთვის. ასევე, მსგავსი ინიციატივები ხელს უწყობს არსებულ და სამომავლო გამოწვევებთან განმკლავებას.

შესაბამისად, მე სრულად მივესალმები და მხარს ვუჭერ აღნიშნული ჟურნალის ავტორებისა და რედაქტორების მიერ გაწეულ შრომას, რადგან ისინი გონებრივ საზრდოს აწვდიან ყველას, ვისაც სურს, რომ ჩაერთოს აქტუალურ დებატებში და შეიტყოს მეტი აღნიშნული დარგის მიმდინარე საკითხებისა და ინოვაციური კვლევის პერსპექტივების შესახებ.

პროფ., დოქტ. პასკუალე სტანციონე

იტალიის მონაცემთა დაცვის საზედამხედველო
ორგანოს (GPDP) პრეზიდენტი

ასოც. პროფ., დოქტ. სულხან გამყრელიძის
მისასალმებელი წერილი

ნათქვამია, „პირველად იყო სიტყვა“. აზრის თავისუფლებისთვის აუცილებელია თავისუფალი პრესის – ბეჭდური ჟურნალ-გაზეთების, ტელევიზიებისა და ონლაინ-გამოცემების არსებობა. საქართველოში ამ მხრივ ფერთა სიუხვეა. ამ ფერთა სიუხვეში შედარებით მოწიწებით არის წარმოდგენილი პროფესიული სამეცნიერო თუ პრაქტიკული დანიშნულების მუდმივმოქმედი გამოცემები, რომელთაც არსებობის სტაბილური და გრძელვადიანი პერსპექტივა აქვთ.

ამ გადასახედიდან მისასალმებელია, რომ პერსონალურ მონაცემთა დაცვის სამსახური იწყებს პროფესიული მუდმივმოქმედი ჟურნალის გამოცემას. პირადი მონაცემების დაცვა და ამ მონაცემთა უსაფრთხოება თანამედროვე ინდუსტრიული საზოგადოების უზარმაზარ გამოწვევად იქცა.

პირად მონაცემთა დაცვის საკითხი ისეთივე ძველია, როგორც ჩვენი სამყარო. ეს პრობლემა დაკავშირებულია საიდუმლოს სოციალურ ინსტიტუტთან. „ხოლო არარაი არს დაფარული, რომელი არა გამოცხადნეს, და დამალული, რომელი არა საცნაურ იყოს,“ – ნათქვამია სახარებაში. მიუხედავად ამისა, კაცთა შორის, ყოველგვარი საიდუმლოს „საცნაურ ყოფა“, გასაჯაროება, რომ მიზანშეუწონელია, კარგად აჩვენა აღსარების საიდუმლოს არსებობამ. ყველასთვის ცნობილია ჰიპოკრატეს ფიცი, რომელიც ანტიკურ ხანაში ჩაისახა და პირადი მონაცემების დაცვის ერთ-ერთ უმნიშვნელოვანეს ინსტრუმენტად იქცა.

ტექნიკურმა პროგრესმა კიდევ უფრო მეტად გაართულა პიროვნულ მონაცემთა დაცვა. გაზრდილი რისკებისა და გამოწვევების ფონზე, ჟურნალის გამოცემა არის ძალიან კარგი წამოწყება, რომელიც ხელს შეუწყობს პირად მონაცემთა დაცვის ინსტიტუტის განვითარებასა და პოპულარიზაციას. ქართულ საზოგადოებას ვულოცავთ ჟურნალის დაფუძნებას და იმედს ვიტოვებთ, რომ აღნიშნული გამოცემა მხარს დაუჭერს ამ სფეროს ევროპეიზაციას.

ასოც. პროფ., დოქტ. სულხან გამყრელიძე

გრ. რობაქიძის სახელობის უნივერსიტეტის
ასოცირებული პროფესორი

საქართველოში საერთაშორისო სამართლებრივი
თანამშრომლობის გერმანული ფონდის (IRZ)
პროექტის კოორდინატორი

პაატა ტურავა*

საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის სამართლებრივი სტატუსი

თანამედროვე დემოკრატიულ და სამართლებრივ სახელმწიფოებში ტენდენციურია დამოუკიდებელი მარეგულირებელი და საზედამხედველო ორგანოების შექმნის პრაქტიკა. შესაბამისად, აქტუალურია მათი ადგილი ხელისუფლების დანაწილების სისტემაში ისევე, როგორც მათი ლეგიტიმაციის საკითხი. აღსანიშნავია, რომ ამგვარი დამოუკიდებელი მარეგულირებელი და საზედამხედველო ორგანოები არ ექცევიან სახელმწიფო უწყებების გავლენის ქვეშ. მათი ამოცანაა საჯარო გამოწვევების საზოგადოების ინტერესებზე მორგებული კოლექტიური გადაწყვეტა. საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის მაგალითზე, ნაშრომში განხილულია დამოუკიდებელი საზედამხედველო ორგანოების ადგილი ხელისუფლების დანაწილების სისტემაში და მათი ლეგიტიმაციის სამართლებრივი საფუძვლები.

საკვანძო სიტყვები: *დამოუკიდებელი მარეგულირებელი და საზედამხედველო ორგანოები, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახური.*

1. შესავალი

საქართველოს კონსტიტუციის მე-4 მუხლის მე-3 პუნქტის თანახმად, სახელმწიფო ხელისუფლება ხორციელდება ხელისუფლების დანაწილების პრინციპზე დაყრდნობით. სახელმწიფო ხელისუფლება ხორციელდება საკანონმდებლო, აღმასრულებელი და სასამართლო ხელისუფლების ორგანოების მეშვეობით. სახელმწიფო ხელისუფლების განმახორციელებელი სუბიექტი უნდა იყოს ხელისუფლების რომელიმე შტოს ორგანო ან

* ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის პროფესორი, სამართლის დოქტორი.

მისი უფლებამოსილება უნდა გამომდინარეობდეს (დელეგირებული უნდა იყოს) სახელმწიფო ორგანოს უფლებამოსილებიდან.

სახელმწიფო მოწყობის სისტემაში გვხდება დამოუკიდებელი საზედამხედველო და მარეგულირებელი ორგანოები, რომლებიც არ მიეკუთვნება სახელმწიფო ხელისუფლების არცერთ შტოს. სახელმწიფო მოწყობის სამართალში კამათს იწვევს საკითხი დამოუკიდებელი საზედამხედველო და მარეგულირებელი ორგანოების საქმიანობის ლეგიტიმაციასთან დაკავშირებით.[1]

ნაშრომის მიზანია, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის მაგალითზე განსაზღვროს დამოუკიდებელი საზედამხედველო ორგანოების ადგილი ხელისუფლების დანაწილების სისტემაში და დაადგინოს მათი ლეგიტიმაციის სამართლებრივი საფუძვლები. კვლევის მიზნებისთვის საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის სამართლებრივი სტატუსის განსაზღვრა ხდება შედარებითი ანალიზის საფუძველზე. შედარებითი კვლევა განხორციელდება ორი მიმართულებით: პირველი, საკვლევი საკითხის შედარება ხდება იმ დამოუკიდებელ საზედამხედველო ორგანოებთან, რომლის შექმნა და ფუნქციონირება გათვალისწინებულია საქართველოს კონსტიტუციით; მეორე მხრივ, შედარების ობიექტს წარმოადგენს ევროკავშირის ქვეყნების პერსონალურ მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოები, რომლებიც შექმნილია ევროკავშირის მონაცემთა დაცვის 95/46/EC დირექტივის[2] საფუძველზე.

2. ტერმინოლოგიური დაზუსტება

წინამდებარე ნაშრომის მიზნებისთვის, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის სამართლებრივი სტატუსის განსაზღვრისას, უნდა დაზუსტდეს კანონმდებლის მიერ გამოყენებული ტერმინის – „სამსახური“ შინაარსი. სამსახურის ცნების ქვეშ მოიაზრება ის თანამდებობა, რომელიც უკავია პერსონალურ მონაცემთა დაცვის სამსახურის უფროსს. ორგანიზაციული მოწყობის მონოკრატიულ სისტემაში,

[1] *ზომერმანი კ. -ჰ.,* საჯარო მმართველობა დემოკრატიულ და სოციალურ სამართლებრივ სახელმწიფოში, წიგნში: საჯარო მმართველობის სამართლებრივი საფუძვლები სახელმძღვანელო, *ხუბუა გ., ზომერმანი კ .-ჰ. (რედ.),* 2016, 24; აგრეთვე, *Weißgärber K.,* Die Legitimation unabhängiger europäischer und nationaler Agenturen, 2016.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *OJ L 281, 23.11.1995,* repealed by 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).

განსხვავებით კოლეგიური ადმინისტრაციული ორგანოსგან, ერთ თანამდებობაში ვლინდება მისი, როგორც ადმინისტრაციული ორგანოს სტატუსი და უფლებამოსილებები[3]. პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომელი არის საჯარო მოსამსახურე და მასზე ვრცელდება „საჯარო სამსახურის შესახებ“ საქართველოს კანონის მოქმედება. საჯარო მოსამსახურეები ახორციელებენ სამსახურის უფროსის უფლებამოსილებებს. მათი უფლებამოსილებები ნაწარმოებია სამსახურის (უფროსის) უფლებამოსილებებიდან. საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის საჯარო მოსამსახურეების სტატუსი და მათი დაცვის გარანტიები არ წარმოადგენს წინამდებარე ნაშრომის განხილვის საგანს[4].

3. საკითხის აქტუალობა

ნაშრომის მიზანია, პასუხი გაეცეს სამეცნიერო კვლევებში წამოჭრილ პრობლემას პერსონალურ მონაცემთა დაცვის სამსახურის სამართლებრივ სტატუსთან დაკავშირებით. თემის აქტუალობას განაპირობებს ის გარემოება, რომ თანამედროვე დემოკრატიულ და სამართლებრივ სახელმწიფოებში ფართოდ არის გავრცელებული დამოუკიდებელი მარეგულირებელი[5] და საზედამხედველო ორგანოების შექმნის პრაქტიკა, რომელიც არ თავსდება სახელმწიფო ხელისუფლების ორგანიზაციული მოწყობის იერარქიულ სისტემაში. კითხვებს აჩენს ასეთი სახელმწიფო ორგანოების მიმართება ხელისუფლების დანაწილების პრინციპთან მათი ლეგიტიმაციის კონტექსტში.[6] შეკითხვის ავტორები აღნიშნავენ, რომ დემოკრატიის პრინციპის თანახმად, ყველა საკითხზე ბოლო სიტყვა ხალხის მიერ არჩეულ პოლიტიკოსებს ეკუთვნით.

[3] *ტურავა ჰ.*, ზოგადი ადმინისტრაციული სამართალი, 2020, 35.

[4] ეს არ ნიშნავს იმას, რომ სამსახურის ინსტიტუციური მოწყობა არ არის მნიშვნელოვანი. პირიქით, ევროკავშირის სტანდარტი მოითხოვს, რომ წევრმა სახელმწიფოებმა საზედამხედველო ორგანო უზრუნველყონ ადამიანური, ტექნიკური და ფინანსური რესურსებით, ასევე, შენობითა და ინფრასტრუქტურით – საკუთარი ფუნქციებისა და უფლებამოსილებების ეფექტიანად განხორციელებისათვის. მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 69, იხ. წიგნში: *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო* და *ევროპის საბჭო*, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 220.

[5] საქართველოს სინამდვილეში დამოუკიდებელი მარეგულირებელი ორგანოები იქმნება ,,ეროვნული მარეგულირებელი ორგანოების შესახებ“ საქართველოს კანონით. საქართველოში მოქმედი ეროვნული მარეგულირებელი ორგანოებია: ა) საქართველოს კომუნიკაციების ეროვნული კომისია; ბ) საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელი ეროვნული კომისია. მათი ლეგიტიმაციის პრობლემა იდენტურია განსახილველ შემთხვევასთან, რამდენადაც მათი შექმნა და ფუნქციონირება არ არის განსაზღვრული საქართველოს კონსტიტუციით. თუმცა ეს არ არის ნაშრომის განხილვის საგანი.

[6] *Couzinet D.,* die Legitimation unabhängiger Behörden an der Schnittstelle von unionalem und nationalem Verfassungsrecht – Zur Zulässigkeit der unionsrechtlichen Verpflichtung der Mitgliedstaaten zur Errichtung unabhängiger Behörden, in: Verwaltungsrechtsraum Europa, 2011, 213-238.

მეცნიერთა მეორე ნაწილი სადავოდ ხდის თავად ამ პრინციპის შინაარს დამოუკიდებელი ორგანოების არსთან მიმართებით.[7]

საჯარო ამოცანების ორგანიზებასა და შესრულებაზე არსებობს მაღალი საზოგადოებრივი ინტერესი. კანონმდებლის მიერ სახელმწიფოებრივი უფლებამოსილებების დელეგირება დამოუკიდებელი ორგანოებისათვის არის ინსტიტუციური პასუხი ამ გამოწვევაზე. თანამედროვე დემოკრატიულ სისტემებში დგას არა მხოლოდ დამოუკიდებელი ორგანოების კონკრეტული დიზაინისა და ამოცანების ზუსტი განსაზღვრის, არამედ მათი ლეგიტიმაციის პრობლემაც. ერთი მხრივ, ისინი არ უნდა მოექცნენ სახელმწიფო ხელისუფლების ორგანოების გავლენის ქვეშ, ხოლო, მეორე მხრივ, ისინი არიან საზოგადოების აგენტები, რომლებსაც სახელმწიფომ ამოცანად დაუსახა, საჯარო გამოწვევებს მოუძებნონ საზოგადოების ინტერესებზე მორგებული კოლექტიური გადაწყვეტა. დამოუკიდებელი ორგანოები არიან ძლიერი აქტორები, რომლებსაც აქვთ არა მხოლოდ სპეციალიზირებული ცოდნა, არამედ დამოუკიდებლობა პოლიტიკურ ხელისუფლებასთან მიმართებით.[8]

ადმინისტრაციული სამართლის მეცნიერებაში დისკუსიას იწვევს საკითხი, თუ რა არის სახელმწიფო ხელისუფლების სისტემაში მყოფი ადმინისტრაციული ორგანო და რა ამოცანები აქვთ ან უნდა ჰქონდეთ მათ. ასევე, თუ რას ნიშნავს დამოუკიდებელი ორგანო და მათი პოლიტიკური დამოუკიდებლობა თუ დამოკიდებულება ხელისუფლებაზე, არსებობს თუ არა ინსტიტუციური მახასიათებლები, რომელთა დაყრდნობითაც შესაძლებელია მათი დამოუკიდებლობის დადგენა; ხოლო ნორმატიული პერსპექტივით – თუ რა კრიტერიუმები უნდა იქნეს გამოყენებული საფუძვლად, რათა შეფასდეს არა მხოლოდ ხელისუფლებისგან პოლიტიკური დამოუკიდებლობის უპირატესობა, არამედ დადგინდეს მათი ლეგიტიმაცია .[9]

პოლიტიკური გავლენებისგან დამოუკიდებელი ორგანოები, რომლებიც ასრულებენ კონკრეტულ საჯაროსამართლებრივ ფუნქციებს, მიიჩნევიან განვითარებული საბაზრო ეკონომიკის მნიშვნელოვან ფაქტორებად. მიუხედავად მათი ლეგიტიმაციის მიმართ კითხვებისა, დამოუკიდებელი მარეგულირებელი და საზედამხედველო ორგანოები განიხილებიან, როგორც მნიშვნელოვანი აქტორები, რომლებიც მოქმედებენ ავტონომიურად და ხელს უწყობენ საჯარო ამოცანების აღქმისა და შესრულების დეპოლიტიზებას. ამაში მოიაზრება, რომ ისინი შეიძლება შედარებით ეფექტიანად იყვნენ დაცული როგორც პოლიტიკოსების, პოლიტიკური პარტიების ან სახელმწიფო მმართველობის ორგანოების მიმართ ოპორტუნისტული ქცევებისგან, ისე (კერძო) ინტერესთა ჯგუფების გავლენებისგან.[10]

---

[7] *Kruse J.*, In: Unabhängige staatliche Institutionen in der Demokratie, 2013, 19-78.

[8] *Schemmel J.,* Verwaltungslegitimation im Wandel – aus deutschem Blickwinkel, 2016, <www.juwiss.de/57-2016/> [13.01.2022].

[9] *Weißgärber K.,* Die Legitimation unabhängiger europäischer und nationaler Agenturen, 2016.

[10] *Ahrens J., Stark M.*, in: Unabhängige staatliche Institutionen in der Demokratie, 2013.

4. ლეგიტიმური საჯარო მმართველობის არსი

რას ნიშნავს ლეგიტიმური საჯარო მმართველობა? კონსტიტუციის თანახმად, ეს არის დემოკრატიული სახელმწიფოს პრინციპის საფუძველზე განხორციელებული მმართველობა, რაც ნიშნავს, რომ იგი უნდა გამომდინარეობდეს ხალხის, როგორც ხელისუფლების წყაროს მიერ მინიჭებული უფლებამოსილებებიდან. აღნიშნულის გათვალისწინებით, ქვეყნის ძირითადი კანონით ჩამოყალიბებული წარმომადგენლობითი დემოკრატიის პირობებში საჯარო მმართველობის ლეგიტიმაციის უპირველესი სათავე პარლამენტია[11].

ლეგიტიმაციის ტრადიციული მოდელის მიხედვით, ლეგიტიმაციის ზემოთ აღნიშნულ წყაროსთან კავშირი არის სამსვეტიანი, რომელიც იწოდება: პერსონალურ, ინსტიტუციურ და საგნობრივ ლეგიტიმაციად[12]. პერსონალური თვალსაზრისით – დემოკრატიულად არის ლეგიტიმირებული ის თანამდებობა, რომელიც დანიშნული ან არჩეულია თავის მხრივ დემოკრატიულად ლეგიტიმირებული სუბიექტის მიერ. ინსტიტუციური ლეგიტიმაცია კი მოითხოვს პირდაპირ საკანონმდებლო ხელისუფლებასთან ან ირიბად (პარლამენტის მიერ არჩეული მთავრობის მეთაურთან ან წევრებთან) ინსტიტუციურ დაქვემდებარებას, რაც მათ საქმიანობაზე საზედამხედველო უფლებამოსილებასაც მოიცავს. საგნობრივი (შინაარსობრივი) ლეგიტიმაცია კი მიიღწევა მათი საქმიანობის პარლამენტის მიერ მიღებული კანონების საფუძველზე განხორციელებით[13]. დამოუკიდებელი საზედამხედველო ორგანოების „ლეგიტიმაციის ჯაჭვის“ შემოწმებაც სწორედ ლეგიტიმაციის ამ სამი კომპონენტის საფუძველზე ხდება.

დამოუკიდებელი მარეგულირებელი და საზედამხედველო ორგანოების გამოყენების მზარდი პრაქტიკის კვალდაკვალ, ევროკავშირის სახელმწიფოების ადმინისტრაციული სამართლის მეცნიერებაში XXI საუკუნის დასაწყისიდან აქტუალური გახდა საჯარო მმართველობის ლეგიტიმაციის თანამედროვე, უფრო მოქნილი მიდგომების ჩამოყალიბების საკითხი. ამ საქმეში მნიშვნელოვანი წვლილი შეაქვთ წევრი სახელმწიფოების საკონსტიტუციო სასამართლოებს, რომლებიც ცდილობენ, გააქარწყლონ დამოუკიდებელი ორგანოების ლეგიტიმაციის დეფიციტის თაობაზე გამოთქმული მოსაზრებები. მიუხედავად ამ მცდელობებისა, ლეგიტიმაციის

[11] იხ. დაწვრილებით *კობახიძე ი.,* კონსტიტუციური სამართალი, 2020, 77.
[12] იქვე, 79.
[13] *Schuppert G. F.,* Verwaltungswissenschaft, 2000, 471.

ტრადიციული მოდელი დღემდე არ კარგავს აქტუალობას ევროკავშირის ცალკეული სახელმწიფოების ადმინისტრაციული სამართლის მეცნიერებასა და პრაქტიკაში[14].

განსაკუთრებით ლეგიტიმაციის ტრადიციული მოდელის ის კომპონენტი, რომელიც გულისხმობს საჯარო მმართველობის ლეგიტიმაციას სახელმწიფო ხელისუფლების იერარქიულ მოწყობასა და საზედამხედველო უფლებამოსილებაზე დაყრდნობით (ინსტიტუციური ლეგიტიმაცია), ხდება შეუთავსებელი ევროკავშირის მიდგომებთან. ევროკავშირის შეხედულებით, კარგი ადმინისტრაცია გულისხმობს დამოუკიდებელ მმართველობას. უპირველეს ყოვლისა, ეს რეალიზდება ევროკავშირის მმართველობით სტრუქტურებში, რომლებიც საკუთარ ფუნქციებს ასრულებენ წევრი ქვეყნების ადმინისტრაციების გავლენების გარეშე. გარდა ამისა, ჩნდება შთაბეჭდილება, რომ ევროკავშირის შეხედულებით, აპოლიტიკური მმართველობითი რგოლის იდეალური მოდელი გულისხმობს ხალხის მიერ არჩეული გადაწყვეტილების მიმღები პირებისგან დამოუკიდებელ ინსტიტუციურ მოწყობას. ამის საფუძველს იძლევა ის ფაქტი, რომ ევროპელი კანონმდებელი წევრი ქვეყნებისგან ითხოვს, რომ ევროპული კანონების აღსრულება იმ ორგანოების მიერ მოხდეს, რომლებიც არ ექვემდებარებიან სახელმწიფო ხელისუფლების ორგანოების მითითებებს. ამის ერთ-ერთი თვალსაჩინო მაგალითია პერსონალურ მონაცემთა დაცვის ევროპული ნორმების ეროვნულ დონეზე დაცვის ვალდებულების ფარგლებში დამოუკიდებელი საზედამხედველო ორგანოს შექმნის მოთხოვნა.

ზემოთ მოცემულ პრობლემას ნათლად ასახავს გერმანიის ფედერაციულ რესპუბლიკასა და ევროკავშირს შორის დავა. დამოუკიდებელი საზედამხედველო და მარეგულირებელი ორგანოები გახდა ლეგიტიმაციის გერმანული მოდელის მნიშვნელოვანი გამოწვევა. სწორედ პერსონალურ მონაცემთა დაცვის ევროპული დირექტივა გახდა გერმანიის ევროინტეგრაციის პროცესის „მწარე“ ტესტი. მონაცემთა დაცვის 95/46/EC დირექტივის 28-ე მუხლი ითვალისწინებს „სრულიად დამოუკიდებელი“ საზედამხედველო ორგანოების შექმნას. გერმანიაში პერსონალურ მონაცემთა დაცვის სამსახურის დამოუკიდებლობის შინაარსი გაგებული იქნა ადგილობრივი თვითმმართველობის ორგანოების დამოუკიდებლობის ანალოგიურად[15], მათი ლეგიტიმაციის საჭიროების კონტექსტში. გერმანული მიდგომით, დამოუკიდებელი ორგანოების ლეგიტიმაცია მიიღწევა ამ სამსახურებზე ინსტიტუციური ლეგიტიმაციის ჯაჭვის შექმნით. ლეგიტიმაციის მიზნებიდან გამომდინარე, დაშვებული იქნა მონაცემთა დაცვის საზედამხედველო ორგანოებზე

[14] *Schuppert G. F.*, Zur Steuerungsfunktion von Verwaltungsorgnisation und Verwaltungsorganisationsrecht, წიგნში: Verwaltungswissenschaft, 2000, 579.

[15] ადგილობრივი თვითმმართველობის ორგანოების მიმართ დაშვებულია სახელმწიფოს მხრიდან სამართლებრივი და დარგობრივი ზედამხედველობის განხორციელება, რაც თავსებადია მისი ავტონომიური მმართველობის პრინციპთან. ზედამხედველობის ეს ფორმები უზრუნველყოფს თვითმმართველობის საკუთარი და დელეგირებული უფლებამოსილებების განხორციელების ლეგიტიმაციას.

შესაბამისი პასუხისმგებელი მინისტრების მხრიდან მითითებების გაცემის შეზღუდული უფლებამოსილება, რაც გულისხმობდა საქმიანობაზე მხოლოდ სამართლებრივი და არა დარგობრივი ზედამხედველობის განხორციელების შესაძლებლობას. ამ მიდგომამ ევროპული კომისია ვერ დაარწმუნა და დაიწყო სამართლებრივი პროცესი გერმანიის ფედერაციული რესპუბლიკის წინააღმდეგ დირექტივის არასწორი შესრულების გამო. ვერც ევროკავშირის სასამართლოზე მოახდინა შთაბეჭდილება სამართლებრივ და დარგობრივ ზედამხედველობას შორის გამიჯვნის დახვეწილმა გერმანულმა კონცეფციამ. კერძოდ, სასამართლომ უარყო დემოკრატიის პრინციპზე დამყარებული ინსტიტუციური ლეგიტიმაციის ის შინაარსი, რომელსაც გერმანიის სახელმწიფო აყალიბებდა. კომისიამ მიიჩნია, რომ დემოკრატიული სახელმწიფოს პრინციპის გავლენა დამოუკიდებელი ორგანოების ლეგიტიმაციაზე ფუნდამენტურად არ არის დამოკიდებული სახელმწიფო ხელისუფლების ორგანოების მხრიდან მითითებების გაცემის შესაძლებლობაზე. გერმანულ ლიტერატურაში ეს გადაწყვეტილება დიდწილად კრიტიკულად იქნა მიღებული. საბოლოოდ, ავსტრიასთან[16] ერთად, განხორციელდა მეორე მცდელობა დაერწმუნებინათ ევროპის სასამართლო სამართლებრივი ზედამხედველობის, როგორც ლეგიტიმაციის ჯაჭვის საჭიროებაზე, თუმცა უშედეგოდ. სასამართლოს არ შეუცვლია საკუთარი პოზიცია.[17]

5. სამსახურის ,,სრული დამოუკიდებლობის“ განმარტება ევროპის სასამართლოს მიერ

ზემოხსენებულ დავაში – „ევროპული კომისია გერმანიის ფედერალური რესპუბლიკის წინააღმდეგ“ (“European Commission v. Federal Republic of Germany”)[18], კომისიამ არ გაიზიარა გერმანიის ფედერაციული რესპუბლიკის პრაქტიკა 95/46/EC დირექტივის 28(1) მუხლის მე-2 ქვეპუნქტში მოცემულ ფრაზასთან („სრული დამოუკიდებლობის პირობებში“) დაკავშირებით, რაც უკავშირდება პერსონალურ მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანოების შექმნას.[19]

---

[16] დამოუკიდებელი ორგანოს ლეგიტიმაციის პრობლემა ასევე იდგა ავსტრიის შემთხვევაშიც, სადაც საქმეში: CJEU, C-614/10, *European Commission v. Republic of Austria* [16.10.2012] ევროკავშირის მართლმსაჯულების სასამართლომ იმავე პრობლემას გაუსვა ხაზი, დამოუკიდებელ ორგანოზე საზედამხედველო უფლებამოსილება ასუსტებდა ევროკავშირის მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ დამოუკიდებლობის მოთხოვნას.

[17] *Schemmel J.,* Verwaltungslegitimation im Wandel – aus deutschem Blickwinkel, 2016, <www.juwiss.de/57-2016/> [13.01.2022].

[18] გადაწყვეტილება CJEU, C-518/07, *European Commission v Federal Republic of Germany* [09.03.2010].

[19] საზედამხედველო ორგანოების დამოუკიდებლობა მნიშვნელოვან მოთხოვნად მიიჩნევა ევროპის საბჭოს სამართალშიც. მოდერნიზებული 108-ე კონვენციის თანახმად, საზედამხედველო ორგანოები ვალდებულნი არიან, „სრული დამოუკიდებლობითა და მიუკერძოებლობით იმოქმედონ მათზე დაკისრებული ფუნქციებისა და უფლებამოსილებების განხორციელებისას“, ინსტრუქციების მოთხოვნისა

მონაცემთა დაცვის ევროპული კომისია, რომელიც ახდენს ფრაზის – „სრული დამოუკიდებლობის პირობებში“, ფართო ინტერპრეტაციას, მოითხოვს, რომ საზედამხედველო ორგანოების მიერ საკუთარი უფლებამოსილებების „სრული დამოუკიდებლობით“ განხორციელება განიმარტოს, როგორც მათი თავისუფლება ნებისმიერი გარე ზემოქმედებისგან, მათ შორის, სახელმწიფო ორგანოთა პირდაპირი ან არაპირდაპირი გავლენისგან. სახელმწიფო ზედამხედველობა, რომელსაც ექვემდებარებოდნენ გერმანიის მიწების პერსონალური მონაცემების დაცვაზე პასუხისმგებელი ორგანოები არღვევდა ამ მოთხოვნას.[20]

ევროკავშირის მართლმსაჯულების სასამართლო 95/46/EC დირექტივის 28-ე მუხლის როგორც სიტყვასიტყვითი მნიშვნელობის, ისე კანონის მიზნების და სისტემური განმარტების საფუძველზე აღნიშნავს, რომ „სრული დამოუკიდებლობა“ საჯარო ორგანოებთან მიმართებით ნიშნავს, რომ გარანტირებულია მათი თავისუფლება მითითებებისა და ზეგავლენებისგან. სასამართლო აღნიშნავს, რომ გერმანიის ფედერაციული რესპუბლიკის პოზიციისგან განსხვავებით, არაფერი მიუთითებს იმაზე, რომ დამოუკიდებლობის მოთხოვნა ეხება მხოლოდ ზემდგომ ორგანოებსა და მათ კონტროლს დაქვემდებარებულ ინსტიტუტებს შორის ურთიერთობას. პირიქით, ტერმინი „დამოუკიდებლობა“ გამყარებულია ზედსართავი სახელით „სრული“, რაც გულისხმობს გადაწყვეტილების მიღების უფლებამოსილებას, რომელიც თავისუფალია ყოველგვარი პირდაპირი თუ არაპირდაპირი გავლენისგან იერარქიული მოწყობის მიღმაც.[21]

ევროკავშირის მართლმსაჯულების სასამართლოს მიდგომის თანახმად, ეროვნული საზედამხედველო ორგანოების დამოუკიდებლობის გარანტია მიზნად ისახავს, უზრუნველყოს პერსონალური მონაცემების დამუშავების მომწესრიგებელი ნორმების დაცვის ეფექტიანი და საიმედო კონტროლი და იგი უნდა განიმარტოს ამ მიზნის გათვალისწინებით. მისი შემოღება ემსახურება თავად იმ პირების და სტრუქტურული ერთეულების დაცვას, რომლებზეც გავლენას ახდენენ მათი გადაწყვეტილებები და არა პერსონალურ მონაცემთა დაცვის ორგანოსათვის სპეციალური სტატუსის მინიჭებას.[22] შესაბამისად, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოები უნდა იყვნენ ობიექტური და მიუკერძოებელი საკუთარი მოვალეობების განხორციელებისას. ამ მიზნით, ისინი დაცული უნდა იყვნენ ყოველგვარი გარე გავლენისგან, მათ შორის, ფედერალური ან

თუ მიღების გარეშე. იხ: მოდერნიზებული 108-ე კონვენცია, მუხლი 15(5), წიგნში: *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 221.

[20] CJEU, C-518/07, *European Commission v Federal Republic of Germany* [09.03.2010], აბზაცი 15.

[21] იქვე, აბზაცი 19.

[22] სასამართლომ ხაზი გაუსვა, რომ საზედამხედველო ორგანოები პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უფლებების „დამცველები“ არიან. მათი შექმნა წევრ სახელმწიფოში მიჩნეულია ფიზიკურ პირთა დაცვის მნიშვნელოვან კომპონენტად პერსონალურ მონაცემთა დამუშავებისას, იქვე, აბზაცი 23.

მიწების მთავრობების პირდაპირი ან ირიბი გავლენისგან და არა მხოლოდ უშუალო ზემდგომი მაკონტროლებელი ინსტიტუტებისგან.[23]

გერმანიის ფედერაციული რესპუბლიკა აცხადებდა, რომ დამოუკიდებელ ორგანოებზე სახელმწიფო ზედამხედველობა მიზნად ისახავდა მხოლოდ იმის უზრუნველყოფას, რომ დამოუკიდებელი ორგანოების ქმედებები შეესაბამებოდეს ეროვნულ და ევროკავშირის მოქმედ დებულებებს და არ იყო მიმართული ამ ორგანოების პოლიტიკური მიზნების მისაღწევად გამოყენებისკენ, რაც წინააღმდეგობაში მოვიდოდა ფიზიკური პირების პერსონალური მონაცემებისა და ძირითადი უფლებების დაცვის მიზნებთან. მიუხედავად იმისა, რომ დამაჯერებლად მიიჩნია ეს არგუმენტები, ევროკავშირის მართლმსაჯულების სასამართლომ არ გამორიცხა, რომ ზედამხედველობის ორგანოები, რომლებიც არიან სახელმწიფო ადმინისტრაციის შემადგენლობაში და ექვემდებარებიან შესაბამისი მიწის მთავრობებს, იყვნენ არაობიექტურნი პერსონალური მონაცემების დამუშავების რეგულაციების ინტერპრეტაციისა და გამოყენებისას.[24]

ევროკავშირის მართლმსაჯულების სასამართლო მიიჩნევს, რომ პერსონალური მონაცემების დამუშავებისას, მიწის მთავრობა შეიძლება, იყოს დაინტერესებული პერსონალური მონაცემების დაცვის წესების შეუსრულებლობით, როდესაც საქმე ეხება ასეთ დამუშავებას არასაჯარო სფეროში. სახელმწიფო შეიძლება თავად იყოს ამ პროცესის მონაწილე, თუ ეს გავლენას ახდენს ან შეიძლება გავლენა მოახდინოს მასზე, მაგალითად, საჯარო და კერძო თანამშრომლობის შემთხვევაში ან კერძო სექტორთან დადებული კონტრაქტების ფარგლებში. გარდა ამისა, მას შეიძლება, ჰქონდეს განსაკუთრებული ინტერესი, როდესაც მას სჭირდება მონაცემთა ბაზებზე წვდომა გარკვეული ამოცანებისთვის, კერძოდ, საფინანსო მმართველობის ან მართლწესრიგის დაცვის მიზნებისთვის. გარდა ამისა, მთავრობა ასევე შეიძლება იყოს მიდრეკილი, რომ უპირატესობა მიანიჭოს ეკონომიკურ ინტერესებს, როდესაც საქმე ეხება ზემოაღნიშნული რეგულაციების გამოყენებას გარკვეული კომპანიების მიერ, რომლებიც ეკონომიკურად მნიშვნელოვანია ქვეყნის ან რეგიონისთვის.[25]

ევროკავშირის მართლმსაჯულების სასამართლო მიიჩნევს, რომ საზედამხედველო ორგანოების გადაწყვეტილებებზე პოლიტიკური გავლენის მოხდენის უბრალო რისკი საკმარისია იმისათვის, რომ ხელი შეუშალოს მათ დამოუკიდებელ ფუნქციონირებას. ერთი მხრივ, როგორც კომისია აღნიშნავს, დამოუკიდებელი მაკონტროლებელი ორგანოების მხრიდან შეიძლება იყოს „წინასწარი მორჩილება“ საზედამხედველო ორგანოების გადაწყვეტილების მიღების პრაქტიკასთან დაკავშირებით; მეორე მხრივ, მაკონტროლებელი ორგანოების, როგორც პირადი ცხოვრების ხელშეუხებლობის უფლების

[23] იქვე, აბზაცი 25.
[24] იქვე, აბზაცი 33-34.
[25] იქვე, აბზაცი 35.

მცველების როლი მოითხოვს, რომ მათი გადაწყვეტილებები, ანუ თავად ისინი, მიკერძოებულობის ყოველგვარ ეჭვზე მაღლა იდგნენ.[26]

გერმანიის ფედერაციული რესპუბლიკის მიერ დემოკრატიის პრინციპიდან გამომდინარე ლეგიტიმაციის საკითხთან დაკავშირებით გამოთქმულ მოსაზრებაზე, ევროკავშირის მართლმსაჯულების სასამართლო აღნიშნავს, რომ ეს პრინციპი არ ნიშნავს იმას, რომ კლასიკური იერარქიული ადმინისტრაციული სტრუქტურის მიღმა არ შეიძლება არსებობდეს საჯარო დაწესებულება, რომელიც მეტ-ნაკლებად დამოუკიდებელი იქნება ხელისუფლებისგან. ასეთი ორგანოების არსებობა და ფუნქციონირების პირობები რეგულირდება ეროვნული კანონმდებლობით, ზოგიერთ წევრ სახელმწიფოში – კონსტიტუციითაც კი და ეს ორგანოები კანონით არიან შებოჭილი და ექვემდებარებიან სასამართლო კონტროლს. ასეთი დამოუკიდებელი საჯარო ორგანოები, როგორიც ასევე არსებობენ გერმანიის სამართლებრივ სისტემაში, ხშირად ასრულებენ მარეგულირებელ ფუნქციას ან ახორციელებენ ამოცანებს, რომლებიც უნდა იყოს პოლიტიკური გავლენის მიღმა, მაგრამ არიან კანონსა და სასამართლო კონტროლს დაქვემდებარებულნი. ზუსტად ასეთივე უნდა იყოს მიდგომა საზედამხედველო ორგანოების მოწყობის მიმართ პერსონალური მონაცემების დამუშავებასთან დაკავშირებით.[27]

ევროკავშირის მართლმსაჯულების სასამართლო აქვე დასკვნის სახით აღნიშნავს, რომ ეს არ გამორიცხავს დამოუკიდებელი ორგანოს მიმართ საპარლამენტო კონტროლს. 95/96/EC დირექტივა არანაირად ავალდებულებს წევრ სახელმწიფოებს, უარი თქვან პარლამენტის მიერ ამ ორგანოების მიმართ რაიმე შესაძლო გავლენაზე. ერთი მხრივ, დამოუკიდებელი მაკონტროლებელი ორგანოების ხელმძღვანელი პირი შეიძლება, დანიშნოს პარლამენტმა ან მთავრობამ; მეორე მხრივ — საკანონმდებლო ორგანოს შეუძლია განსაზღვროს მაკონტროლებელი ორგანოების კომპეტენცია. გარდა ამისა, საკანონმდებლო ორგანოს შეუძლია, დაავალდებულოს ეს ორგანოები წარუდგინონ ანგარიში პარლამენტს საკუთარი საქმიანობის შესახებ. ყოველივე ზემოაღნიშნულიდან გამომდინარე, ის ფაქტი, რომ პერსონალური მონაცემების დაცვის სამსახური დამოუკიდებელია სახელმწიფო ადმინისტრაციისგან, თავისთავად არ ართმევს ამ ორგანოებს დემოკრატიულ ლეგიტიმაციას.[28]

მონაცემთა დაცვის ევროპული კომისიის და ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებები დამოუკიდებელი მარეგულირებელი ორგანოს „სრული დამოუკიდებლობის“ შინაარსთან დაკავშირებით იძლევა მყარ პოლიტიკურ საფუძვლებს წევრი სახელმწიფოებისთვის, რომ შექმნან რეალურად დამოუკიდებელი მარეგულირებელი ორგანოები. თუმცა იგი არ იძლევა სამართლებრივ გადაწყვეტას, განსაკუთრებით მაშინ, როდესაც მათ შექმნას და ფუნქციონირებას არ აქვს კონსტიტუციური საფუძველი.

[26] იქვე, აბზაცი 36.
[27] იქვე, აბზაცი 42.
[28] იქვე, აბზაცი 43-46.

საკანონმდებლო ხელისუფლების კონსტიტუციური ბოჭვის გარეშე დატოვება აჩენს საფრთხეებს, რომლებიც ყურადღების მიღმა რჩება აღნიშნული ორგანოების ზემოთ მოცემულ მსჯელობებში.

6. კანონი, როგორც ლეგიტიმაციის წყარო

დამოუკიდებელი საზედამხედველო ორგანოების ლეგიტიმაციის ელემენტი – საგნობრივი ლეგიტიმაცია, ერთი შეხედვით, არ დგას კითხვის ნიშნის ქვეშ. სინამდვილეში ეს ასე არ არის. მართალია, პრობლემას არ ქმნის ლეგიტიმაციის წყაროს – სამართლებრივი აქტების მარეგულირებელი შინაარსი, თუმცა დავას იწვევს იქ მოცემული რეგულირების ტექნიკა.

საკანონმდებლო ტექნიკის გერმანული მოდელის შესაბამისად, ადმინისტრაციული სამართლის სფეროში კანონის ნორმები ხშირად კონდიციონალური ბუნებისაა, ანუ აგებულია „თუ მაშინ“ პრინციპით. ასეთი მიდგომის შემთხვევაში, საკანონმდებლო პროგრამები ფუნდამენტურად ვიწრო დერეფანს ტოვებს მისი აღმასრულებლისთვის. ამ მოდელთან კორელაციაშია ტრადიციული მიდგომა – მმართველობითი გადაწყვეტილების შინაარსობრივი ლეგიტიმაცია კანონისადმი დაქვემდებარების გზით. პრობლემურია ფრანგული და ბრიტანული ადმინისტრაციული ტრადიციების გავლენით შექმნილი საკანონმდებლო ტექნიკა, რომელიც ნორმებს ფინალური სახით აყალიბებს, სადაც შესაბამისი გადაწყვეტილებების პოვნა შესაძლებელია გადაწყვეტილების მიმღების ფართო დისკრეციის ფარგლებში, სახელმწიფო ხელისუფლებასა და სამართლებრივი ურთიერთობის მონაწილეებს შორის დიალოგის გზით.

ფინალური ნორმით მინიჭებული თავისუფლების ფარგლებში მიღებული გადაწყვეტილებების მიმართ ჩნდება ლეგიტიმაციის პრობლემა. ამ საკითხის გადაწყვეტას ემსახურება ადმინისტრაციული სამართლის მეცნიერებაში ჩამოყალიბებული დოქტრინა საჯარო მმართველობის დისკრეციული უფლებამოსილების შესახებ. რამდენადაც ეს ინსტიტუტი ბოლომდე ვერ ხსნის პრობლემას, დოქტრინის ფარგლებში ხდება ლეგიტიმაციის სხვა წყაროების მოშველიება, მათ შორის, სახელდება „Output-ლეგიტიმაცია“. ამ მოდელში აქცენტი კეთდება „მონაწილეობით ლეგიტიმაციაზე“, რაც გულისხმობს ისეთი პროცედურული რეგულაციების არსებობას, რომლებიც უზრუნველყოფს საზოგადოების ჩართულობას გადაწყვეტილების მიღების პროცესში.

პერსონალურ მონაცემთა დაცვის სამართალი არის ის ერთ-ერთი დარგი, სადაც განსაკუთრებულ მნიშვნელობას იძენს ინტერესთა შეპირისპირების საფუძველზე გადაწყვეტილების მიღების საკითხი. საჯარო ინფორმაციის ხელმისაწვდომობის საკითხის გადაწყვეტისას, როდესაც საჯარო ინფორმაციის ღიაობის უფლება უპირისპირდება ინფორმაციის საიდუმლოების უფლებას, სამართლებრივი შედეგის

განსაზღვრაში კანონმდებელი საჯარო დაწესებულებას ანიჭებს თავისუფალ სივრცეს, რაც იწოდება ადმინისტრაციული ორგანოს დისკრეციულ უფლებამოსილებად[29]. დისკრეციული უფლებამოსილების უშეცდომოდ განხორციელების ინსტრუმენტი არის საქართველოს ზოგადი ადმინისტრაციული კოდექსის (შემდგომში – სზაკ) მე-7 მუხლში მოცემული საჯარო და კერძო ინტერესების პროპორციულობის პრინციპი[30]. ინტერესთა შეპირისპირება განიმარტება როგორც არგუმენტაციის ტექნიკა, რომელიც ემსახურება სამართლის ნორმით მინიჭებული მოქმედების თავისუფლების კონკრეტიზაციას. ადამიანის უფლებათა ევროპული სასამართლო, ევროკავშირის მართლმსაჯულების სასამართლო, საქართველოს საკონსტიტუციო სასამართლო და საქართველოს საერთო სასამართლოები განსაკუთრებულ აქცენტს აკეთებენ ინტერესთა შეპირისპირებას და დაბალანსებული გადაწყვეტილების მიღებაზე.[31]

პრობლემის გადაწყვეტის გზა ვერ იქნება პერსონალური მონაცემების დაცვის კანონმდებლობაში ფინალურ ნორმებზე უარის თქმა. კანონმდებელმა შეძლებისდაგვარად ზუსტად უნდა განსაზღვროს დისკრეციული უფლებამოსილების მიზანი და ფარგლები და ხელი უნდა შეუწყოს ნორმის აღმასრულებელს განუსაზღვრელი ცნებებისა და შეფასების თავისუფალი სივრცის გამოსაყენებლად აუცილებელი კრიტერიუმების დადგენით.

7. პერსონალურ მონაცემთა დაცვის სამსახურის ადგილი ხელისუფლების მოწყობის სისტემაში

ინსტიტუციური მოწყობის თვალსაზრისით, პერსონალურ მონაცემთა დაცვის სამსახური არ არის აღმასრულებელი ხელისუფლების სისტემის ქვეშ მოქცეული საჯარო მმართველობის ორგანო. სზაკ-ის მე-3 მუხლის მე-2 ნაწილის თანახმად, მასზე არ ვრცელდება აღნიშნული კოდექსის მოქმედება. რაც ნიშნავს იმას, რომ პერსონალურ

[29] საქართველოს ზოგადი ადმინისტრაციული კოდექსის მე-2 მუხლის პირველი ნაწილის „ლ“ ქვეპუნქტის თანახმად, დისკრეციული უფლებამოსილება არის უფლებამოსილება, რომელიც ადმინისტრაციულ ორგანოს ან თანამდებობის პირს ანიჭებს თავისუფლებას საჯარო და კერძო ინტერესების დაცვის საფუძველზე კანონმდებლობის შესაბამისი რამდენიმე გადაწყვეტილებიდან შეარჩიოს ყველაზე მისაღები გადაწყვეტილება.

[30] თუკი პროპორციულობის პრინციპს პერსონალური მონაცემების დამუშავების უფლებამოსილებაზე გადმოვიტანთ, ეს ნიშნავს იმას, რომ პერსონალური მონაცემების დამუშავება უნდა ემსახურებოდეს ლეგიტიმური მიზნის მიღწევას და ეს ღონისძიება უნდა იყოს გამოსადეგი, აუცილებელი და თანაზომიერი.

[31] იხ. *ტურავა პ.*, საჯარო დაწესებულებებში პერსონალური ინფორმაციის ხელმისაწვდომობა, 2022, 15.

მონაცემთა დაცვაზე საზედამხედველო უფლებამოსილება არც ფუნქციურად არის საჯარო მმართველობა[32].

სზაკ-ის მე-3 მუხლის შინაარსზე დაყრდნობით შესაძლებელია, დასკვნის სახით ითქვას, რომ პერსონალურ მონაცემთა დაცვის სამსახური არ ახორციელებს საჯარო მმართველობას. მისი საქმიანობა ასევე არ არის არც კანონშემოქმედება და მართლმსაჯულება. საკითხი, თუ რა არის ის ფუნქცია, რომელიც ხორციელდება პერსონალურ მონაცემთა დაცვის სამსახურის მიერ, ღიად არის დატოვებული კანონმდებლის მიერ. ერთი რამ არის ნათელი, ჩამოთვლილი სამი ფუნქციის მიღმა არსებობს კიდევ სხვა ფუნქცია, რომელიც საჭიროებს კანონის დონეზე შეფასებას და სახელის დარქმევას.

დამოუკიდებელ საზედამხედველო ორგანოებს – საქართველოს სახალხო დამცველი, ეროვნული ბანკი, სახელმწიფო აუდიტის სამსახური, რომელთა შექმნა და ფუნქციონირება საქართველოს კონსტიტუციითაა გათვალისწინებული, შესაძლებელია, ეწოდოს კონსტიტუციური ორგანოები, ხოლო მათი ფუნქციები მოხსენიებულ იქნას, როგორც კონსტიტუციური ფუნქციები.

პერსონალურ მონაცემთა დაცვის სამსახურს არ აქვს კონსტიტუციური საფუძველი, შესაბამისად, მას ვერ ეწოდება კონსტიტუციური ორგანო. რამდენადაც იგი შექმნილია, როგორც საპარლამენტო კონტროლის განხორციელებაში პარლამენტის დამხმარე ორგანო, შესაძლებელია, მას საპარლამენტო კონტროლის ორგანო ეწოდოს. თუმცა, აქვე უნდა აღინიშნოს, რომ მის უფლებამოსილებებში ასევე გვხვდება ისეთი კლასიკური მმართველობითი ფუნქცია, როგორიცაა ადმინისტრაციული სამართალდარღვევების პრევენცია და სამართალდარღვევაზე რეაგირების რეპრესიული ღონისძიებების გამოყენება.

მიუხედავად იმისა, რომ ზემოთ განხილული მონაცემთა დაცვის ევროპული დირექტივა და ევროკავშირის სასამართლო არ ითხოვს პერსონალურ მონაცემთა დაცვის სამსახურის ჩამოყალიბებას კონსტიტუციით გათვალისწინებული დამოუკიდებელი საზედამხედველო ორგანოს სახით, საზედამხედველო ორგანოების გამიჯვნას ორ ნაწილად – საკონსტიტუციო ზედამხედველობის და საპარლამენტო კონტროლის ორგანოებად, აქვს სამართლებრივი დატვირთვა. გამიჯვნის მნიშვნელობა ვლინდება არა მათ მიერ განხორციელებული უფლებამოსილებების სამართლებრივი მნიშვნელობის (გადაწყვეტილებების შესასრულებლად სავალდებულო ძალის) თვალსაზრისით, არამედ მათი დამოუკიდებლობის გარანტიების ასპექტში.

საქართველოს საკონსტიტუციო სასამართლოს პრაქტიკის მიხედვით, „ამა თუ იმ სახელმწიფო თანამდებობის სტატუსს განაპირობებს შესაბამისი საქმიანობის ბუნება,

[32] სზაკ-ის მე-3 მუხლის მე-3 ნაწილი. სზაკ-ის მოქმედება ვრცელდება სამსახურის იმ საქმიანობაზე, რომელიც დაკავშირებულია ადმინისტრაციული ფუნქციის განხორციელებასთან, რაც არ არის ჩვენი კვლევის ობიექტი.

მისი არსი. კერძოდ, მნიშვნელოვანია, დადგინდეს მოცემული თანამდებობა განეკუთვნება საკანონმდებლო, აღმასრულებელ, სასამართლო ხელისუფლებას, წარმოადგენს სხვა კონსტიტუციურ ორგანოს, თუ არ გააჩნია პირდაპირ განსაზღვრული კონსტიტუციური სტატუსი. სახელმწიფო თანამდებობების სტატუსის განსაზღვრისას მხედველობაშია მისაღები ასევე განსახორციელებელი ფუნქციების ხასიათი. ბუნებრივია, განსხვავებულია სხვადასხვა სტატუსის მქონე სახელმწიფო თანამდებობის პირთა მიმართ წარდგენილი საკვალიფიკაციო მოთხოვნები და მათ საქმიანობაში ჩაურევლობის კონსტიტუციური გარანტიებიც. მაგალითისთვის, მოსამართლის, სახალხო დამცველის, პარლამენტის წევრისა და მთავრობის წევრის (მინისტრის) სხვადასხვაგვარი ფუნქციისა და კონსტიტუციურსამართლებრივი როლის შესაბამისად, აღნიშნული სუბიექტები უნდა იქნენ განხილული, როგორც „განსხვავებული დაცვის გარანტიებით აღჭურვილი სახელმწიფო თანამდებობის პირები“[33].

საქართველოს საკონსტიტუციო სასამართლო ხაზს უსვამს იმ გარემოებას, რომ სახელმწიფო ინსპექტორის სამსახური არ არის საქართველოს კონსტიტუციაში სახელდებით პირდაპირ მოხსენიებული ინსტიტუტი. ამის ხაზგასმას აქვს ის მნიშვნელობა, რომ ყოველგვარი ჩარევა, რომელიც დაკავშირებულია კონსტიტუციურ ინსტიტუტებსა და თანამდებობებთან განსხვავებულად ფასდება, ვიდრე კონსტიტუციით გაუთვალისწინებელი ინსტიტუტებისა და თანამდებობების მიმართ განხორციელებული ჩარევა. ეს გამოწვეულია იმით, რომ იმ დამოუკიდებელი საზედამხედველო ორგანოების, რომლებიც არ არიან კონსტიტუციით გათვალისწინებული, შექმნა, რეორგანიზაცია და გაუქმება არის საკანონმდებლო ორგანოს დისკრეცია. ხოლო კონსტიტუციური დამოუკიდებელი მარეგულირებელი და საზედამხედველო ორგანოების შემთხვევაში პარლამენტის ეს დისკრეცია შეზღუდულია. ამავდროულად, როგორც საკონსტიტუციო სასამართლო აღნიშნავს, იმის მხედველობაში მიღებით, რომ სახელმწიფო ინსპექტორის ინსტიტუტის, როგორც სახელმწიფოს მიერ პოზიტიური ვალდებულების ფარგლებში შექმნილი დამოუკიდებელი სამსახურის მნიშვნელობა დემოკრატიულ საზოგადოებაში განსაკუთრებულია და განმტკიცებულია იმით, რომ ამ სამსახურის ხელმძღვანელი გადაწყვეტილების მიღებისა თუ სამსახურის უფლებამოსილების განხორციელების პროცესში უნდა იყოს დამოუკიდებელი, მიუკერძოებელი და თავისუფალი ყოველგვარი შესაძლო გავლენისაგან. საკონსტიტუციო სასამართლო მიიჩნევს, რომ დამოუკიდებელ ორგანოთა ფუნქციებიდან და დაცვის ობიექტიდან გამომდინარე, ასეთი ორგანოების ინსტიტუციური ავტონომია მნიშვნელოვანია ამ სამსახურების საქმიანობის შეუფერხებელი განხორციელებისა და სტაბილურობისთვის, რაც, საერთო ჯამში,

[33] იხ. საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება N1/9/1673,1681, 17 ნოემბერი 2022.

ემსახურება სახელმწიფოში არსებული კონსტიტუციური სიკეთეების დაცვის ვალდებულებას და ხელს უწყობს დემოკრატიული პროცესების განვითარებას[34].

საკონსტიტუციო სასამართლოს გადაწყვეტილების ანალიზი ადასტურებს დამოუკიდებელი საზედამხედველო ორგანოს შექმნის და ფუნქციონირების საკონსტიტუციო საფუძვლების მნიშვნელობას. კონსტიტუციის მიღმა საკითხის მოწესრიგება შეუძლებელია, არ იწვევდეს განსხვავებულ შედეგს. საქართველოს პარლამენტის უფლებამოსილება კონსტიტუციის მიღმა, კანონის მიღების გზით შექმნას დამოუკიდებელი საზედამხედველო ორგანო, ავტომატურად წარმოშობს მის დისკრეციას მის შექმნასთან, რეორგანიზაციასთან და გაუქმებასთან დაკავშირებით. საქართველოს საკონსტიტუციო სასამართლომ ცალსახად აღიარა პარლამენტის დისკრეციული უფლებამოსილება ორ კრიტერიუმზე დაყრდნობით: ა. პარლამენტის მიერ დამოუკიდებელი ორგანოს დანიშვნის უფლებამოსილება, როგორც დისკრეციული უფლებამოსილების წარმოშობის წყარო; და ბ. დამოუკიდებელი ორგანოს კონსტიტუციური სტატუსის არარსებობა. რაც შეეხება სასამართლოს მიერ დადგენილ მოთხოვნას, შრომითი უფლებების დაცვის ვალდებულებიდან გამომდინარე შესაბამისი საკომპენსაციო ღონისძიების დადგენის აუცილებლობის თაობაზე, აღნიშნული არ ახდენს გავლენას განსახილველ საკითხსა და საბოლოო დასკვნაზე, რომ საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის დამოუკიდებლობის დაცვის ხარისხი განსხვავდება კონსტიტუციური დამოუკიდებელი საზედამხედველო ორგანოების დაცვის გარანტიებისგან.

აღნიშნული პრობლემიდან გამოსავალი ვერ იქნებოდა საკონსტიტუციო სასამართლოს განსხვავებული გადაწყვეტილება. სხვაგვარი გადაწყვეტილების მიღება იქნებოდა პრობლემის ხელოვნური გადაწყვეტის მცდელობა. სასამართლომ ამ გადაწყვეტილებით ნათლად დაანახა საჯარო სამართლის მეცნიერებას და პრაქტიკას, პირველ რიგში, საკანონმდებლო ხელისუფლებას, განსახილველ თემაზე შემდგომი მსჯელობის და სათანადო გადაწყვეტილების მიღების აუცილებლობა.

8. პერსონალურ მონაცემთა დაცვის სამსახურის შექმნა, მისი დამოუკიდებლობა და საპარლამენტო კონტროლი

საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის ლეგიტიმაცია უნდა შემოწმდეს ზემოთ განხილული ლეგიტიმაციის ტრადიციული თეორიის ელემენტებზე დაყრდნობით:

[34] იხ. იქვე.

ა) **პერსონალური ლეგიტიმაციის** კონტექსტში, რაც გულისხმობს სამსახურის უფროსის დანიშვნას ხალხის მიერ ლეგიტიმირებული ორგანოს მხრიდან, პერსონალურ მონაცემთა დაცვის სამსახური სრულად აკმაყოფილებს ამ მოთხოვნას და შესაბამისობაშია ევროკავშირის მიერ დადგენილ სტანდარტთან, რამდენადაც პერსონალურ მონაცემთა დაცვის სამსახურის უფროსს ირჩევს საქართველოს პარლამენტი[35].

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის შესარჩევი კონკურსის ჩატარების წესი, კერძოდ, საკონკურსო კომისიის შექმნა საქართველოს პრემიერ-მინისტრის ბრძანებით და კომისიის შემადგენლობა[36] არის არა მისი ლეგიტიმაციის განმსაზღვრელი კრიტერიუმი, არამედ ემსახურება მისი მაღალი სტატუსის ხაზგასმას და დამოუკიდებლობის გარანტიების შექმნას. ეს ასევე გამოწვეულია სამსახურის ფუნქციის შინაარსით, რაც ვრცელდება ხელისუფლების სამივე შტოზე.

ბ) **საგნობრივი ლეგიტიმაციის** შინაარსი არ დგას კითხვის ნიშნის ქვეშ, რამდენადაც პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობა ხორციელდება საქართველოს პარლამენტის მიერ მიღებული კანონის საფუძველზე.

მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვის სამსახური არ არის კონსტიტუციური ორგანო, მისი დამოუკიდებლობის საკანონმდებლო გარანტიები არის მაღალი დონის, რაც იძლევა სამსახურის უფლებამოსილებების რეალურად პოლიტიკური და სხვა ინტერესთა ჯგუფებისგან ჩაურევლად განხორციელების შესაძლებლობას. კერძოდ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს, რომ სამსახური უფლებამოსილებების განხორციელებისას დამოუკიდებელია და არ ექვემდებარება არცერთ ორგანოს და თანამდებობის პირს. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსსა და პერსონალურ მონაცემთა დაცვის სამსახურის მოსამსახურეზე რაიმე ზემოქმედება და მათ საქმიანობაში უკანონო ჩარევა აკრძალულია და კანონით ისჯება[37]. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის უფლებამოსილების ვადის 6 წლით განსაზღვრის მიზანია, რომ ის არ

[35] იხ. 40^3 მუხლი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.

[36] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის შესარჩევი კონკურსი ცხადდება და საკონკურსო კომისია იქმნება საქართველოს პრემიერ-მინისტრის ბრძანებით. ამ საკონკურსო კომისიის წევრები არიან: ა) საქართველოს მთავრობის წარმომადგენელი; ბ) საქართველოს პარლამენტის ადამიანის უფლებათა დაცვისა და სამოქალაქო ინტეგრაციის კომიტეტის თავმჯდომარე; გ) საქართველოს პარლამენტის იურიდიულ საკითხთა კომიტეტის თავმჯდომარე; დ) საქართველოს უზენაესი სასამართლოს თავმჯდომარის მოადგილე; ე) საქართველოს გენერალური პროკურორის პირველი მოადგილე ან მოადგილე; ვ) საქართველოს სახალხო დამცველი ან საქართველოს სახალხო დამცველის წარმომადგენელი; ზ) საქართველოს სახალხო დამცველის მიერ იმ არასამეწარმეო (არაკომერციული) იურიდიული პირის წევრთაგან ღია კონკურსის წესით შერჩეული, სათანადო გამოცდილების მქონე პირი, რომელსაც აქვს ადამიანის უფლებათა დაცვის სფეროში ან/და მონაცემთა დაცვის სფეროში მუშაობის გამოცდილება. 40^3 მუხლი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.

[37] იხ. იქვე, 40^9 მუხლი.

ემთხვეოდეს საქართველოს პარლამენტის უფლებამოსილების ვადას და ამით იქნეს მიღწეული მისი პოლიტიკური ზეგავლენისგან დაცვა[38]. იგივე მიზანი აქვს საკანონმდებლო აკრძალვას, რომ პირი პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის თანამდებობაზე არ შეიძლება არჩეულ იქნეს ზედიზედ ორჯერ[39]. პერსონალურ მონაცემთა დაცვის სამსახურის კანონით განსაზღვრული სამართლებრივი გარანტიები[40] ემსახურება მისი დამოუკიდებლობის უზრუნველყოფას.

რაც შეეხება პერსონალურ მონაცემთა დაცვის სამსახურისთვის კანონმდებლის მიერ ფინალური ბუნების მქონე ნორმების საფუძველზე მინიჭებულ ფართო დისკრეციას, მისი დაძლევა შესაძლებელია კანონის ნორმების დახვეწისა და სამსახურის მიერ ნორმის შეფარდების სწორი პრაქტიკის ჩამოყალიბებით.

გ) პერსონალურ მონაცემთა დაცვის სამსახური არ არის სრულ შესაბამისობაში **ინსტიტუციური ლეგიტიმაციის** ტრადიციული მოდელის შინაარსთან, რაც ითხოვს მასზე საზედამხედველო მექანიზმის არსებობას. თუმცა, ამ მიმართულებითაც სახეზეა მინიმალური სტანდარტი საპარლამენტო ზედამხედველობის სახით, რაც გულისხმობს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ვალდებულებას საქართველოს პარლამენტს წელიწადში ერთხელ, არაუგვიანეს 31 მარტისა, წარუდგინოს ანგარიში საქართველოში მონაცემთა დაცვის მდგომარეობის, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლის შესახებ[41].

საზოგადოების წინაშე ანგარიშვალდებულების გამოხატულებაა პერსონალურ მონაცემთა დაცვის სამსახურის ვალდებულება, განხორციელებული საქმიანობის შესახებ ინფორმაცია მიაწოდოს საზოგადოებას პერსონალურ მონაცემთა დაცვის სამსახურის ვებგვერდის მეშვეობით[42], რაც ზემოთ აღნიშნული დეფიციტის შევსებას ემსახურება.

დასკვნის სახით შეიძლება ითქვას, რომ საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის ლეგიტიმაციის საფუძველს ქმნის სამი ელემენტი: პარლამენტის მიერ მისი არჩევა, მისი უფლებამოსილებების კანონით განსაზღვრა და საპარლამენტო კონტროლი. ინსტიტუციური ლეგიტიმაციის დეფიციტის შევსება არ უნდა მოხდეს იერარქიული დაქვემდებარების შექმნის ხარჯზე, არამედ დამოუკიდებელი ორგანოს სტატუსის გაზრდით, რაზეც ქვემოთ არის საუბარი.

[38] იქვე, 40^3 (8) მუხლი.
[39] იქვე, 40^3 (8) მუხლი.
[40] იქვე, 40^5 მუხლი.
[41] იქვე, 40^{10} მუხლი.
[42] იქვე, 40^{10} (4) მუხლი.

9. პერსონალურ მონაცემთა დაცვის სამსახურის უფლებამოსილებები

პერსონალურ მონაცემთა დაცვის სამსახური ახორციელებს საქართველოში მონაცემთა დამუშავების კანონიერების კონტროლს. ამ სფეროში პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის ძირითადი მიმართულებებია: მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციის გაწევა, მონაცემთა დამუშავების კანონიერების შემოწმება (ინსპექტირება) განცხადების საფუძველზე ან საკუთარი ინიციატივით, საქართველოში მონაცემთა დაცვის მდგომარეობისა და მასთან დაკავშირებული მნიშვნელოვანი მოვლენების შესახებ ინფორმაციის საზოგადოებისთვის მიწოდება და მისი ინფორმირებულობის გაზრდა[43].

პრაქტიკაში არაერთგვაროვნად არის გაგებული პერსონალურ მონაცემთა დაცვის სამსახურის ვალდებულება, შესაბამისი თხოვნის არსებობის შემთხვევაში, კონსულტაცია გაუწიოს სახელმწიფო ხელისუფლების ორგანოებს, მუნიციპალიტეტის ორგანოებს, სხვა საჯარო დაწესებულებებს, კერძო სამართლის იურიდიულ პირებსა და ფიზიკურ პირებს მონაცემთა დამუშავებასა და დაცვასთან დაკავშირებულ ნებისმიერ საკითხზე[44]. კერძოდ, პერსონალურ მონაცემთა დაცვის სამსახურისთვის დასმულ შეკითხვაზე – უნდა გაიცეს თუ არა პერსონალური მონაცემები, მის ავტორს აქვს მოლოდინი, რომ სამსახურის პასუხი იქნება კი ან არა, შესაბამისი დასაბუთებით. ეს მოლოდინი არ შეესაბამება სამსახურის კანონით დადგენილ მანდატს.

პერსონალურ მონაცემთა დაცვის სამსახური არ არის უფლებამოსილი, ჩაერიოს მონაცემთა დამმუშავებლის დისკრეციულ უფლებამოსილებაში. სამსახურის საკონსულტაციო მანდატი შემოიფარგლება იმაზე მითითებით, რომ პერსონალური მონაცემების დამუშავება საჭიროებს ან არ საჭიროებს საჯარო და კერძო ინტერესების შეპირისპირების საფუძველზე გადაწყვეტილების მიღებას. დისკრეციული უფლებამოსილების უშეცდომოდ განხორციელება არის მონაცემთა დამმუშავებლის უფლებამოსილება და პასუხისმგებლობა.

10. დასაცავი სიკეთე

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

[43] იქვე, 40^{11} მუხლი.
[44] იქვე, 40^{15} მუხლი.

იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.

საიდუმლოება, როგორც სოციალური მოვლენა, წარმოიქმნება მაშინ, როდესაც არსებობს კონფლიქტი ურთიერთსაპირისპირო ინტერესებს შორის, სადაც კონკრეტული ინფორმაცია შესაძლოა, გამოყენებული იქნეს ინსტრუმენტად ამ დაპირისპირებაში. პერსონალური მონაცემების არსი მდგომარეობს იმაში, რომ იგი შეიცავს არა მხოლოდ ფაქტებს, არამედ ადამიანების მიმართებას ამ ფაქტებისადმი; საინტერესო ხდება ის ინფორმაცია, რომელიც წარმოადგენს ადამიანებს შორის ურთიერთობის საგანს და არის სხვებისგან დაფარული.[45]

პერსონალურ მონაცემთა დაცვის უფლება უნდა მივიჩნიოთ დამოუკიდებელ ფუნდამენტურ უფლებად თუ პირადი ცხოვრების პატივისცემის ფარგლებში დაცულ უფლებათა ნაწილად, არ არის ამ ნაშრომის განხილვის თემა. უდავოა ის ფაქტი, რომ პერსონალურ მონაცემთა დაცვის უფლება სათავეებს იღებს ამერიკის შეერთებული შტატებში დამკვიდრებული “Right of Privacy” პრინციპიდან. აღნიშნული პრინციპის ფარგლებში პერსონალური მონაცემების დამუშავებასთან დაკავშირებით აღიარებულია სუბიექტის ორი სამართლებრივი პოზიცია: პირველი, “right to be let alone”, მეორე მხრივ – “right to share and withhold”. პირველი პრინციპი ეყრდნობა მოსაზრებას, რომ ყველას უნდა ჰქონდეს უფლება, ცხოვრების ცალკეულ სფეროებში მარტო იგრძნოს თავი, ხოლო მეორე გულისხმობს პიროვნების თავისუფალ არჩევანს, გასცემს თუ არა მასთან დაკავშირებულ ინფორმაციას[46].

პერსონალურ მონაცემთა დაცვის უფლებასთან მიმართებით ჩამოყალიბებული მიდგომა მდგომარეობს იმაში, რომ ის არ არის აბსოლუტური უფლება. მისი კანონიერი შეზღუდვის ერთ-ერთი კრიტერიუმი, რომელსაც აღიარებს, როგორც ევროპის საბჭოს, ისე ევროკავშირის სამართალი, არის სხვათა უფლებებისა და თავისუფლებების დაცვა.[47]

პერსონალურ მონაცემთა დაცვა თანამედროვე და აქტუალურ უფლებად მიიჩნევა, რომელიც ქმნის კონტროლისა და დაბალანსების სისტემას პიროვნების დასაცავად პერსონალურ მონაცემთა დამუშავების პროცესში. პერსონალურ მონაცემთა დამუშავებასთან მიმართებით მნიშვნელოვანია შემდეგი სტანდარტის დაცვა: პერსონალურ მონაცემთა დამუშავება უნდა იყოს სამართლიანი, ხორციელდებოდეს კონკრეტული მიზნებით, შესაბამისი პირის თანხმობით ან ლეგიტიმური საფუძვლით,

[45] დაწვრილებით იხ. *სხირტლაძე ნ.,* პერსონალურ მონაცემთა დაცვის სამართლებრივი ასპექტები, 2017, 154-155.

[46] იხ. *ტურავა პ., ავალიშვილი ლ., ჯორბენაძე ს., კლდიაშვილი გ.,* (რედ.), ინფორმაციის თავისუფლება - გზამკვლევი საჯარო დაწესებულებებისთვის (მეორე გამოცემა), 2016, 8

[47] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 64.

რომელსაც ადგენს კანონმდებლობა. ადამიანებს ხელი უნდა მიუწვდებოდეთ საკუთარ პერსონალურ მონაცემებზე და ჰქონდეთ მათი გასწორების შესაძლებლობა, პერსონალურ მონაცემთა დაცვის უფლებასთან შესაბამისობას კი აკონტროლებდეს დამოუკიდებელი ორგანო.[48]

პერსონალური მონაცემების დაცვის საკითხი მაშინ ხდება აქტუალური, როდესაც მას უპირისპირდება ინფორმაციის საჯაროობის ინტერესი. პერსონალური ინფორმაციის დაცვა გულისხმობს კერძო და საჯარო ინტერესებს შორის ბალანსის მიღწევას[49]. პერსონალურ მონაცემთა დაცვაზე კონტროლი კი იმის შემოწმებაა, თუ რამდენად თანაზომიერია კერძო და საჯარო ინტერესების შეპირისპირების საფუძველზე მიღებული გადაწყვეტილება.[50] პერსონალურ მონაცემთა დაცვის სამსახურის მიუკერძოებლობის მიმართ ყოველთვის იარსებებს ეჭვები, თუ მისი უფლებამოსილების ფარგლებში არ მოექცევა საჯარო ინფორმაციის ხელმისაწვდომობაზე ზედამხედველობის უფლებამოსილება. პერსონალური მონაცემების დაცვასა და საჯარო ინფორმაციის ხელმისაწვდომობაზე პასუხისმგებლობის ერთ ხელში გაერთიანება შესაძლებელს გახდის, ორივე უფლების დაცვა მოხდეს თანაბარ დონეზე და მიღებული იქნას დაბალანსებული გადაწყვეტილება, რომლის მიმართ ორივე მხარეს ექნება თანაბარი ნდობა.

11. დასკვნა

საქართველოს კონსტიტუციის თანახმად, სახელმწიფო ხელისუფლება ხორციელდება ხელისუფლების დანაწილების პრინციპის საფუძველზე. საქართველოს კონსტიტუცია პირდაპირ არ ამბობს, რომ ხელისუფლების დანაწილება გულისხმობს მის დაყოფას ხელისუფლების სამ შტოდ. თუმცა კონსტიტუციის მოწესრიგების სფეროს გაცნობით დგინდება სახელმწიფო ხელისუფლების სამ შტოდ გამიჯვნის აუცილებლობა. საქართველოს კონსტიტუციაში დამოუკიდებელი საზედამხედველო ორგანოების უფლებამოსილებების განსაზღვრა ნათლად ადასტურებს მათ განსაკუთრებულ მნიშვნელობას თანამედროვე, სამართლებრივ და დემოკრატიულ სახელმწიფოში. აღნიშნული გვაძლევს საკმარის საფუძველს იმისა, რომ კონსტიტუციურ დამოუკიდებელ საზედამხედველო ორგანოებს ხელისუფლების მეოთხე შტოს ორგანოები ეწოდოს და აღიარებულ იქნას ხელისუფლების დანაწილების და უფლებამოსილებათა გამიჯვნის ოთხშტოიანი მოდელი.

თუკი დასაშვებია საქართველოს პარლამენტის მიერ საქართველოს კონსტიტუციის მიღმა დამატებით დამოუკიდებელი საზედამხედველო ორგანოს შექმნის

[48] იქვე, 23.
[49] *Khakzadeh-Leiler L.*, *Schmid S.*, *Weber K.*, Interessenabwägung und Abwägungsentscheidungen, 2014, 15, 85.
[50] *ტურავა პ.*, საჯარო დაწესებულებებში პერსონალური ინფორმაციის ხელმისაწვდომობა, 2022, 20.

უფლებამოსილება, აღიარებულ უნდა იქნას მისი განსხვავებული სტატუსი, ხოლო მისი შექმნის გამართლება უნდა მოვძებნოთ საქართველოს მიერ საპარლამენტო ზედამხედველობის განხორციელების უფლებამოსილებაში. ეს იძლევა შესაძლებლობას, პარლამენტის მიერ შექმნილი დამოუკიდებელი საზედამხედველო ორგანო მიჩნეულ იქნას ამ ფუნქციის მხარდამჭერ ორგანოდ და ეწოდოს საპარლამენტო კონტროლის ორგანო.

პარლამენტის მიერ თვითბოჭვის საფუძველზე დამოუკიდებელი საზედამხედველო ორგანოსათვის მინიჭებული დამოუკიდებლობის გარანტიები, რაც გულისხმობს მის საქმიანობაში ჩაურევლობას, არ იწვევს პარლამენტის დისკრეციული უფლებამოსილების გაუქმებას ამ ორგანოს შექმნის, რეორგანიზაციის ან გაუქმების ნაწილში. მოსაზრება, რომ დისკრეციული უფლებამოსილების ფარგლებში გადაწყვეტილების მიღება არ გულისხმობს დაუსაბუთებელი გადაწყვეტილების მიღების შესაძლებლობას, არის მართებული, თუმცა პარლამენტის მიერ საკუთარი უფლებამოსილების ფარგლებში კანონიერი და დასაბუთებული გადაწყვეტილება სამსახურის რეორგანიზაციის თაობაზე, შეიძლება საფრთხეს უქმნიდეს სამსახურის „სრული დამოუკიდებლობის“ გარანტიებს (თუნდაც „მსუსხავი ეფექტის“ სახით). პრობლემიდან გამოსავალი არ არის საქართველოს პარლამენტის დისკრეციის შეზღუდვა ნორმის სხვაგვარი ინტერპრეტაციის გზით, რამდენადაც პარლამენტის უფლებამოსილებების ვიწრო განმარტება წინააღმდეგობაში მოვიდოდა თავად კონსტიტუციასთან. პრობლემის გადაჭრის გზა არის კონსტიტუციის მიღმა არსებული დამოუკიდებელი საზედამხედველო ორგანოებისათვის კონსტიტუციური სტატუსის მინიჭება. საკანონმდებლო ხელისუფლების კონსტიტუციური ნორმის საფუძველზე ბოჭვა არის დამოუკიდებელი საზედამხედველო ორგანოების „სრული დამოუკიდებლობის“ გარანტი. ეს ასევე მოხსნიდა მისი ლეგიტიმაციის პრობლემას, განსაკუთრებით, ორგანიზაციული ლეგიტიმაციის კონტექსტში.

სახელმწიფო ხელისუფლების სისტემაში დამოუკიდებელი საზედამხედველო ორგანოების საკონსტიტუციო საფუძვლების შექმნა[51] ნათლად განსაზღვრავს მათ კონსტიტუციურ სტატუსს სახელმწიფო ხელისუფლების მოწყობის სისტემაში, რაც თავის მხრივ აუცილებელს გახდის *ჯონ ლოკისა* და *შარლ ლუი დე მონტესკიეს* მიერ ჩამოყალიბებული ხელისუფლების დანაწილების თეორიის (ხელისუფლების ორი შტოდან სამი შტოს გამოყოფის დასაბუთებამდე) შემდგომ განვითარებას ხელისუფლების ოთხი შტოს აღიარებამდე: საკანონმდებლო, აღმასრულებელი, სასამართლო და დამოუკიდებელი საზედამხედველო ორგანოების სახით.

[51] იგულისხმება იმ დამოუკიდებელი ორგანოების კონსტიტუციის ქვეშ მოქცევა, რომლებიც არ არიან კონსტიტუციური ორგანოს სტატუსის ქვეშ. ყველა დამოუკიდებელი საზედამხედველო ორგანო უნდა მოექცეს ერთი სტანდარტის ქვეშ.

ბიბლიოგრაფია:

1. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
2. „ეროვნული მარეგულირებელი ორგანოების შესახებ“ საქართველოს კანონი, სსმ, 26, 30/09/2002.
3. საქართველოს ზოგადი ადმინისტრაციული კოდექსი, სსმ, 32(39), 15/07/1999.
4. *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 220, 221.
5. *ზომერმანი კ.-ჰ.,* საჯარო მმართველობა დემოკრატიულ და სოციალურ სამართლებრივ სახელმწიფოში, წიგნში: საჯარო მმართველობის სამართლებრივი საფუძვლები სახელმძღვანელო, *ხუბუა გ., ზომერმანი კ.-ჰ. (რედ.)*, 2016, 24.
6. *კობახიძე ი.,* კონსტიტუციური სამართალი, 2020, 77, 79.
7. *სხირტლაძე ნ.,* პერსონალურ მონაცემთა დაცვის სამართლებრივი ასპექტები, 2017, 154-155.
8. *ტურავა პ.,* ზოგადი ადმინისტრაციული სამართალი, 2020, 35.
9. *ტურავა პ.,* საჯარო დაწესებულებებში პერსონალური ინფორმაციის ხელმისაწვდომობა, 2022, 15, 20.
10. *ტურავა პ., ავალიშვილი ლ., ჯორბენაძე ს., კლდიაშვილი გ.,* (რედ.), ინფორმაციის თავისუფლება - გზამკვლევი საჯარო დაწესებულებებისთვის (მეორე გამოცემა), 2016, 8.
11. საქართველოს საკონსტიტუციო სამართლოს 2022 წლის 17 ნოემბრის № 1/9/1673,1681 გადაწყვეტილება.
12. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *OJ L 281, 23.11.1995,* repealed by 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).
13. *Ahrens J., Stark M.*, in: Unabhängige staatliche Institutionen in der Demokratie, 2013.
14. *Couzinet D.,* die Legitimation unabhängiger Behörden an der Schnittstelle von unionalem und nationalem Verfassungsrecht – Zur Zulässigkeit der unionsrechtlichen Verpflichtung der Mitgliedstaaten zur Errichtung unabhängiger Behörden, in: Verwaltungsrechtsraum Europa, 2011, 213-238.
15. *Kruse J.,* In: Unabhängige staatliche Institutionen in der Demokratie, 2013, 19-78.

16. *Khakzadeh-Leiler L.*, *Schmid S.*, *Weber K.*, Interessenabwägung und Abwägungsentscheidungen, 2014, 15, 85.
17. *Schemmel J.,* Verwaltungslegitimation im Wandel – aus deutschem Blickwinkel, 2016, <www.juwiss.de/57-2016/> [13.01.2022].
18. *Schuppert, G. F.,* Verwaltungswissenschaft, 2000, 471.
19. *Weißgärber K.,* Die Legitimation unabhängiger europäischer und nationaler Agenturen, 2016.
20. CJEU, C-614/10, *European Commission v. Republic of Austria* [16.10.2012].
21. CJEU, C-518/07, *European Commission v Federal Republic of Germany* [09.03.2010].

ნორბერტ ბერნსდორფი*

საძიებო სისტემის ოპერატორები და „დავიწყების უფლება“

„დავიწყების უფლება“ წარმოადგენს შედარებით ახლადშექმნილ იურიდიულ კონცეფციას, რომელსაც დიდი მნიშვნელობა აქვს ინტერნეტ-პოლიტიკისათვის. საძიებო სისტემების პროგრესული ევოლუცია და გავრცელება, ასევე მათი მზარდი ძალა გვაჩვენებს, რომ პირადი ცხოვრების ხელშეუხებლობის გარკვეული მოცულობით დაცვა გარდაუვალია. ეს სტატია ყურადღებას ამახვილებს ევროკავშირის მართლმსაჯულების სასამართლოს 2014 წლის ცნობილ გადაწყვეტილებაზე და 2019 წლის გადაწყვეტილებებზე, რომლებიც სასამართლოს ადრე მოქმედი პრაქტიკის შემავსებელია. ასევე, ყურადღებაა გამახვილებული მასთან მჭიდროდ დაკავშირებულ სამართლებრივ ინსტრუმენტებზე, როგორებიცაა მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) მე-17 მუხლი.

საკვანძო სიტყვები: *„დავიწყების უფლება“, საინფორმაციო საზოგადოება, პერსონალური მონაცემები, მონაცემების დაცვა, მონაცემთა წაშლის უფლება, საძიებო სისტემის ოპერატორი, ინტერნეტ- პოლიტიკა, ევროკავშირის მართლმსაჯულების სასამართლო.*

1. შესავალი

ინტერნეტს აქვს „სპილოს მეხსიერება“ და არაფერი ავიწყდება. საძიებო სისტემები წარმოადგენენ ჩვენი საინფორმაციო საზოგადოების „მცველებს“.[1] არსებობს კი რაიმე საშუალება, რომელიც აიძულებს საძიებო სისტემის ოპერატორებს, წაშალონ ზოგიერთი

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

[1] *Boehme-Neßler V.*, Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2014, 825.

ვებგვერდის მისამართები საძიებო სისტემის შედეგებიდან ან ამოშალონ გარკვეული პერსონალური მონაცემები, რომელთა საძიებო სისტემის მიერ დამუშავება პიროვნებებს აღარ სურთ?

2. განხილვა

„დავიწყების უფლება“ წარმოადგენს შედარებით ახლადშექმნილ იურიდიულ კონცეფციას, რომელიც დიდ გავლენას ახდენს ინტერნეტ-პოლიტიკაზე. გლობალურ დონეზე იგი ჯერაც საკამათო თემაა, გარკვეულწილად იმიტომ, რომ წინააღმდეგობაში მოდის მისსავე ინტერპრეტაციასთან და აგრეთვე, მის იმპლემენტაციასთან დაკავშირებული პრაქტიკული საკითხების გამო.[2] ეს კონცეფცია ასევე ცნობილია, როგორც „წაშლის უფლება“, რომლის მეშვეობით პიროვნებებს შეუძლიათ, მოსთხოვონ ორგანიზაციებს კონკრეტულ შემთხვევებში მათი პერსონალური მონაცემების წაშლა. თუმცა ორგანიზაციებს ყოველთვის არ უწევთ ამის გაკეთება! ეს უფლება შეიძლება, გამოყენებული იყოს მონაცემთა დამმუშავებლების წინააღმდეგ, რომლებიც ვალდებულნი არიან დაუყოვნებლივ გამოეხმაურონ მას.

„დავიწყების უფლებას“ საფუძვლად ევროკავშირის მართლმსაჯულების სასამართლოს 2014 წლის გადაწყვეტილება უდევს.

2.1. ევროკავშირის მართლმსაჯულების სასამართლოს 2014 წლის 13 მაისის გადაწყვეტილება C-131/12 საქმეზე: “გუგლ ესპანეთი”, “გუგლ კორპორაცია”/ესპანეთის მონაცემთა დაცვის ორგანო, მარიო კოსტეხა გონსალესი[3]

2.1.1. 2010 წელს ესპანეთის მონაცემთა დაცვის სააგენტომ სასამართლოს სარჩელით მიმართა კომპანია – “La Vanguardia Ediciones SL”-ის, „გუგლ ესპანეთის“ (“Google Spain”) და „გუგლ კორპორაციის“ (“Google Inc.”) წინააღმდეგ. დავის საგანი იყო ის, რომ როდესაც ინტერნეტის მომხმარებელს „გუგლ-ჯგუფის“ საძიებო სისტემაში შეჰყავდა საკუთარი სახელი, ძიების შედეგების ჩამონათვალი აჩვენებდა გაზეთ „ლა ვანგუარდიას“ (“La Vanguardia”) ორი გვერდის ბმულებს. კერძოდ, ეს გვერდები მოიცავდა ორ განცხადებას უძრავი ქონების აუქციონის შესახებ, რომელიც ორგანიზებული იყო სოციალური

[2] იხ. *Perarnaud Cl.*, Right to Be Forgotten, Digwatch Observatory, <https://www.dig.watch/topics/right-to-be-forgotten, Keyword: Right to be forgotten in 2022> [30.10.2022].

[3] CJEU, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, [2014].

უზრუნველყოფისათვის, მოსარჩელის დავალიანების ანაზღაურების მიზნით კონფისკაციის პროცედურის შემდეგ. აღნიშნული საჩივრით მოსარჩელე მოითხოვდა, რომ პირველი, „ლა ვანგუარდიას“ დავალებოდა მითითებული გვერდების წაშლა ან გადაკეთება (რათა მასთან დაკავშირებული პერსონალური მონაცემები აღარ გამოჩენილიყო) ან მონაცემების დასაცავად გამოეყენებინათ საძიებო სისტემისათვის ხელმისაწვდომი ნებისმიერი საშუალება. მეორე მოთხოვნა შეეხებოდა „გუგლ ესპანეთს“ (“Google Spain”) ან „გუგლ კორპორაციას“ (“Google Inc.”), რომლებსაც უნდა წაეშალათ ან დაემალათ მასთან დაკავშირებული პერსონალური მონაცემები, რათა აღარ გამოჩენილიყო ძიების შედეგებში.[4]

2.1.2. სასამართლოს გადაწყვეტილებაში მოცემულია, რომ უპირველეს ყოვლისა, ინტერნეტში გამოქვეყნებული ინფორმაციის ავტომატური, მუდმივი და სისტემატური ძებნით, სისტემის ოპერატორი „აგროვებს“ მონაცემებს *პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ ევროპის პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის* შესაბამისად (მონაცემთა დაცვის დირექტივა).[5] უფრო მეტიც, სასამართლომ მიიჩნია, რომ ოპერატორი, ინდექსირების პროგრამის ფარგლებში, „პოულობს“, „იწერს“ და „ორგანიზებას უწევს“ მითითებულ მონაცემებს, რომლებსაც შემდგომში თავის სერვერებზე „ინახავს“ და მომხმარებლებისთვის შედეგების ნუსხის ფორმით „ამჟღავნებს“ და „ხელმისაწვდომს ხდის“. ოპერაციები, რომელთაც გამოხატულად და უპირობოდ შეეხებათ ზემოხსენებული დირექტივა, კლასიფიცირდება როგორც „დამუშავება“, მიუხედავად იმ ფაქტისა, რომ საძიებო სისტემის ოპერატორი პერსონალური მონაცემების გარდა სხვა ინფორმაციასთან მიმართებით, მათ განსხვავებულად ახორციელებს. სასამართლომ აგრეთვე აღნიშნა, რომ დირექტივის თანახმად, ეს ოპერაციები ასევე კლასიფიცირდება როგორც „დამუშავება“ მაშინაც კი, თუ ისინი შეეხებიან მხოლოდ იმ მასალას, რომელიც უკვე გამოქვეყნებულია მედიაში წარმოდგენილი ფორმით. ასეთ შემთხვევაში, 95/46/EC დირექტივისგან ზოგადი გამონაკლისის დაწესება გამოიწვევს დირექტივის მოქმედების დიდწილად ჩამორთმევას.

შემდგომში სასამართლომ დაადგინა, რომ დირექტივის თანახმად, ამგვარ დამუშავებასთან მიმართებით საძიებო სისტემის ოპერატორი „დამმუშავებელია“, რაკი იგი წარმოადგენს ოპერატორს, რომელიც განსაზღვრავს დამუშავების მიზანსა და საშუალებებს. ამასთან დაკავშირებით სასამართლომ აღნიშნა, რომ რამდენადაც ასეთი საძიებო სისტემის აქტივობა არის ვებგვერდის გამომქვეყნებლის დამატებითი

[4] CJEU, Press and Information, Press Release No 70/14, 2014.
[5] *Official Journal of the European Communities*, L 281, 1995, 31.

საქმიანობა და მნიშვნელოვანი ზეგავლენის გამო პასუხისმგებელია პირადი ცხოვრების დაცულობისა და პერსონალური მონაცემების დაცვის ფუნდამენტურ უფლებაზე, საძიებო სისტემის ოპერატორმა საკუთარი პასუხისმგებლობით, უფლებამოსილებითა და უნარით უნდა უზრუნველყოს მისი საქმიანობის დირექტივის მოთხოვნებთან შესაბამისობა. ეს არის ერთადერთი გზა, რათა 95/46/EC დირექტივაში განსაზღვრულ გარანტიებს ჰქონდეთ სრულყოფილი ძალა და რომ მონაცემთა სუბიექტების (განსაკუთრებით მათი პირადი ცხოვრების) ეფექტიანი და სრული დაცვა ნამდვილად იქნეს მიღწეული[6].

ამ თვალსაზრისით სასამართლომ აღნიშნა, რომ ასეთი ოპერატორის მიერ პერსონალური მონაცემთა დამუშავება ინტერნეტის მომხმარებელს შესაძლებლობას აძლევს შედეგების სიის საშუალებით გაეცნოს ინტერნეტში მისი პიროვნების შესახებ ინფორმაციის სტრუქტურირებულ მიმოხილვას, როდესაც ძიებას იგი პიროვნების სახელით აწარმოებს. უფრო მეტიც, სასამართლომ აღნიშნა, რომ ეს ინფორმაცია პოტენციურად შეიცავს მისი პირადი ცხოვრების მრავალ ასპექტს და რომ საძიებო სისტემის გარეშე ამ ინფორმაციებს შორის ურთიერთკავშირი ძალიან ძნელად ან საერთოდ ვერ დგინდება. ინტერნეტის მომხმარებლებს ამგვარად შეუძლიათ შექმნან მეტ-ნაკლებად დეტალური პროფილი იმ პიროვნების შესახებ, რომელზეც ხორციელდება ძიება. გარდა ამისა, პიროვნების უფლებებში ჩარევის ზეგავლენა იზრდება იმ მნიშვნელოვანი როლის გამო, რომელსაც დღევანდელ საზოგადოებაში ინტერნეტი და საძიებო სისტემა თამაშობს და რომელიც ყოველმხრივ ასახავს ძიების შედეგების ჩამონათვალში შესულ ინფორმაციას. სასამართლოს აზრით, მისი პოტენციური შესაძლებლობის გათვალისწინებით, ასეთი ჩარევა შეუძლებელია გამართლებული იყოს უბრალოდ იმ ეკონომიური ინტერესით, რომელიც სისტემის ოპერატორს მონაცემთა დამუშავების მიმართ აქვს. თუმცა იმდენად, რამდენადაც შედეგების ნუსხიდან ბმულების ამოღება ინფორმაციაზე წვდომის თვალსაზრისით ზეგავლენას ახდენს ინტერნეტ-მომხმარებლის ლეგიტიმურ ინტერესზე, სასამართლომ დაადგინა, რომ სამართლიანი ბალანსი შესაძლოა, მოიძებნოს ასეთ ინტერესსა და მონაცემთა სუბიექტის ფუნდამენტურ უფლებას, კერძოდ, პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებას შორის. სასამართლომ ამ მხრივ აღნიშნა, რომ მართალია, მონაცემთა სუბიექტის უფლებები, როგორც წესი, გადაწონის ინტერნეტის მომხმარებელთა ინტერესებს, მაგრამ ეს ბალანსი შეიძლება დამოკიდებული იყოს, კონკრეტულ შემთხვევებში, საძიებო ინფორმაციის ბუნებასა და მონაცემთა სუბიექტის პირადი ცხოვრებისადმი მის სენსიტიურობაზე, ასევე, ამ ინფორმაციის მოპოვებისადმი საზოგადოების ინტერესზე, რომელიც შეიძლება

[6] CJEU, Press and Information, Press Release No 70/14.

განსხვავდებოდეს იმ როლის მიხედვით, რომელსაც მონაცემთა სუბიექტი საზოგადოებრივ ცხოვრებაში ასრულებს.[7]

სასამართლო სიტყვა-სიტყვით აღნიშნავს:[8] „... *დირექტივის 95/46/EC მე-12(ბ) მუხლის და მე-14 მუხლის პირველი პარაგრაფის (ა) ქვეპარაგრაფის ინტერპრეტაცია გულისხმობს, რომ იმ დებულებების გამოყენების პირობების შეფასებისას, ყველაფერთან ერთად ისიც უნდა იქნეს განხილული, მონაცემთა სუბიექტს აქვს თუ არა უფლება, რომ მოცემულ დროს, ძიების შედეგების ჩამონათვალში აღნიშნული ინფორმაცია აღარ იყოს დაკავშირებული მის სახელთან, ასეთი უფლების არარსებობა გამოიწვევს მონაცემთა სუბიექტის დაზარალებას. რადგანაც ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებული ფუნდამენტური უფლებების შესაბამისად (ევროკავშირის ფუნდამენტურ უფლებათა ქარტია – ავტორი)[9] მონაცემთა სუბიექტს შეუძლია მოითხოვოს, რომ შედეგების სიიდან წაშლის შედეგად აღნიშნული ინფორმაცია აღარ იყოს საჯაროდ ხელმისაწვდომი. მონაცემთა სუბიექტის უფლება – აღარ იყოს მისი მონაცემები საჯაროდ ხელმისაწვდომი, როგორც წესი, გადაწონის არამხოლოდ საძიებო სისტემის ოპერატორის ეკონომიკურ ინტერესს, არამედ ინფორმაციაზე წვდომის საჯარო ინტერესსაც. თუმცა, ეს ასე არ იქნებოდა, თუ აღმოჩნდებოდა, რომ განსაკუთრებული მიზეზების გამო – როგორიცაა საზოგადოებრივ ცხოვრებაში მონაცემთა სუბიექტის მიერ შესრულებული როლი, მის ფუნდამენტურ უფლებებში ჩარევა გამართლებულია, ფართო საზოგადოების უპირატესი ინტერესით, ჰქონდეს მოცემულ ინფორმაციაზე წვდომა შედეგების ნუსხაში მისი შეყვანის შედეგად.“*

2.2. ევროკავშირის მართლმსაჯულების სასამართლოს 2019 წლის 24 სექტემბრის გადაწყვეტილება C-507/17 საქმეზე: “შპს გუგლი”/ინფორმატიკისა და თავისუფლებების ეროვნული კომისია (CNIL)[10]

2.2.1. შემთხვევა 2015/2016 წლებში მოხდა. სასამართლოს გადაწყვეტილებით, საფრანგეთის მონაცემთა დაცვის ორგანომ (CNIL) „გუგლის კორპორაციას“ (“Google Inc.”) 100.000 ევროს ოდენობის ჯარიმა დააკისრა, მოთხოვნის – გაეუქმებინა ბმული მისი საძიებო სისტემის დომენური სახელების ყველა განფენილობაზე – უარყოფის გამო. გადაეცა რა საფრანგეთის მონაცემთა დაცვის ორგანოს ოფიციალური გაფრთხილება,

[7] იქვე.
[8] CJEU, Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], para. 99.
[9] Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.
[10] CJEU, Case C-507/17, *Google LLC v. Commission nationale de l`informatique et des libertes* (CNIL) [2019].

რომ დაეკმაყოფილებინა ბმულის გაუქმების მოთხოვნა მის ყველა განფენილობაზე, „გუგლ კორპორაციამ“ (შპს „გუგლის“ კანონიერი მემკვიდრე – ავტორი) უარი განაცხადა აღნიშნულის განხორციელებაზე და შემოიფარგლა სადავო ბმულების წაშლით მხოლოდ იმ შედეგებიდან, რომლებიც ნაჩვენები იყო ევროკავშირის (EU) წევრ სახელმწიფოებში მისი საძიებო სისტემის ვერსიების შესაბამისი დომენური სახელებიდან ჩატარებული ძიების შედეგად. „გუგლ კორპორაციამ“ მოსთხოვა სახელმწიფო საბჭოს აღნიშნული სასამართლოს გადაწყვეტილების გაუქმება. მას მიაჩნდა, რომ ბმულის გაუქმების უფლება აუცილებლად არ ნიშნავს, რომ სადავო ბმულები გაუქმებული იყოს გეოგრაფიული შეზღუდვების გარეშე, მისი ძიების სისტემის ყველა დომენური სახელებიდან (“domain names”)[11].

სახელმწიფო საბჭოს სურდა გაეგო, ევროკავშირის კანონმდებლობა პერსონალურ მონაცემთა დაცვის შესახებ[12] განიმარტება თუ არა იმგვარად, რომ ბმულის გაუქმების მოთხოვნის დაკმაყოფილებისას, საძიებო სისტემის ოპერატორს მოეთხოვება აღნიშნული გაუქმების განხორციელება მისი საძიებო სისტემის ყველა ვერსიაზე თუ – პირიქით, ეს მოთხოვნა შეეხება საძიებო სისტემის მხოლოდ იმ ვერსიას, რომელიც შეესაბამება ყველა წევრ სახელმწიფოს ან მხოლოდ იმ წევრი სახელმწიფოს ვერსიას, რომლის რეზიდენტი სარგებლობს ამ გაუქმებით[13].

2.2.2. აღნიშნულ გადაწყვეტილებაში მართლმსაჯულების სასამართლომ განსაზღვრა „დავიწყების უფლების“ ფარგლები საძიებო სისტემის კონტექსტში. სასამართლომ აღნიშნა, რომ გლობალიზებულ მსოფლიოში, ინტერნეტის მომხმარებლების (მათ შორის ევროკავშირის ფარგლებს გარეთ არსებული ინტერნეტის მომხმარებლების) წვდომას ბმულის მონაცემებზე, რომელშიც მოცემულია ინფორმაცია იმ პიროვნების შესახებ, რომლის ინტერესის ობიექტი მდებარეობს ევროკავშირში, მყისიერი და მნიშვნელოვანი ზეგავლენის მოხდენა შეუძლია ევროკავშირში თავადა ამ პიროვნებაზე; ასე, რომ ბმულის გლობალური გაუქმება სრულ შესაბამისობაში იქნება დაცვის მიზანთან, რაც განსაზღვრულია ევროკავშირის სამართლით. თუმცა ბევრი სახელმწიფო არ აღიარებს ბმულის გაუქმების უფლებას ან სხვაგვარი მიდგომა გააჩნიათ ამ უფლებისადმი. სასამართლომ დაამატა, რომ პერსონალურ მონაცემთა დაცვის უფლება აბსოლუტური უფლება არ არის და იგი უნდა განიხილებოდეს მისი ფუნქციის მიხედვით, რომელსაც საზოგადოებაში ასრულებს. ასევე აღნიშნული უნდა შეფასდეს

[11] CJEU, Press and Information, Press Release No 112/19, 2019.
[12] Directive 95/46/EC and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals 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 – GDPR), OJ 2016 L 119, 1, first Corrigendum, OJ 2016 L 314, second Corrigendum, OJ 2018 L 127, and third Corrigendum, OJ 2021 L 074.
[13] CJEU, Press and Information, Press Release No 112/19, 2019.

სხვა ფუნდამენტურ უფლებებთან ურთიერთშეწონვის საფუძველზე, პროპორციულობის პრინციპის შესაბამისად. გარდა ამისა, ბალანსი, ერთი მხრივ, პირადი ცხოვრების უფლებასა და პერსონალური მონაცემთა დაცვასა და მეორე მხრივ, ინტერნეტ მომხმარებლების ინფორმაციის თავისუფლებას შორის შესაძლებელია მნიშვნელოვნად განსხვავდებოდეს[14].

ამგვარად, სასამართლომ დაასკვნა, რომ ამჟამად, ევროკავშირის სამართლის მიხედვით, საძიებო სისტემის ოპერატორი, რომელიც გარემოებებიდან გამომდინარე, წევრი სახელმწიფოს საზედამხედველო თუ სამართლებრივი ორგანოს ბრძანების შედეგად დააკმაყოფილებს მონაცემთა სუბიექტის მოთხოვნას ბმულის გაუქმების შესახებ, არ არის ვალდებული განახორციელოს ასეთი გაუქმება მისი საძიებო სისტემის ყველა ვერსიაზე. თუმცა ევროკავშირის კანონმდებლობა მოითხოვს, რომ საძიებო სისტემის ოპერატორმა ასეთი ბმულები ყველა წევრი სახელმწიფოს შესაბამისი საძიებო სისტემის ვერსიებზე გააუქმოს და მიიღოს საკმარისად ეფექტიანი ზომები, რათა უზრუნველყოს მონაცემთა სუბიექტის ფუნდამენტური უფლებების სათანადო დაცვა. ამგვარად, ასეთი ბმულების გაუქმებას, თუ საჭიროა, თან უნდა მოჰყვებოდეს იმგვარი ზომები, რომლებიც საძიებო სისტემის ვერსიის მეშვეობით შესაძლებელს გახდიან, „ევროკავშირის ფარგლებს გარეთ“ იმ ბმულების ძებნის ეფექტიანად თავის არიდებას, რომლებიც წარმოდგენილია ბმულების გაუქმების მოთხოვნაში (მაგალითად, გეო-ბლოკირება – ავტორი). ეროვნული სასამართლოების გადასაწყვეტია, შეესაბამება თუ არა „გუგლს კორპორაციის“ მიერ მიღებული ზომები დადგენილ მოთხოვნებს. დაბოლოს, სასამართლომ აღნიშნა, რომ მიუხედავად იმისა, რომ ევროკავშირის კანონი ამჟამად არ მოითხოვს საძიებო სისტემის ყველა ვერსიაზე მითითების გაუქმებას, იგი ასევე არც კრძალავს ასეთ პრაქტიკას.[15]

სასამართლომ სიტყვა-სიტყვით ჩამოაყალიბა:[16] *„... რომ 95/46/EC დირექტივის 12(ბ) მუხლის და 14-ე მუხლის პირველი პარაგრაფის (ა) ქვეპარაგრაფისა და 2016/679 რეგულაციის 17(1) მუხლზე დაყრდნობით, როცა საძიებო სისტემის ოპერატორი ბმულის გაუქმების მოთხოვნას ზემოხსენებული მუხლების შესაბამისად აკმაყოფილებს, მას მოეთხოვება, ამ ბმულების გაუქმება განახორციელოს არათუ მისი საძიებო სისტემის ყველა ვერსიაზე, არამედ საძიებო სისტემის მხოლოდ იმ ვერსიაზე, რომელიც მიესადაგება ყველა წევრ სახელმწიფოს, და სადაც საჭიროა, მიიღოს ზომები, რომლებიც სამართლებრივი მოთხოვნების დაკმაყოფილებისას, ეფექტიანად აარიდებენ ან სულ მცირე, სერიოზულ წინააღმდეგობას გაუწევენ ინტერნეტის მომხმარებელს მონაცემთა სუბიექტის სახელით ერთ-ერთი წევრი სახელმწიფოდან ძებნის განხორციელებაში, დაწყებული წვდომიდან, ძიების შემდგომ ნაჩვენები შედეგების ჩამონათვალის*

[14] იქვე.
[15] CJEU, Press and Information, Press Release No 112/19, 2019.
[16] CJEU, Case C-507/17, *Google LLC v. Commission nationale de l`informatique et des libertes* (CNIL) [2019], para. 73.

საშუალებით იმ ბმულებამდე, რომლებიც წარმოადგენენ აღნიშნული მოთხოვნის საგანს...“

2.3. ევროკავშირის მართლმსაჯულების სასამართლოს 2019 წლის 24 სექტემბრის გადაწყვეტილება C-136/17 საქმეზე: “G.C. ” და სხვები/ინფორმატიკისა და თავისუფლებების ეროვნული კომისია (CNIL)[17]

2.3.1. ქალბატონმა “G.C.”-მ და სხვებმა, სახელმწიფო საბჭოს წინაშე საქმე აღძრეს ინფორმატიკისა და თავისუფლების ნაციონალური კომისიის (CNIL) წინააღმდეგ, ამავე CNIL-ის მიერ მიღებულ ოთხ გადაწყვეტილებასთან დაკავშირებით, რომლებითაც უარი ეთქვათ „გუგლ კორპორაციისათვის“ ოფიციალური გაფრთხილების გაგზავნაზე ისეთ სხვადასხვა ბმულების გაუქმებასთან დაკავშირებით, რომლებიც მათი სახელებით მოძებნის შემდეგ, ძიების შედეგების ჩამონათვალში ჩანდა. აღნიშნული ბმულები უკავშირდებოდა მესამე პირის მიერ გამოქვეყნებულ ვებგვერდებს, რომლებიც მოიცავდნენ სატირულ ფოტომონტაჟს ქალი პოლიტიკოსის შესახებ, რომელიც ფსევდონიმით იყო ონლაინ განთავსებული და ასევე სტატიებს ერთ-ერთი პიროვნების შესახებ, რომელიც საუბრობდა საკუთარ, როგორც „საენტოლოგიის ეკლესიის“ საზოგადოებასთან ურთიერთობის ოფიცრის შესაძლებლობებზე; ასევე, მამაკაცი პოლიტიკოსის სასამართლო გამოძიებისა და კიდევ ერთი პიროვნების სასჯელზე, რომელიც მიესაჯა არასრულწლოვანზე სექსუალური ძალადობის გამო. სახელმწიფო საბჭო დაეყრდნო 95/46/EC დირექტივას, რათა დაედგინა, ვრცელდებოდა თუ არა საძიებო სისტემის ოპერატორზე (მისი პასუხისმგებლობის, უფლებამოსილებისა და შესაძლებლობების გათვალისწინებით) განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას (მაგალითად, პოლიტიკური შეხედულება, რელიგიური ან ფილოსოფიური რწმენა და სექსუალური ცხოვრება) მონაცემთა დამმუშავებლებისთვის დადგენილი აკრძალვა.[18]

2.3.2. სასამართლომ განმარტა, რომ იმ პერსონალურ მონაცემთა დამუშავება, რომელიც ააშკარავებს რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიურ რწმენას ან სავაჭრო-კავშირის წევრობას და ასევე, უკავშირდება ჯანმრთელობასა და სექსუალურ ცხოვრებას, აკრძალულია, გარდა საგამონაკლისო შემთხვევებისა. დამატებით, კონკრეტული გამონაკლისის

[17] CJEU, *G.C. and Others v. Commission nationale de l`informatique et des libertes (CNIL)* [2019].
[18] CJEU, Press and Information, Press Release No 113/19, 2019.

გარდა, დამუშავება იმ მონაცემებისა, რომლებიც უკავშირდება სამართალდარღვევებს, სისხლის სამართლის ბრალდებებს ან უსაფრთხოების ღონისძიებებს, შეიძლება განხორციელდეს მხოლოდ სახელმწიფო უწყების ზედამხედველობით; აგრეთვე სისხლის სამართლის ნასამართლობის ერთიანი რეესტრი შეიძლება ფუნქციონირებდეს მხოლოდ სახელმწიფო უწყების ზედამხედველობით. სასამართლომ მხედველობაში მიიღო, რომ ეს აკრძალვა და შეზღუდვები ვრცელდება, ევროკავშირის კანონით გათვალისწინებული გამონაკლისების გარდა, ყველა იმ დამმუშავებლებზე, რომლებიც ამგვარ დამუშავებას ახორციელებენ. თუმცა მან აღნიშნა, რომ საძიებო სისტემის ოპერატორი პასუხისმგებელია არა იმიტომ, რომ დებულებით განსაზღვრული პერსონალური მონაცემები ჩანს მესამე პირის მიერ გამოქვეყნებულ ვებგვერდზე, არამედ აღნიშნული გვერდის მითითების გამო და კონკრეტულად ინტერნეტმომხმარებელთათვის ძებნის შედეგების ჩამონათვალში ვებგვერდის ბმულის ჩვენების გამო.[19]

სასამართლომ დაადგინა, რომ მაშინ, როცა მონაცემთა სუბიექტის უფლებები, როგორც წესი, გადაწონის ინტერნეტმომხმარებელთა ინფორმაციის თავისუფლებას, კითხვის ნიშნის ქვეშ ბალანსის საკითხი დგება, რაც დამოკიდებულია აღნიშნული ინფორმაციის ხასიათზე და მონაცემთა სუბიექტის პირად ცხოვრებასთან მიმართებით მის სენსიტიურობაზე, ასევე ამ ინფორმაციის მოპოვებისადმი საზოგადოების ინტერესზე, რომელიც შეიძლება განსხვავდებოდეს, კერძოდ, იმისდა მიხედვით, თუ რა როლს ასრულებს მონაცემთა სუბიექტი საზოგადოებრივ ცხოვრებაში. ამრიგად, სასამართლომ დაასკვნა, რომ როცა საძიებო სისტემის ოპერატორი იღებს ვებგვერდზე ისეთი ბმულის გაუქმების მოთხოვნას, რომელზეც განსაკუთრებული მონაცემებია გამოქვეყნებული, კონკრეტული საქმის რელევანტური გარემოებების საფუძველზე და მონაცემთა სუბიექტის პირადი ცხოვრებისა და მონაცემთა დაცვის ფუნდამენტურ უფლებებში ჩარევის სერიოზულობის მხედველობაში მიღებით, ოპერატორმა უნდა დაადგინოს, რომ აღნიშნული ბმულის ჩართვა შედეგების ჩამონათვალში, რომელიც ჩანს მონაცემთა სუბიექტის სახელით ძებნის შედეგად, უპირობოდ აუცილებელია იმ ინტერნეტმომხმარებელთა ინფორმაციის თავისუფლების დასაცავად, რომლებიც ამგვარი ძიების მეშვეობით პოტენციურად არიან დაინტერესებულნი ვებგვერდზე წვდომის შესაძლებლობით.[20]

უფრო მეტიც, როცა დამუშავება უკავშირდება მონაცემთა სუბიექტის მიერ აშკარად გასაჯაროებულ მონაცემებს, საძიებო სისტემის ოპერატორს შეუძლია, უარი განაცხადოს ბმულის გაუქმების მოთხოვნაზე მხოლოდ იმ შემთხვევაში, თუ დამუშავება აკმაყოფილებს კანონიერების ყველა სხვა პირობას და თუ მონაცემთა სუბიექტს არ აქვს

[19] იქვე.
[20] იქვე.

უფლება, შეეწინააღმდეგოს აღნიშნულ დამუშავებას, მის კონკრეტულ სიტუაციასთან დაკავშირებულ დამაჯერებელ ლეგიტიმურ საფუძველზე დაყრდნობით.

სასამართლოს სიტყვა-სიტყვით აღნიშნა[21]: *„ ...რომ საძიებო სისტემის ოპერატორის მიერ განსაკუთრებული კატეგორიის მონაცემების დამუშავება, რომელიც გათვალისწინებულია 95/46/EC დირექტივის 8(1) მუხლით, შეიძლება დაექვემდებაროს გამონაკლისებს, რომლებიც განსაზღვრულია 8(2)(ა) და (ე) მუხლში, რომელთა თანახმად, აკრძალვა არ ვრცელდება, თუ მონაცემთა სუბიექტმა გასცა აშკარად გამოხატული თანხმობა ასეთ დამუშავებაზე, გარდა იმ შემთხვევისა, როცა შესაბამისი წევრი სახელმწიფოების კანონი კრძალავს ასეთ თანხმობას ან სადაც დამუშავება უკავშირდება მონაცემებს, რომლებიც აშკარად გასაჯაროვდა მონაცემთა სუბიექტის მიერ. ეს გამონაკლისი მეორდება (ევროკავშირის) 2016/67 რეგულაციის 9(2)(ა) და (ე) მუხლში...*

...რომ, 95/46/EC დირექტივის დებულებების ინტერპრეტაცია უნდა გულისხმობდეს, რომ უპირველესად – ინფორმაცია, რომელიც შეეხება ფიზიკური პირის წინააღმდეგ აღძრულ სამართალწარმოებას, ასევე გარემოების მიხედვით, მისგან გამომდინარე ბრალდებასთან დაკავშირებული ინფორმაცია, წარმოადგენს მონაცემებს, რომლებიც შეეხება „დანაშაულსა“ და „სისხლის სამართლის ნასამართლობას“ 95/46/EC დირექტივის მუხლი 8(5)-ს მიხედვით, და მეორე – საძიებო სისტემის ოპერატორი ვალდებულია, რომ დაეთანხმოს ვებგვერდის იმ ბმულის გაუქმების მოთხოვნას, რომელიც აჩვენებს სამართალწარმოების ადრეულ ეტაპთან დაკავშირებით მითითებულ ინფორმაციას და სამართალწარმოების მიმდინარეობის გათვალისწინებით, არ შეესაბამება არსებულ სიტუაციას იმდენად, რამდენადაც 95/46/EC დირექტივის მუხლი 8(4)-ში მითითებული მნიშვნელოვანი საჯარო ინტერესის საფუძვლების შემოწმებისას დადგენილია, რომ საქმის ყველა გარემოების მხედველობაში მიღებით მონაცემთა სუბიექტის ფუნდამენტური უფლებები, რომლებიც გარანტირებულია მე-7 და მე-8 მუხლებით, ეწინააღმდეგება პოტენციურად დაინტერესებული ინტერნეტმომხმარებლის უფლებებს, რომლებიც დაცულია ქარტიის მუხლი 11-ით (გამოხატვისა და ინფორმაციის თავისუფლება - ავტორი)...“

3. მონაცემთა დაცვის ზოგადი რეგულაციის შესაბამისი მუხლი და პრეამბულის პუნქტი

ევროკავშირის სასამართლოს 2014 წლის გადაწყვეტილების შესაბამისად, ევროპარლამენტმა და საბჭომ დაამტკიცეს ციტირებული მონაცემთა დაცვის ევროკავშირის ზოგადი რეგულაცია 2016/679 (GDPR). მონაცემთა დაცვის ზოგადი

[21] CJEU, *G.C. and Others v. Commission nationale de l`informatique et des libertes (CNIL)* [2019], para. 61 and para. 79.

რეგულაცია (GDPR), რომელიც მიღებულ იქნა 2016 წლის აპრილში და ძალაშია 2018 წლის მაისიდან, წარმოადგენს პერსონალურ მონაცემთა დაცვის ევროკავშირის რეგულაციური ჩარჩოს უახლესი რეფორმის მთავარ ნაწილს. მან ჩაანაცვლა დირექტივა 95/46/EC და გახდა მონაცემთა დაცვის ყველაზე მნიშვნელოვანი მომწესრიგებელი აქტი ევროკავშირში[22].

„დავიწყების უფლება“ მოცემულია ზოგადი რეგულაციის (GDPR) მე-17 მუხლში:

მონაცემთა წაშლის უფლება („დავიწყების უფლება“)

1. მონაცემთა სუბიექტს აქვს უფლება, მოითხოვოს მის შესახებ მონაცემთა დაუყოვნებლივ/გაუმართლებელი დაყოვნების გარეშე წაშლა და დამმუშავებელი ვალდებულია, წაშალოს აღნიშნული მონაცემები თუ სახეზეა ერთ-ერთი შემდეგი საფუძველი:
    ა) მონაცემები აღარ არის საჭირო იმ მიზნისათვის, რომლისთვისაც მოხდა მათი შეგროვება ან სხვაგვარად დამუშავება;
    ბ) მონაცემთა სუბიექტი გაითხოვს თანხმობას, რომელიც იყო მონაცემთა დამუშავების საფუძველი მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის, ან მე-9 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის შესაბამისად და აღარ არსებობს მონაცემთა დამუშავების სხვა სამართლებრივი საფუძველი;
    გ) მონაცემთა სუბიექტმა მოითხოვა მისი მონაცემების დამუშავების შეწყვეტა 21-ე მუხლის პირველი პუნქტის შესაბამისად და არ არსებობს მონაცემთა დამუშავების სხვა საფუძველი, ან მონაცემთა სუბიექტი ითხოვს მონაცემთა დამუშავების შეწყვეტას 21-ე მუხლის მე-2 პუნქტის შესაბამისად;
    დ) მონაცემების დამუშავება მოხდა უკანონოდ;
    ე) მონაცემები უნდა წაიშალოს ევროკავშირის ან წევრი სახელმწიფოს იმ საკანონმდებლო ვალდებულების შესასრულებლად, რომელიც დამმუშავებლისთვის შესასრულებლად სავალდებულოა;
    ვ) მონაცემები შეგროვდა მე-8 მუხლის პირველი პუნქტით გათვალისწინებული ელექტრონული მომსახურებისთვის.
2. როცა დამმუშავებელმა პერსონალური მონაცემები გაასაჯაროვა და პირველი პუნქტის შესაბამისად მას ეკისრება მათი წაშლის ვალდებულება, ხელმისაწვდომი ტექნოლოგიისა და განხორციელების ხარჯების გათვალისწინებით, მან უნდა მიიღოს

[22] დამატებითი ინფორმაციისთვის, იხ.: *Bieker F.*, The Right to Data Protection – Individual and Structural Dimensions of Data Protection in EU Law, Information, Technology and Law, Series, Vol. 34, Kiel, The Hague, 2022; *Kuner Ch., Bygrave L. A.*, *Docksey Ch.*, *Drechsler L. (eds.),* The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020; *von Lewinsky K., Rüpke G., Eckardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, München, 2022.

გონივრული ზომები (მათ შორის ტექნიკური), რათა შეატყობინოს მონაცემთა სხვა დამმუშავებლებს მონაცემებთან დაკავშირებული ნებისმიერი ბმულის, მათი ასლის ან დუბლიკატის წაშლის თაობაზე მონაცემთა სუბიექტის მოთხოვნის შესახებ.

3. ამ მუხლის პირველი და მე-2 პუნქტები არ ვრცელდება თუ მონაცემთა დამუშავება აუცილებელია:
    ა) გამოხატვის თავისუფლებისა და ინფორმაციის მიღების უფლების განხორციელებისათვის;
    ბ) ევროკავშირის ან წევრი სახელმწიფოს კანონის შესაბამისად დამმუშავებლის კანონისმიერი ვალდებულების შესასრულებლად, ან საჯარო ინტერესის სფეროში შემავალი ფუნქციების შესასრულებლად ან დამმუშავებლისათვის კანონით მინიჭებული უფლებამოსილების განსახორციელებლად;
    გ) საჯარო ინტერესის მიზნებისათვის საყოველთაო ჯანმრთელობის დაცვის სფეროში მე-9 მუხლის მე-2 პუნქტის „თ“ და „ი“ ქვეპუნქტების და მე-9 მუხლის მე-3 პუნქტის შესაბამისად;
    დ) საჯარო ინტერესებისათვის არქივირების მიზნით, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისათვის 89-ე მუხლის პირველი პუნქტის შესაბამისად, იმ შემთხვევაში თუ, ამ მუხლის პირველი პუნქტით განსაზღვრული უფლების განხორციელება შეუძლებელს გახდის ან მნიშვნელოვნად დააზიანებს დამუშავების მიზნების მიღწევას; ან
    ე) სამართლებრივი მოთხოვნის დადგენის, განხორციელების ან დაცვის მიზნებისთვის.

შესაბამისი დასახელების წესს ახლავს ზოგადი რეგულაციის (GDPR) პრეამბულის 66-ე პუნქტი:

ონლაინ სივრცეში დავიწყების უფლების გასამყარებლად, მონაცემთა წაშლის უფლება იმგვარად უნდა გაფართოვდეს, რომ დამმუშავებელი, რომელმაც გამოაქვეყნა პერსონალური მონაცემები, ვალდებული უნდა იყოს, რომ აღნიშნული მონაცემების სხვა დამმუშავებლებს დაუკავშირდეს და სთხოვოს მონაცემების ბმულებისა და ასლების წაშლა. ამ დროს დამმუშავებელმა უნდა იმოქმედოს გონივრულად და გამოიყენოს მის ხელთ არსებული ტექნოლოგია და საშუალებები, მათ შორის, ტექნიკური ზომები, რათა მონაცემთა სუბიექტის მოთხოვნაში მითითებული ინფორმაცია პერსონალური მონაცემების დამმუშავებლებს შეატყობინოს.

4. ძირითადი დასკვნები

„დავიწყების უფლება“ ასახავს პიროვნების მოთხოვნას, წაიშალოს კონკრეტული მონაცემები, რათა მესამე პირებმა ვეღარ შეძლონ მათი მოძიება.[23] იგი შეიძლება განიმარტოს, როგორც წარსული ცხოვრებიდან იმ მოვლენებზე „გაჩუმების უფლება“, რომლებიც აღარ ხორციელდება.[24] განსაკუთრებული გარემოებების საფუძველზე, მონაცემთა სუბიექტს შეუძლია, მოსთხოვოს საძიებო სისტემის ოპერატორს, ამოიღოს (გააუქმოს) ძებნის შედეგებიდან ის ბმულები, რომლებსაც მივყავართ იმ ვებგვერდებამდე, რომლებიც შეიცავენ მასთან დაკავშირებულ პერსონალურ მონაცემებს.[25] „დავიწყების უფლება“ წარმოადგენს ადამიანის უფლებას, მაგრამ არა აბსოლუტურ უფლებას. როცა ძებნის შედეგების წაშლამ შესაძლოა, უარყოფითი გავლენა მოახდინოს სხვებზე, მაშინ ასეთი მოთხოვნა ყურადღებით უნდა შემოწმდეს სხვის უფლებებთან მიმართებით. ეს ნიშნავს, რომ „დავიწყების უფლება“ არ არის უპირობოდ გარანტირებული; იგი შეზღუდულია განსაკუთრებით მაშინ, როცა უპირისპირდება ინფორმაციული საზოგადოების გამოხატვის თავისუფლებასა და ინფორმაციის უფლებას ქარტიის მე-11 მუხლის შესაბამისად. სხვა გამონაკლისებს მიეკუთვნება შემთხვევები, როცა წაშლის მოთხოვნას დაქვემდებარებული მონაცემების დამუშავება, აუცილებელია სამართლებრივი ვალდებულებების შესასრულებლად, საზოგადოებრივი ინტერესებიდან, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებიდან გამომდინარე დასაარქივებლად ან იურიდიული მოთხოვნების დასაცავად.[26] შედეგები: თუ მხედველობაში მივიღებთ შეპირისპირებულ ინტერესებს და ინტერნეტის ჰიპერ-დამაკავშირებელ ბუნებას, „დავიწყების უფლება“ უფრო რთული კონცეფციაა, ვიდრე უბრალო მოთხოვნა ინდივიდების მხრიდან, რომ ორგანიზაციამ წაშალოს მათი პერსონალური მონაცემები.[27]

მონაცემთა სუბიექტს არ მოეთხოვება, განახორციელოს საკუთარი „დავიწყების უფლება“. თუმცა მისი განხორციელების შემთხვევაში, წაშლის თაობაზე მოთხოვნა არ ექვემდებარება რაიმე კონკრეტულ ფორმას.[28] ძიების სისტემის ოპერატორსაც შეუძლია, რომ არ მოითხოვოს რაიმე კონკრეტული ფორმა. ეს უფლება უნდა განხორციელდეს დამმუშავებლების მიმართ, რომლებმაც მასზე რეაგირება უნდა მოახდინონ

[23] იხ. *Weber R. H.*, “The Right to be Forgotten”, More than a Pandora´s Box, Journal on Intellectual Property, Information, Technology and E-Commerce Law (JIPITEC), 2011, 120.
[24] *Pino G.*, The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights, *van Hoecke M., Ost F. (eds.),* The Harmonization of Private Law in Europe, 2000, 237.
[25] იხ. *Globocnik J.*, The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17), Journal of European and International IPLaw (GRUR International), Vol. 69, Issue 4, 2020, 381.
[26] Art. 17(3) of the GDPR; see *GDPR.EU*, < https://www.gdpr-info.eu/issues/right-to-be-forgotten> [31.10.2022].
[27] *GDPR.EU*, <https://www.gdpr-info.eu/issues/right-to-be-forgotten> [31.10.2022].
[28] *GDPR.EU*, <https://www.gdpr-info.eu/issues/right-to-be-forgotten> [31.10.2022].

„გაუმართლებელი დაყოვნების“ გარეშე.[29] მიუხედავად შემთხვევის სირთულისა, რეაგირება ნებისმიერ შემთხვევაში, ერთი თვის ვადაში უნდა განხორციელდეს. დამმუშავებელმა უნდა დაადგინოს მონაცემთა სუბიექტის ვინაობა და შეუძლია მოითხოვოს დამატებითი ინფორმაცია.[30] ყველაფერმა ამან შეიძლება, პრობლემა შეუქმნას ორგანიზაციას, რადგან ნებისმიერმა მისმა თანამშრომელმა შეიძლება, მიიღოს კანონიერი სიტყვიერი მოთხოვნა.

5. დასკვნა

წლების ან ათწლეულების შემდეგ, „შეცდომისათვის“ უნდა „დაისაჯოს“ პიროვნება საძიებო სისტემებში ინდექსირებული ისეთი ვებსაიტების გამო, როგორიცაა „გუგლი“?[31] „დავიწყების უფლება“ წარმოიშვა ინდივიდების სურვილიდან, წარმართულიყო მათი ცხოვრება ავტონომიურად, წარსულში ჩადენილი კონკრეტული ქმედების გამო მუდმივი ან პერიოდული სტიგმატიზაციის გარეშე.[32] ეს უფლება შეიქმნა ევროპის მართლმსაჯულების სასამართლოს 2014 წლის ცნობილი გადაწყვეტილებით, რომელიც შემდგომ განვითარდა 2019 წლის ორი გადაწყვეტილებით. ამ უკანასკნელმა საძიებო სისტემების მიერ სენსიტიურ მონაცემთა დამუშავება „ნაცრისფერი ზონიდან“ გამოიყვანა, რაც გამოიწვია სასამართლოს პირველმა გადაწყვეტილებამ; თუმცა, „დავიწყების უფლების“ ზოგიერთი მნიშვნელოვანი ასპექტი პასუხგაუცემელი დარჩა.[33] ეს უფლება ახლა გათვალისწინებულია მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) მე-17 მუხლით. ის კვლავ ღიაა გაუმჯობესებისთვის. თუმცა ეს არავითარ შემთხვევაში შეამცირებს ინტერნეტის ხარისხს ცენზურის საშუალებით.[34]

[29] Art. 17 (1) of the GDPR.

[30] *European Commission* – Rules for Business and Organizations, < https://www.ec.europa.eu/info/law/law-topic/data-protection> [30.10.2022].

[31] იხ. *Cooper B.*, Google And The Right To Be Forgotten, Search Engine Journal (SEJ) 2022, <https://www.searchenginejournal.com/google-and-the-right-to-be-forgotten> [29.10.2022].

[32] *Mantelero A.*, The EU Proposal for a General Data Protection Regulation and the Roots of the “Right to be Forgotten”, Computer Law & Security Review, Vol. 29, Issue 3, 2013, 231.

[33] *Globocnik J.*, The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17), Journal of European and International IPLaw (GRUR International), Vol. 69, Issue 4, 2020, 381.

[34] იხ. *Mayes T.*, We Have No Right to Be Forgotten Online, <https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet> [20.03.2011].

ბიბლიოგრაფია:

1. Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.
2. Directive 95/46/EC and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals 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 – GDPR), OJ 2016 L 119, 1, first Corrigendum, OJ 2016 L 314, second Corrigendum, OJ 2018 L 127, and third Corrigendum, OJ 2021 L 074.
3. *Bieker F.*, The Right to Data Protection – Individual and Structural Dimensions of Data Protection in EU Law, Information, Technology and Law, Series, Vol. 34, Kiel, The Hague, 2022.
4. *Boehme-Neßler V.*, Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2014, 825.
5. *Cooper B.*, Google And The Right To Be Forgotten, Search Engine Journal (SEJ) 2022, <https://www.searchenginejournal.com/google-and-the-right-to-be-forgotten> [29.10.2022].
6. *European Commission* – Rules for Business and Organizations, <https://www.ec.europa.eu/info/law/law-topic/data-protection> [30.10.2022].
7. *Globocnik J.*, The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17), Journal of European and International IPLaw (GRUR International), Vol. 69, Issue 4, 2020, 381.
8. *Kuner Ch., Bygrave L. A.*, *Docksey Ch*., *Drechsler L*. *(eds.),* The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020.
9. *von Lewinsky K., Rüpke G., Eckardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, München, 2022.
10. *Mantelero A.*, The EU Proposal for a General Data Protection Regulation and the Roots of the "Right to be Forgotten", Computer Law & Security Review, Vol. 29, Issue 3, 2013, 231.
11. *Mayes T.*, We Have No Right to Be Forgotten Online, <https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet> [20.03.2011].
12. *Perarnaud Cl.*, Right to Be Forgotten, Digwatch Observatory, <https://www.dig.watch/topics/right-to-be-forgotten, Keyword: Right to be forgotten in 2022> [30.10.2022].
13. *Pino G.*, The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights, *van Hoecke M., Ost F. (eds.),* The Harmonization of Private Law in Europe, 2000, 237.
14. *Weber R. H.*, "The Right to be Forgotten", More than a Pandora´s Box, Journal on Intellectual Property, Information, Technology and E-Commerce Law (JIPITEC), 2011, 120.

15. CJEU, Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014].
16. CJEU, Case C-507/17, *Google LLC v. Commission nationale de l`informatique et des libertes* (CNIL) [2019].
17. CJEU, *G.C. and Others v. Commission nationale de l`informatique et des libertes (CNIL)* [2019].
18. CJEU, Press and Information, Press Release No 70/14, 2014.
19. CJEU, Press and Information, Press Release No 112/19, 2019.
20. <https://www.gdpr-info.eu/issues/right-to-be-forgotten> [31.10.2022].

ატილა პეტერფალვი*
დანიელ ესტერი**

როდესაც ჩვენი მანქანები გვსწავლობენ: ევროპის კავშირის მცდელობები ხელოვნური ინტელექტის საფუძველზე გადაწყვეტილების მიღებისა და პროფილირების რეგულირებასთან დაკავშირებით

ნაშრომის პირველი ნაწილში განხილულია მონაცემებზე ორიენტირებული მანქანურ სწავლებასა და ავტონომიური და ავტომატური გადაწყვეტილებების მიღების უნარის მქონე კომპიუტერული პროგრამის შესაბამისობა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) კონკრეტულ დებულებებთან, რომელიც ძალაშია 2018 წლის 25 მაისიდან. თავდაპირველად, თემა წარმოდგენილია ზოგადი შესავლის სახით ხელოვნური ინტელექტის (AI) სოციალურ ზეგავლენის შესახებ. შემდეგ, აღვნიშნავთ საბაზისო ტექნოლოგიურ ფონს და მანქანური სწავლების რამდენიმე ძირითად კონცეფციას, ასეთ მონაცემთა დამუშავების სამართლებრივად რელევანტურ საკითხებს. მოგვიანებით მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) შესაბამისი დებულებები, ასევე მათ გამოყენებასთან დაკავშირებული ზოგიერთი საკითხი და მათი გადაჭრის გზები იქნება წარმოდგენილი. კვლევის მეორე ნაწილში განხილულია მონაცემებით მართული ავტომატური პროფილირების სოციალური ზეგავლენის ცნობილი მაგალითი, ე. წ. „კემბრიჯ ანალიტიკის“ სკანდალში ამომრჩევლების სურვილსა და შეგნებაზე ირიბი ზეგავლენა, რომელშიც მონაცემთა დაცვის ფენომენის მნიშვნელობა კარგად არის წარმოჩენილი. ბოლო თავში კი მოკლედ არის წარმოდგენილი ევროკავშირის ხელოვნური ინტელექტის (AI) ახალი კოდექსის პროექტი და მისი მცდელობა, ახალი კანონმდებლობით დაარეგულიროს ეს ფენომენი, რომელიც

* ეტვოშ ლორანდ უნივერსიტეტის საპატიო პროფესორი, სამართლის დოქტორი; უნგრეთის მონაცემთა დაცვისა და ინფორმაციული თავისუფლების ეროვნული საზედამხედველო ორგანოს პრეზიდენტი.
** სამართლის დოქტორი; უნგრეთის მონაცემთა დაცვისა და ინფორმაციული თავისუფლების ეროვნული საზედამხედველო ორგანოს, ავტორიზაციისა და ინციდენტის შეტყობინების დეპარტამენტის უფროსის მოადგილე.

სულ უფრო და უფრო მეტ სამეცნიერო და პროფესიულ დებატებს წარმოშობს.

საკვანძო სიტყვები: *ავტომატური გადაწყვეტილების მიღება, პროფილირება, GDPR (მონაცემთა დაცვის ზოგადი რეგულაცია), ხელოვნური ინტელექტი, მანქანური სწავლება, „კემბრიჯ ანალიტიკა“, AI (ხელოვნური ინტელექტის) რეგულაცია.*

1. შესავალი: ხელოვნური ინტელექტი, როგორც რეგულირებადი ფენომენი

ბოლო ხანებში, აქტიური სამეცნიერო მსჯელობა დაიწყო ხელოვნური ინტელექტის (AI) განვითარებასა და ფუნქციონირებასთან დაკავშირებით ასევე იურისტებს შორის. მაშინ, როცა ხუთი-ექვსი წლის წინ ამ თემის წამოწევაც კი ფუტურისტული და იდეალისტური ჩანდა, დღეს მოქმედი ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის ცალკეული მუხლები წარმოადგენენ ავტომატური გადაწვეტილების მიღების მოწესრიგების მცდელობას; უფრო მეტიც, აპირებენ, მიიღონ ევროკავშირის ზოგადი სამართლებრივი რეგულაცია ხელოვნურ ინტელექტზე დაფუძნებული პროგრამული უზრუნველყოფის განვითარებასა და ფუნქციონირებასთან დაკავშირებით.

თუმცა, უნდა აღინიშნოს, რომ ავტონომიური გადაწყვეტილების მიღების უნარის მქონე კომპიუტერული პროგრამებისა და მანქანების სამყაროს მხრიდან გამოვლენილ არაკეთილგანწყობასთან დაკავშირებული პირველყოფილი შიში ჯერაც შეინიშნება ყოველდღიურ ახალ ამბებში და ამ ფენომენთან დაკავშირებით გამართულ სამეცნიერო კონფერენციებზე, კითხვა პასუხის დროსაც კი.

ბოლო წლებში, ჩვენ მივაღწიეთ იმ ეტაპს, როცა კანონმდებლისთვის შეუძლებელია, გადადოს აღნიშნული საკითხების სამართლებრივი რეგულირება: ხელოვნური ინტელექტი იმდენად მომწიფდა, რომ იგი გადაიქცა საზოგადოებრივ ფენომენად, რომელიც მოწესრიგებას საჭიროებს. ამას კი ბიძგი მისცა მომხმარებლის პროფილირებისა და ავტომატური გადაწყვეტილების მიღების საკითხებთან დაკავშირებით მომხდარმა შემთხვევებმა, მაგალითად, კემბრიჯ ანალიტიკის სკანდალი, რომელიც დეტალურად განიხილება ამ ნაშრომში.

თუმცა, მოდით, არ გავუსწროთ დროს. უპირველეს ყოვლისა, ვნახოთ, სად დაიწყო ურთიერთობა მანქანებსა და მონაცემებს შორის, რა გავლენის მოხდენა შეუძლია მას

ადამიანებზე და რა სახის ტიპურ სოციალურ და სამართლებრივ რეაქციებთან შეიძლება იყოს დაკავშირებული.

2. რატომ გვეშინია მანქანების? და რატომ არ უნდა გვეშინოდეს მათი?

როგორც ადამიანები, მიდრეკილნი ვართ „მოაზროვნე მანქანებს“ მივანიჭოთ გარკვეულწილად ანტროპომეტრული თვისებები, რომლებიც დამახასიათებელია ცოცხალი ორგანიზმებისათვის, და საბოლოოდ გავაიგივოთ ისინი ცხოვრების ახალ ფორმასთან — რომელიც მიჩნეულია როგორც სხვასთან შედარებით აღმატებული — რომელიც საფრთხეს უქმნის კაცობრიობას. ფილოსოფიაში, ეს ფენომენი პირველად აღწერა იაპონელმა ფილოსოფოსმა — *მასაჰირო მორიმ,* რომელმაც გამოიყენა *ზებუნებრივი ველის* ცნება 1970-იან წლებში. მისი აზრით, როდესაც რობოტები უფრო მეტად დაემსგავსებიან ადამიანებს, ჩვენი სიმპათია მათ მიმართ გაიზრდება, მაგრამ გარკვეულ ზღვრამდე, ანუ როგორც კი მეტისმეტად ადამიანის მსგავსები გახდებიან, ჩვენ უცბად მივიჩნევთ მათ როგორც ექსცენტრიულს, საშიშსა და საფრთხის მომცველს[1].

ფესვები ამ პესიმისტური აზროვნებისა, რომელიც გამოყოფს იმ ხელოვნური არსების პირვანდელ სახეს, რომელიც იღვიძებს დამოუკიდებელ ცნობიერებაში და ანადგურებს მის შემქმნელს, შეიძლება მოძიებულ იქნეს მე-20 საუკუნის ადრეული პერიოდის ლიტერატურასა და ფოლკლორში (როგორიცაა ფრანკენშტეინის ამბავი). უფრო მეტიც, ადამიანსა და ხელოვნურ არსებებს შორის კონფლიქტმა არამხოლოდ მხატვრული ლიტერატურის დონეზე იჩინა თავი, არამედ ინდუსტრიული რევოლუციის დროსაც — შიშმა მანქანების მიმართ, „რომლებიც წაართმევდნენ ადამიანებს სამუშაოს“, ბიძგი მისცა ლუდიტების მოძრაობის დაწყებას 1810-იან წლებში[2].

უახლესი პესიმისტური ან უფრო მეტიც, *მშფოთვარე* თეორიები დასაწყისშივე ეფუძნება „ტექნოლოგიური განსაკუთრებულობის“ პრობლემას, რომელიც *რაი კურცველის* აზრით, წარმოადგენს მომავალ ეპოქას, *„რომელშიც ისეთი სწრაფი და საფუძვლიანი ტექნოლოგიური ცვლილება ხორციელდება, რომ იგი იწვევს ადამიანის ისტორიის სტრუქტურის რღვევას“. კარცუელის აზრით,* სუპერ ადამიანური ინტელექტის წარმოშობას, მისი განსაკუთრებულობის შედეგად, შეეძლო არსებობიდან ადამიანის მარტივად განდევნა[3].

სტიუარტ რასელის და *პიტერ ნორვიგის* ნაშრომში წარმოდგენილი განსხვავებული, უფრო ოპტომისტური თეორიების მიხედვით, რომლებიც აანალიზებენ და აჯამებენ AI-

[1] Masahiro M., The Uncanny Valley, In: IEEE Robotics and Automation, Vol. 19, 2012, 2.

[2] *Barthelmess U., Furbach U.,* Do We Need Asimov's Laws? In: Lecture Notes in Informatics. Bonn, Gesellschaft für Informatik, 2014, 5.

[3] *Kurzweil R.,* A szingularitás küszöbén, 2014, in: *Marosán G.,* Mi vár ránk a szingularitáson túl? Népszava, 2019, 12, 15.

ის ფენომენს (როგორიცაა *ჟ. გუდის* ან *მორავცის* დოგმები), ხელოვნური ინტელექტის ხედვა, რომელიც იმონებს ადამიანს, წარმოიშობა სუპერადამიანის ან ზებუნებრივის მიმართ პირველყოფილი, ფუნდამენტური შიშისგან, ადრეულ დროში არსებული მოჩვენებებისადმი და გრძნეულებისადმი შიშის მსგავსად. ოპტიმისტები ამტკიცებენ, თუ ხელოვნური ინტელექტისთვის შესაფერისი დიზაინია შექმნილი, ანუ როგორიცაა აგენტები, რომლებიც ასრულებენ საკუთარი ბატონების მიზნებს, მაშინ ხელოვნური ინტელექტი, რომელიც ახლანდელი დიზაინის თანდათანობითი პროგრესის შედეგია, უფრო მეტად მოემსახურება მას, ვიდრე დაიმონებს.“[4]

„ნავიგაციონისტური“ მსოფლმხედველობის თანახმად, ამ ორი კონცეფციის გაერთიანება, ინტელექტის აფეთქების წარმოშობა სინგულარობის პარალელურად შეუძლებელია, მაგრამ საბოლოოდ, კაცობრიობას უდიდესი როლი და პასუხისმგებლობა ექნება მის განვითარებაში. აქედან გამომდინარე, მომავლის უმთავრესი გამოწვევა იქნება მანქანური ინტელექტის ბრძნული ნავიგაცია შესაფერისი მიმართულებით, რომელიც გასცდება გამოთვლისა და პრობლემის გადაჭრის ადამიანურ შესაძლებლობებს. ნავიგატორების შეხედულება ადამიანის პასუხისმგებლობასა და ობიექტურ რეალობაზე ითვალისწინებს ხელოვნური ინტელექტის (AI) მოწიფულობას და პასუხისმგებლიანი მშობლისა და მასწავლებლის იმიჯს. ადამიანური პასუხისმგებლობის მნიშვნელობა, რომელიც ყოველი ტექნოლოგიური განვითარების უკან დგას, არ უნდა იყოს გაზვიადებული ამ თემის სამართლებრივი ასპექტიდან დამუშავების თვალსაზრისით. ბრძნული ნავიგაცია და განვითარება ყველაზე კარგად ჩანს ინტელექტუალური პროგრამული უზრუნველყოფის მონაცემებით-მართულ სწავლებასთან მიმართებით[5].

3. ხელოვნური ინტელექტი ხელოვნური ცნობიერების წინააღმდეგ

არ არის აუცილებელი, რომ ტექნოლოგიური სინგულარობის წარმოშობა, რომელიც თან ახლავს გამოთვლითი შესაძლებლობების აქსელერაციას (არა აქვს მნიშვნელობა რა ფორმით მოხდება ეს), ასახავდეს „მოაზროვნე მანქანას“, რომელიც საბოლოოდ განაცხადებს რომ ევოლუციის თვალსაზრისით მან ჩაანაცვლა თავისი შემქმნელი ადამიანი.

პირველ რიგში, ჩვენ, ადამიანები ვანიჭებთ მნიშვნელობას მანქანის მიერ განხორციელებული გამოთვლების შედეგებს, ჩვენ მასში ვხედავთ ერთგვარ ინტელექტს,

[4] *Russell St. J., Norvig P.,* Mesterséges Intelligencia – Modern megközelítésben, Budapest, Panem, 2000, Ch. 26.
[5] *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: *A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről*, Török *Bernát T., Ződi Zsolt Z. (szerk.),* 2021, 189, 190.

რომელიც სავარაუდო მნიშვნელობის კომპლექსურობისა და ავთენტურობის გამო ცნობიერებად არის მიიჩნეული.

ამჟამად გავრცელებული სამეცნიერო პოზიციის მიხედვით, აბსტრაქტული მანქანის აზროვნების წინაპირობას ხელოვნური ინტელექტი კი არ წარმოადგენს, არამედ *ხელოვნური ცნობიერება* (AC), რომელსაც მაინც არ შეუძლია არსებობა თვით-იდენტურობისა და თვით-ანალიზის უნარის მქონე აგენტის გარეშე. ყველაფერი ეს მოითხოვს შინაგანი მდგომარეობის მუდმივ განსაზღვრას და მის შედარებას მიმდინარე გარეგან მდგომარეობასთან. ათასობით წლის წინ პლატონმა განაცხადა, რომ ის, რასაც ჩვენ აზროვნებას ვუწოდებთ, არაფერია თუ არა სულის ჩუმი საუბარი საკუთარ თავთან[6].

ცნობიერების საფუძველს წარმოადგენს თვით-ცნობიერების (ან თვით-აზროვნების) არსებობა, რაც გულისხმობს საკუთარი თავის ასახვას, გამოცალკევებას ან გაუცხოებას გარემოსგან და ამის შედეგად საკუთარ თავისადმი მიდგომის და თავზე წარმოდგენის შექმნას. თვითშეგნების ევოლუცია და განვითარება, ასევე საკუთარი თავის გარემოსგან გამოყოფა ნელი პროცესია.

მაგალითად, ჩვილ ბავშვს არ აქვს ჩამოყალიბებული თვით-აზროვნება. *ჟაკ ლაკანი*, ფრანგი ფსიქო-ანალიტიკოსი, სარკის სტადიას უკავშირებს ჩვილების რეაქციას, რომელსაც ისინი გამოხატავენ საკუთარი თავის ამოცნობისას, როცა სარკეში არეკლილი საკუთარი იმიჯის წინ დგანან. *ლაკანის* აზრით, ეს „აჰა გამოცდილება“ და მოვლენების თანამიმდევრობა, რომელსაც მივყავართ თვით-ცნობიერების გამოვლენამდე, შეიძლება მოხდეს ჩვილებში ექვსი თვის ასაკიდან[7].

ამის საპირწონედ, ინტელექტი ნიშნავს პრობლემების სწრაფად და ეფექტიანად გადაჭრის უნარს ინფორმაციის აღქმისა და დამუშავების საშუალებით და მიღებული ცოდნის დაგროვებას შემდგომში გამოსაყენებლად. მაშინ, როცა ინტელექტის მოდელირებისას პროგრამული უზრუნველყოფა ადამიანზე უფრო ეფექტიანი და სწრაფია, მას მაინც არ შესწევს უნარი, დაინახოს საკუთარი თავი როგორც პირი, რომელიც გამოყოფილი და გაუცხოვებულია გარემოსგან (და არა მხოლოდ იმიტომ, რომ მას არ უჭირავს ხელში სარკე).

თუ დავესესხებით *ლაზლო ზ. კარვალიცის* მიერ გამოყენებულ ტერმინს, მანქანის შიგნით ხდება მხოლოდ „კოდით მანიპულაცია“ და არა ინფორმაციის დამუშავება. მანქანა ასრულებს ოპერაციებს მისი პროგრამული უზრუნველყოფის შესაბამისი სიგნალით, მაგრამ თვით ოპერირების მხრივ არა აქვს „მეტა დონე“. ეს შეიძლება შევადაროთ პროცესს, როცა ვინმე სწავლობს მიმატებას, გამოკლებას, გამრავლებას და გაყოფას, მაგრამ არ იცის რატომ, როდის ან რა მიზნით არის საჭირო ეს. ცნობიერების

[6] *Szathmáry Z., Barna M.,* Büntetőjogi kérdések az információk korában (mesterséges intelligencia, big data, profilozás), Budapest, HVG Orac, 2018, 44.

[7] *Lacan J.,* A tükör-stádium mint az én funkciójának kialakítója, ahogyan ezt a pszichoanalitikus tapasztalat feltárja a számunkra, Thalassa, Vol. 4, 1993, 2.

დონეზე პროგრამას არა აქვს მიზანი, სურვილი, მითითებები, რისთვისაც მას მოუწევდა შეექმნა ახალი ცნებები (მნიშვნელობები) გარემოსთან და ადრე უკვე შექმნილ ცნებებთან დაკავშირებით და შემდგომ ამის საფუძველზე მიეღო გადაწყვეტილებები[8].

ალვა ნოე, კარგად ცნობილი მეცნიერი საინფორმაციო მეცნიერების სფეროში, გამოიყენებს რა სისტემურ მიდგომას, ხელოვნურ ინტელექტს (AI) უწოდებს *ფსევდო-ინტელექტს,* რათა ხაზი გაუსვას განსხვავებას ცოცხალ ორგანიზმებსა და ხელოვნურ ინტელექტს შორის: „ცალკეულ უჯრედს გააჩნია თავისი ცხოვრებისეული ისტორია; იგი, გარემოს, რომლის გარემოცვაშიც აღმოჩნდება და რომლის ორგანიზებასაც ახდენს, გადააქცევს ღირებულ ადგილად. იგი ეძებს საზრდოს. იგი ქმნის საკუთარ თავს და საკუთარი თავის შექმნით ნერგავს აზრს, ცნებას სამყაროში. მანქანისგან განსხვავებით, ამებას გააჩნია ინფორმაცია [საკუთარ თავზე], იგი აგროვებს და ამუშავებს მას“[9].

პრობლემის გადაჭრის უნარის, რომელიც მოცემულ შემთხვევაში ბრწყინვალედ არის მოდელირებული ხელოვნური ინტელექტით, გაერთიანება ადამიანის თვით-ამსახველ ცნობიერებასთან, შედეგად გვაძლევს თვით-წინააღმდეგობრივ დისკურსს, რომლის არსსაც ვერ ჩასწვდება ვერც „განგანშის ამტეხი“ პირი, რომელიც დარწმუნებულია სინგულარობის საფრთხის შემცველ გამოვლენაში და ვერც მეორე პირი, რომელიც უარყოფს სინგულარობას.

სხვათა შორის, ზოგიერთი „განგაშის ამტეხი“ ავტორები ასევე აღნიშნავენ, რომ ინტელექტუალური მანქანები უნდა იყვნენ შექმნილნი როგორც ადამიანთა საზოგადოებისადმი „მეგობრულად“ განწყობილი ორგანიზმები, რათა თავი ავარიდოთ მტრული ხელოვნური ინტელექტის წარმოშობას და ამ მიზნით, ისინი მოითხოვენ ეთიკური პრინციპების პროგრამებში ჩართვას[10]. თუმცა, ასევე უნდა აღინიშნოს, რომ ამ შემთხვევებშიც კი შეუძლებელია პროგრამების მიერ მეგობრობის თუ თანაგრძნობის აბსტრაქტული ცნებების ნამდვილი მნიშვნელობისა და ამ მნიშვნელობების შინაარსის გაცნობიერება, მაგრამ კონკრეტული ამოცანების ფარგლებში, მათ მიერ გაკეთებული გამოთვლების შედეგებს ადამიანი — დამკვირვებელი აღიქვამდა, როგორც მეგობრულს და ადამიანის განვითარების მხარდამჭერს[11].

საბოლოოდ: (თვით-)ცნობიერება და ინტელექტი წარმოადგენენ განსხვავებულ ცნებებს, მაგრამ მაინც, ჩვენი მიზანია გავაერთიანოთ ისინი ხელოვნურ ინტელექტთან (AI) მიმართებით არსებულ საზოგადოებრივ დისკურსში.

---

[8] *Karvalics L. Z.,* Mesterséges intelligencia – a diskurzusok újratervezésének kora, Információs Társadalom, Vol. 15, 2015, 13.

[9] ციტ.: იქვე, 14.

[10] *Goertzel B., Pitt J.,* Nine Ways to Bias Open-Source AGI Toward Friendliness, Journal of Evolution and Technology, Vol. 22, 2011, Quoted by: *Pokol B.,* A mesterséges intelligencia társadalma, 2018, 55-56.

[11] *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 191.

თუმცა როგორ არის დაკავშირებული ხელოვნური ინტელექტის ფენომენი პერსონალურ მონაცემთა დამუშავებასთან? ნაშრომის შემდეგ ნაწილებში შევეცდებით ნათელი მოვფინოთ ამ საკითხს.

4. ხელოვნური ინტელექტისა და პერსონალურ მონაცემებს შორის ურთიერთდამოკიდებულება

დღესდღეობით, სისტემები, ხელოვნურ ინტელექტზე დაფუძნებული პროგრამული უზრუნველყოფა და საშუალებები, რომლებიც ყოველდღიურად გამოიყენება, გვთავაზობენ საკითხის გადაჭრის ახალ გზებს, რომლებიც უმეტეს შემთხვევაში, მომხმარებლის პერსონალურ მონაცემთა დამუშავების თანმხლებია. სახლის რობოტები, რომლებსაც მომხმარებლები იყენებენ ან ჭკვიანი სატელეფონო აპლიკაციები, რომლებიც აანალიზებენ ადამიანთა ქცევას, გამუდმებით აკონტროლებენ მომხმარებელთა ქცევებსა და რეაქციებს, რათა მათი მოთხოვნის შესაბამისად, რაც შეიძლება სრულყოფილი მომსახურება გაუწიონ მათ. შემთხვევითი არ არის, რომ იმ საშუალებებსა და სერვისებში, რომლებიც იყენებენ ამოცანების თანამედროვე ტექნოლოგიური გადაწყვეტის გზებს, ყველა ვირტუალურ შემთხვევაში მნიშვნელოვანი საკვანძო სიტყვა არის პერსონალიზაცია. თუმცა პერსონალიზების გარდა მზარდი მოთხოვნაა იმ ტექნოლოგიებისადმი, რომლებიც წინასწარმეტყველებენ მომხმარებლის საჭიროებებს. ეს გულისხმობს უფრო რთული გადაწყვეტილების მიმღებ მექანიზმებს, რისი მიღწევაც შესაძლებელია ხელოვნურ ინტელექტზე დაფუძნებული თვითსწავლების სისტემის საშუალებით[12].

ზემოხსენებულ საკითხზე ნორვეგიის პერსონალურ მონაცემთა დაცვის ორგანოს (“Datatilsynet”) მოხსენებაში ხელოვნური ინტელექტი (AI) აღწერილია როგორც სისტემა, რომელსაც შეუძლია სწავლა საკუთარი გამოცდილების საფუძველზე და რთული პრობლემების გადასაჭრელად იმ ცოდნის გამოყენება, რომელიც მან სხვადასხვა სიტუაციებში შეიძინა. ამ კონცეფციის არსი მდგომარეობს იმაში, რომ ხელოვნური ინტელექტი სწავლობს მის მიერ „დანახული“ პერსონალური მონაცემების საშუალებით (პრაქტიკულად, მონაცემები, რომლებიც მითითებულია მასში) და ამის საფუძველზე იღებს გადაწყვეტილებებს ან პროგნოზებს[13].

ხშირად, ხელოვნური ინტელექტი და მანქანური სწავლება სინონიმებად მოიხსენებიან, თუმცა ამ ორ ფენომენში სხვადასხვა ცნება იგულისხმება. ხელოვნური

[12] იქვე, 193.

[13] *Datatilsynet,* Artificial Intelligence and Privacy, Report, 2018, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].

ინტელექტი (AI) არის კრებითი ტერმინი, რომელიც აერთიანებს პროგრამის მიერ ავტომატური გადაწყვეტილებების მიღების დროს განხორციელებულ ყველა პროცედურას. ამისგან განსხვავებით, მანქანურ სწავლებას უფრო ვიწრო გაგება აქვს და დაკავშირებულია ხელოვნური ინტელექტის განვითარების რომელიმე დარგთან. მისი არსი მდგომარეობს იმაში, რომ სისტემა გამოცდილების საფუძველზე ქმნის დამოუკიდებელ ცოდნას. ამ სისტემას დამოუკიდებლად ან ადამიანის დახმარებით შეუძლია რეგულაციებისა და წესების გამოცნობა და იდენტიფიცირება მაგალითებისა და მონაცემთა ბაზებში მოძიებული ნიმუშების საფუძველზე, ხოლო შემდეგ გადაწყვეტილების მიღება იმ კანონზომიერებაზე დაყრდნობით, რომელსაც აღმოაჩენს მიღებული ცოდნის ბაზაში[14].

5. როგორ ვასწავლოთ მანქანებს მონაცემები?

მონაცემთა დაცვის ანალიზის თვალსაზრისით, ხელოვნური ინტელექტის ფუნქციონირების ერთ-ერთ ყველაზე მნიშვნელოვან სფეროს წარმოადგენს მანქანური სწავლების ფენომენი, რომლის თანახმად, პროგრამა „სწავლობს“ მასში ატვირთული მონაცემების საფუძველზე და იღებს სხვადასხვაგვარ გადაწყვეტილებებს. ყველაზე ხშირად ბაზარზე ჩანს, რომ გამოყენებულ ტექნოლოგიას პრაქტიკულად შესწევს უნარი, წინასწარ განსაზღვროს იმ ადამიანის საჭიროებები, რომელიც მას გამოიყენებს.

მანქანური სწავლების პროცესში, ხელოვნური ინტელექტის მიერ განხორციელებული მონაცემების დამუშავება შეიძლება სამ ეტაპად დაიყოს, ესენია:[15]

ა) პირველი, დიდი რაოდენობით სატესტო მონაცემები შეყავთ სისტემაში და ალგორითმი ცდილობს მოდელებისა და მსგავსებების პოვნას ამ ტესტების ნაკრებში. თუ ალგორითმი იპოვის ასეთ იდენტიციფირებად მოდელებს, იგი აღნიშნავს და გადაარჩენს მათ შემდგომი გამოყენებისგან. ამგვარი ნიმუშების საფუძველზე, მოდელის დახმარებით სისტემას შეუძლია შემდგომში მოახდინოს ე. წ. *მოდელის* შექმნა. მაშინ, სისტემას შესწევს უნარი დაამუშაოს რეალური მონაცემები, რომელსაც იგი „ხედავს“ (პრაქტიკულად, მასში ატვირთული მონაცემები) უკვე იდენტიფიცირებული ნიმუშების საფუძველზე.

ბ) შემდეგ, ახალი, „მოქმედი“ მონაცემები, რომლებიც სწავლისთვის გამოყენებული მონაცემების მსგავსია, აიტვირთება სისტემაში. ადრე შექმნილი მოდელის საფუძველზე

[14]*Szepesvári C.*, Gépi tanulás – rövid bevezetés, 2005, 22, <http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf> [28.11.2022].
[15]*Datatilsynet,* Artificial Intelligence and Privacy, Report, 2018, 7, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].

ხელოვნური ინტელექტი (AI) გადაწყვეტს, მის მიერ შესწავლილი მოდელებიდან თუ რომელი ჰგავს ახალ მონაცემს ყველაზე მეტად.

გ) და ბოლოს, სისტემა შეგვატყობინებს გადაწყვეტილებას, რომელიც მასში შეტანილ ახალ მონაცემებთან დაკავშირებით შესწავლილი მოდელის საფუძველზე მიიღო.

ასევე მნიშვნელოვანია აღინიშნოს, რომ არ არის აუცილებელი, მოდელი, რომელიც შექმნილია მანქანური სწავლების პროცესში, შეიცავდეს საწყის მონაცემებს, რომლებიც საფუძვლად ედო მის შესწავლას[16].

6. ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) შესაბამისი ტერმინები

სისტემები, რომლებსაც საფუძვლად მანქანური სწავლება უდევს, უფრო და უფრო ხშირად გამოიყენებიან პერსონალურ მონაცემებთან დაკავშირებული გადაწყვეტილებების მისაღებად. ინტერნეტში განთავსებული პერსონალიზებული რეკლამები და სხვა შინაარსობრივი მასალა (კონტენტი) კარგ მაგალითებს წარმოადგენენ იმის საჩვენებლად, თუ როგორ ფუნქციონირებენ ალგორითმები, რომლებიც აანალიზებენ და შეისწავლიან ადამიანთა ქცევებს და ასევე, თუ როგორ გამოიყენება ჩვენი პერსონალური მონაცემები უფრო მეტად პერსონალიზებული, გამიზნული მასალის საჩვენებლად. ცნება „ავტომატური გადაწყვეტილების მიღება“ მჭიდროდ არის დაკავშირებული პროფილირებასთან, რადგანაც მიღებული გადაწყვეტილებების პარალელურად, ალგორითმის მიერ მოცემული პიროვნების უფრო მეტად უნიკალური პროფილი იქმნება.

მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) არ განსაზღვრავს იმას, თუ რა იგულისხმება ხელოვნური ინტელექტს ან მანქანურ სწავლებაში. მიუხედავად იმისა, რომ რეგულაციაში რამდენჯერმეა ნახსენები ავტომატური გადაწყვეტილების მიღება, იგი მაინც არ გვაძლევს ამ ტერმინის ზუსტ განმარტებას.

29-ე მუხლის საფუძველზე მოქმედი მონაცემთა დაცვის სამუშაო ჯგუფის (“WP 29”), რომელიც შეიძლება მიჩნეულ იქნას ევროპული მონაცემთა დაცვის საბჭოს წინამორბედად, შესაბამისი რეკომენდაციის მიხედვით, ავტომატური გადაწყვეტილების მიღება ნიშნავს ტექნოლოგიური საშუალებებით ადამიანის ჩარევის გარეშე გადაწყვეტილების მიღების უნარს[17]. სხვა სიტყვებით რომ ითქვას, ექსკლუზიურად

[16] იქვე, 10.

[17] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 8, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

ავტომატური გადაწყვეტილების მიღებაში ადამიანი არ მონაწილეობს. ეს ნიშნავს, რომ გადაწყვეტილებას, რომელიც მიღებულია მანქანის მიერ, ანუ მხოლოდ ავტომატურად, უმეტეს შემთხვევაში წინ უნდა უძღოდეს მონაცემთა ავტომატური დამუშავება, რაც, უმეტეს შემთხვევაში, ხდება მანქანური სწავლების პროცესში სისტემის მიერ მოპოვებული და იდენტიფიცირებული მოდელების საფუძველზე[18].

მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) კიდევ ერთი ძირითადი ელემენტია პროფილირების ცნება, რომელიც, განსხვავებით ავტომატური გადაწყვეტილების მიღებისა, უკვე განსაზღვრულია რეგულაციის მე-4(4) მუხლით. კონცეფციიდან გამომდინარე, პროფილირების მიზანს წარმოადგენს ფიზიკური პირის პერსონალური მახასიათებლების შეფასება. ზოგადად შეიძლება ითქვას, რომ პროფილირება ნიშნავს ფიზიკურ პირზე (ან ფიზიკური პირთა ჯგუფზე) ინფორმაციის შეგროვებას და მათი მახასიათებლების ან ქცევითი ნიმუშების შეფასებას, რათა მოხდეს მათი კლასიფიცირება გარკვეულ კატეგორიებად და ჯგუფებად. კლასიფიკაციის მიზანს კი წარმოადგენს მონაცემთა სუბიექტის ინტერესების, მოსალოდნელი ქცევის ან კონკრეტული შესაძლებლობების ანალიზი[19]. პიროვნების პროფილის საფუძველზე შემდგომში შესაძლებელი იქნება პერსონალიზებული მესიჯებისა და სერვისების მონაცემთა სუბიექტისათვის გაგზავნა.

მნიშვნელოვანია აღინიშნოს, რომ ავტომატური გადაწყვეტილების მიღებისა და პროფილირების კონცეფციები არაა სრულიად იდენტური. ავტომატური გადაწყვეტილების მიღების პროცედურა არ კვალიფიცირდება, როგორც პროფილირება და პროფილირება შეიძლება, განხორციელდეს ავტომატური გადაწყვეტილების მიღების მექანიზმების ჩართვის გარეშე. თუმცა, უმეტეს შემთხვევებში, ეს ორი ცნება ერთმანეთს ავსებს, ასე რომ, მათი ერთად განხილვა გამართლებულია მონაცემთა დაცვის თვალსაზრისით.

7. ავტომატური გადაწყვეტილების მიღებისა და პროფილირების რეგულირება ევროკავშირის მონაცემთა დაცვის ზოგად რეგულაციაში (GDPR)

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის 22-ე მუხლი მოიცავს ზოგად მოთხოვნებს ავტომატური გადაწყვეტილების მიღების ფენომენისა და მასთან მჭიდროდ დაკავშირებულ პროფილირებასთან მიმართებით. აღნიშნული მუხლის (I) პარაგრაფის

[18] *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 199-200.

[19] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 8, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

შესაბამისად, მონაცემთა სუბიექტს უფლება აქვს, *არ დაექვემდებაროს მხოლოდ* ავტომატურად მიღებულ იმ გადაწყვეტილებას, პროფილირების ჩათვლით, რომლებსაც აქვთ *იურიდიული ძალა ან მსგავსი მნიშვნელობის ზემოქმედების ძალა* სუბიექტთან მიმართებით. მიუხედავად რეგულაციის ამგვარი ფორმულირებისა, ეს დებულება, ფაქტობრივად, მონაცემთა სუბიექტისთვის გარანტირებულ უფლებას კი არ წარმოადგენს, არამედ იგი არის ზოგადი აკრძალვა დამმუშავებლის მიმართ, რომელიც დაუშვებლად ცნობს გადაწყვეტილების მიღების პროცესის გამოყენებას მხოლოდ ავტომატური დამუშავების საფუძველზე. ეს აკრძალვა მოქმედებს მიუხედავად იმისა, მიიღებს თუ არა მონაცემთა სუბიექტი ზომებს საკუთარი პირადი მონაცემების დამუშავებასთან დაკავშირებით. ამრიგად, როგორც მთავარი წესი, რეგულაცია (GDPR) ზოგადად კრძალავს ისეთი ინდივიდუალური გადაწყვეტილების მხოლოდ ავტომატურად მიღებას, რომელიც იძლევა სამართლებრივ ან მსგავსი მნიშვნელობის შედეგებს.[20]

უფრო მეტიც, წესები, რომლებიც მოქმედებენ ექსკლუზიურად ავტომატური გადაწყვეტილების მიღებასთან მიმართებით, უნდა გამოიყენებოდნენ მხოლოდ იმ შემთხვევებში, როცა გადაწყვეტილებას აქვს იურიდიული ან მსგავსი მნიშვნელობის ზემოქმედების ძალა მონაცემთა სუბიექტზე, რომელიც წარმოადგენს ფიზიკურ პირს. მონაცემთა დაცვის რეგულაცია არ განსაზღვრავს ცნებებს — „იურიდიული ძალა“ ან „ანალოგიური ძალის მქონე“, თუმცა რეგულაციის ფორმულირებებით ნათელია, რომ 22-ე მუხლი ვრცელდება მხოლოდ იმ შემთხვევებზე, რომლებსაც მძიმე შედეგები აქვთ.[21]

იურიდიული ძალა გულისხმობს, რომ ავტომატური გადაწყვეტილება ზეგავლენას ახდენს პიროვნების კანონიერ უფლებებზე. ასევე შეიძლება, გავლენა ჰქონდეს პიროვნებისათვის ხელშეკრულებით მინიჭებულ იურიდიულ მდგომარეობაზე ან მის უფლებებზე. “WP29”-ს მიხედვით, ასეთი იურიდიული ძალის მაგალითებია ფიზიკურ პირებთან დაკავშირებით იმგვარი ავტომატური გადაწყვეტილებები, რომელთა შედეგად შეწყდა ხელშეკრულებები, ასევე, როცა უარი ეთქვათ ან მიენიჭათ კანონით გარანტირებული სოციალური უზრუნველყოფის შეღავათები (როგორიცაა ბავშვებთან დაკავშირებული შეღავათები ან საცხოვრებლით უზრუნველყოფა), აგრეთვე უარი ეთქვათ ქვეყანაში შესვლაზე ან მოქალაქეობაზე.[22]

კანონით ან ხელშეკრულებით განსაზღვრულ უფლებებზე ავტომატური გადაწყვეტილებების ზეგავლენა შეეხება იმ შემთხვევებს, რომელთა შედარებით დეტალური ახსნა შესაძლებელია. თუმცა, ამასთან ერთად, ცნების — „ანალოგიური

[20] *Veale M., Edwards L.,* Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision Making and Profiling. Computer, Law and Security Review, Vol. 34, 2018, 2, 400.
[21] იქვე, 401.
[22] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 22, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

იურიდიული ძალის მქონე“, უფრო ბუნდოვან ფორმულირებას გამოხატავს ზოგადი რეგულაციის 22-ე მუხლი, რომლითაც ასევე დადგენილია აკრძალვის საფუძვლები.

ზოგადი რეგულაციის (GDPR) პრეამბულის 71-ე პუნქტი (დეკლარაციული ნაწილი) მოიცავს რეკომენდაციას აღნიშნულ ცნებასთან დაკავშირებით, რადგანაც მასში ჩამოთვლილია შემდეგი მაგალითები: „უარი კრედიტის ონლაინ გამოყენებაზე“ ან „თანამშრომელთა შერჩევის (რეკრუტირება) ონლაინ პრაქტიკა ადამიანის მონაწილეობის გარეშე“.

ძნელია ზუსტად დადგინდეს ზღვარი, რომელიც მიჩნეული იქნება როგორც *საკმარისად მნიშვნელოვანი.* თუმცა “WP29”-ის მიხედვით, შემდეგი გადაწყვეტილებები მიეკუთვნება ამ კატეგორიას: გადაწყვეტილებები, რომლებიც გავლენას ახდენენ ინდივიდის ფინანსურ მდგომარეობაზე, როგორიცაა კრედიტის მიღების უფლება; გადაწყვეტილებები, რომლებიც გავლენას ახდენენ პიროვნებისათვის ჯანდაცვის სამსახურების ხელმისაწვდომობაზე; გადაწყვეტილებები, რომლებიც ართმევენ ინდივიდებს დასაქმების შესაძლებლობას ან სერიოზული რისკის წინაშე აყენებენ მათ; გადაწყვეტილებები, რომლებიც გავლენას ახდენენ განათლების ხელმისაწვდომობაზე, როგორიცაა უნივერსიტეტში მიღება.[23]

“WP29”-ის შესაბამისად, ავტომატური გადაწყვეტილებები, რომლებიც შეეხება მომხმარებლის ონლაინ პროფილირებიდან გამომდინარე მიზნობრივ რეკლამებს, უმეტეს შემთხვევაში, არ ახდენენ მსგავსი მნიშვნელობის ზეგავლენას ფიზიკურ პირზე (მაგალითად, ტანსაცმლის რეკლამა). თუმცა ამ კატეგორიაშიც კი არსებობს მონაცემთა დამუშავების გარკვეული ოპერაციები, რომლებმაც შეიძლება, მოახდინონ გარკვეული გავლენა საზოგადოებრივ ჯგუფზე, როგორიცაა მოზარდები დაუცველ სიტუაციაში. მაგალითად, თუ პიროვნებას ფინანსური პრობლემები სავარაუდოდ შეექმნა პროფილის საფუძველზე და გამიზნულად, რეგულარულად იღებს რეკლამებს მაღალი პროცენტის სესხებზე, იგი პოტენციურად დამატებით ვალებს დააგროვებს (იმ შემთხვევაში, თუ იგი მიიღებს ასეთ შეთავაზებებს)[24]. 22-ე მუხლის ზოგადი აკრძალვა არ ვრცელდება ასეთ შემთხვევებზე. ძირითადი წესის მიხედვით, პროფილი, რომელიც გენერირებულია ფინანსური პრობლემების მქონე მომხმარებელზე, (მანქანური სწავლების მეშვეობით) არ შეიძლება, გამოყენებული იყოს ისეთ სამიზნედ, რომელიც გამოიწვევს მომხმარებლის დამატებით ფინანსურ რისკს. პროფილერები, რომლებიც აწარმოებენ მონაცემთა დამუშავებას, ვერ დაამტკიცებენ, რომ გადაწყვეტილება სესხის გამოტანასთან დაკავშირებით მიღებული იქნა მათგან დამოუკიდებლად მონაცემთა სუბიექტის მიერ, რადგანაც პროფილირება, რომელიც საფუძვლად უდევს მომხმარებლის გადაწყვეტილებს, არ არის კანონიერი.

[23] იქვე, 23.
[24] იქვე, 24.

როგორც ზემოთ აღვწერეთ, 22(1) მუხლი ითვალისწინებს ექსკლუზიურად იურიდიული ან ანალოგიური მნიშვნელობის ძალის მქონე ავტომატური ინდივიდუალური გადაწყვეტილების ზოგად აკრძალვას. თუმცა არსებობს ამ ზოგადი აკრძალვიდან გამონაკლისები, რომლებსაც განსაზღვრავს 22(2) მუხლი. შესაბამისად, აკრძალვა არ გავრცელდება, თუ გადაწყვეტილება:

1. *აუცილებელია* მონაცემთა სუბიექტსა და დამმუშვებელს შორის ხელშეკრულები დასადებად ან შესასრულებლად;
2. *დასაშვებია/გათვალისწინებულია* ევროკავშირის ან წევრი სახელმწიფოების კანონით, რომელიც ვრცელდება დამმუშავებელზე და რომელიც ადგენს მონაცემთა სუბიექტის უფლებების, თავისუფლებების და კანონიერი ინტერესების დაცვის სათანადო გარანტიებს; ან
3. ეფუძნება მონაცემთა სუბიექტის აშკარად გამოხატულ *თანხმობას.*

პირველი გამონაკლისია ხელშეკრულების შესრულება, რომლის საფუძველზე მონაცემთა დამმუშავებლებს შეუძლიათ, გამოიყენონ ავტომატური გადაწყვეტილების მიღების პროცესები ხელშეკრულებით გათვალისწინებული მიზნებისათვის და ხელშეკრულებიდან გამომდინარე სამართლებრივ ურთიერთობაში. “WP29”-ის მიხედვით, ასეთ შემთხვევაში მონაცემთა დამმუშავებელმა უნდა დაამტკიცოს, რომ ავტომატური გადაწყვეტილების მიღება მონაცემთა დამუშავების ყველაზე შესაფერისი მეთოდია ხელშეკრულებით განსაზღვრული მიზნების მისაღწევად. მეცნიერებისა და ტექნოლოგიის მდგომარეობის, ასევე მათი განხორციელების ხარჯების გათვალისწინებით, თუ ხელშეკრულებაში დასახული ამოცანის შესრულება ეფექტიანად და რისკების პროპორციულად შესაძლებელია სხვა საშუალებებით, მაშინ ავტომატური გადაწყვეტილების მიღება აღარ არის საჭირო და ცალსახად ეწინააღმდეგება კიდეც მონაცემთა დაცვის პრინციპებს.[25]

მეორე გამონაკლისს წარმოადგენს შემთხვევა, როცა ავტომატური გადაწყვეტილების მიღება მოცემულ მონაცემთა დამუშავების პროცესთან დაკავშირებით შესაძლებელია ევროკავშირის ან წევრი სახელმწიფოების კანონმდებლობის შესაბამისად. რელევანტური კანონმდებლობა ასევე უნდა განსაზღვრავდეს შესაფერის ზომებს მონაცემთა სუბიექტის უფლებების, თავისუფლებისა და ლეგიტიმური ინტერესების დასაცავად. მონაცემთა დაცვის ზოგადი რეგულაციის პრეამბულის 71-ე პუნქტის მიხედვით, ასეთი შემთხვევა შეიძლება იყოს, მაგალითად, როცა კანონი სახელმწიფოს ხდის უფლებამოსილს, გამოიყენოს ავტომატური გადაწყვეტილების მიღების

[25] 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 L 119, 4/5/2016, 1–88, Article 25.

მექანიზმები იმისათვის, რომ აიცილოს თაღლითობა და გადასახადებისაგან თავის არიდება.

ბოლოს, მესამე გამონაკლისს წარმოადგენს შემთხვევა, როცა ავტომატური გადაწყვეტილების მიღებას საფუძვლად უდევს მონაცემთა სუბიექტის გამოხატული თანხმობა.[26]

თავად მონაცემთა დაცვის ზოგად რეგულაციაში (GDPR) არ არის განმარტებული ცნება — „გამოხატული თანხმობა“[27], თუმცა, თვითონ ცნება „მონაცემთა სუბიექტის თანხმობა“ მოითხოვს მისი დეკლარაციის ან გამოხატვის აქტის კანონიერებას. გარდა ამისა, ტერმინი „თანხმობის“ განმარტებასთან დაკავშირებით “WP29” გვაძლევს შემდეგნაირ რეკომენდაციას.

ყველაზე თვალსაჩინო მეთოდს გამოხატული თანხმობის უზრუნველსაყოფად წარმოადგენს თანხმობის განმტკიცება წერილობითი განცხადებით. თუმცა ხელმოწერილი განცხადება არ არის ერთადერთი გზა თანხმობის მისაღებად. “WP29”-ის მიხედვით, ციფრულ ან ონლაინ კონტექსტში შესაძლებელია, რომ მონაცემთა სუბიექტმა გასცეს საჭირო განცხადება ელექტრონული ფორმის შევსებით, ელექტრონული ფოსტის გაგზავნით ან სკანირებული დოკუმენტის ატვირთვით, სადაც გამოყენებულია მისი ხელმოწერა ან ელექტრონული ხელმოწერა. დაბოლოს, გამოხატული თანხმობის ვალიდურობა შეიძლება დადასტურდეს თანხმობის ორ-საფეხურიანი დამოწმებით (ორფაქტორიანი აუთენტიფიკაციის გამოყენება).[28]

8. ავტომატური გადაწყვეტილების მიღებისა და პროფილირების გავლენა საზოგადოებაზე ან „კემბრიჯ ანალიტიკას“ საქმე

ერთ-ერთი ყველაზე კარგად ცნობილი საქმე, რომელიც გვაჩვენებს დამოკიდებულებას მონაცემებით მართულ ეკონომიკას, პროფილირებასა და მიზნობრივ რეკლამირებას შორის, საჯაროდ ხელმისაწვდომი 2018 წლის დასაწყისში გახდა, თუმცა მის წინამორბედ შემთხვევებს ადგილი 2010-იანი წლების დასაწყისშიც ჰქონდა: *ალექსანდრე კოგანმა*, კემბრიჯის უნივერსიტეტის ფსიქოლოგიის

[26] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 25, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

[27] მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR), მუხლი 4 (11): მონაცემთა სუბიექტის „თანხმობა“ ნიშნავს მონაცემთა სუბიექტის სურვილის ნებაყოფლობით, კონკრეტულ, ინფორმირებულ, მკაფიო გამოხატულებას, რომელიც გადმოცემულია განცხადებით ან ნათლად და აქტიურად გამოხატული ქმედებით და რომლის საშუალებითაც იგი აცხადებს თანხმობას მასთან დაკავშირებული პერსონალური მონაცემების დამუშავებაზე.

[28] *Article 29 Data Protection Working Party,* Guidance on the Consent according to Regulation (EU) 2016/679 (WP259rev.01.), 2018, 20-22, <http://naih.hu/files/wp259-rev-0_1_HU.PDF> [28.11.2022].

განყოფილების მკვლევარმა, ფეისბუქისთვის აპლიკაცია შექმნა (“Facebook”), რომელსაც „ეს არის თქვენი ციფრული ცხოვრება“ (მოკლედ: “TIYDL”) უწოდა. “TIYDL” წარმოადგენდა პროგრამას, რომელიც გართობის მიზნებისათვის აანალიზებდა პიროვნებას და ქმნიდა მომხმარებლის ფსიქოლოგიურ პროფილს. „ფეისბუქმა“, როგორც რეგისტრაციის დროს წარდგენილი პერსონალური მონაცემების დამმუშავებელმა, გასცა აპლიკაციის კვლევითი მიზნებით მართვის ნებართვა. სხვათაშორის, ნებისმიერს შეუძლია ასეთი აპლიკაციის შექმნა; მომხმარებლის მონაცემებზე წვდომის წესები განსაზღვრულია ფეისბუქის მიერ „ფეისბუქის პლატფორმის პოლიტიკით“ (“Facebook Platform Policy”), რომელიც ძალაშია და გაიცემა აპლიკაციის შემქმნელებზე. თუ აპლიკაცია შეესაბამება წესების გამოყენების პირობებს, იგი გახდება ხელმისაწვდომი სოციალური მედიუმისათვის.[29]

აპლიკაციის გამოყენება ექვემდებარებოდა ინდივიდუალურ მონაცემთა დამუშავებაზე სუბიექტების თანხმობას, რომლებსაც ასევე უნდა სცოდნოდათ მათი მონაცემების გამოყენების მიზანი. დაახლოებით 270, 000 მომხმარებელმა გამოიყენა პროგრამა მოცემული პირობების შესაბამისად.[30] თუმცა შემდგომში აღმოაჩინეს, რომ აპლიკაციისათვის ხელმისაწვდომი იყო არამარტო ის მონაცემები, რომლებსაც სუბიექტი იყენებდა, არამედ მისი მეგობრების მონაცემებიც. ფსიქოლოგიური პროფილი, რომელიც შედგენილი იყო მომხმარებელზე და მის მეგობრებზე, შეიცავდა ინფორმაციას მათი პოლიტიკური ორიენტაციის შესახებ, რომელი საიტის ან მსახიობის მიმდევრები იყვნენ, რა დამოკიდებულება ჰქონდათ რელიგიისადმი და სად იყო მათი ადგილმდებარეობა ე. წ. “OCEAN”[31] მასშტაბით, რაც წარმოადგენს ხუთი მახასიათებლის ინგლისური სახელების აკრონიმს[32].

გარდა ამისა, *კოგანმა* მის მიერ დამუშავებული მონაცემების მთლიანი კრებული მესამე პირებს გადასცა, მათ შორის *კემბრიჯის ანალიტიკასა და ეუნოია ტექნოლოგიას* (“Cambridge Analytica and Eunoia Technologies”). ეს ეწინააღმდეგებოდა ფეისბუქის

[29] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 119-120.

[30] *Németh S.,* A közösségi oldalak szolgáltatóinak jogi felelőssége, PhD értekezés (műhelyvitára benyújtott változat), 2021, 119, <https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf> [28.11.2022].

[31] “OCEAN” მასშტაბის ხუთ-განზომილებიანი მოდელის კომპონენტები: გამოცდილებისადმი გახსნილობა (გამომგონებლური/ცნობისმოყვარე თანამიმდევრული/ფრთხილის წინააღმდეგ) — ცნობიერება (ეფექტიანი/ორგანიზებული ექსტრავაგანტური/დაუდევარის წინააღმდეგ) — ექსტრავერსია (კონტაქტური/ენერგიული განცალკევებული/თავშეკავებულის წინააღმდეგ) — შეთანხმებლობა (მეგობრული/თანამგრძნობი კრიტიკული/გონივრულის წინააღმდეგ) — ნევროტიზმი (მგრძნობიარე/ნერვიული მოქნილი/თავდაჯერებულის წინააღმდეგ), იხ.: <http://medicalonline.hu/cikk/megelozheto_e_az_alzheimer_kor_> [28.11.2022].

[32] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 121.

პლატფორმის პოლიტიკას, რომელიც "TIYDL" შექმნის დროს ძალაში იყო, რადგანაც იგი კრძალავდა მომხმარებლის თანხმობის გარეშე მონაცემის მესამე პირზე გაყიდვას, ასევე „დეველოპერის საკუთარი მიზნებისათვის" მეგობრის მონაცემების გამოყენებას.[33]

ფეისბუქმა შენიშნა, რომ პროგრამა აგროვებდა და ამუშავებდა მომხმარებლების მეგობრების მონაცემებს და რომ 2015 წელს, *კოგანმა* გადასცა მონაცემები მესამე პირებს, სწორედ ამიტომ აპლიკაცია საიტიდან მოხსნა. ამავე დროს მათ შეწყვიტეს ხელშეკრულება *კოგანთან* და მოითხოვეს მისგან და მონაცემთა ტრანსფერის მიმღებებისგან წერილობითი მტკიცებულება მათ მიერ უკანონოდ დამუშავებული პერსონალური მონაცემების სრული კრებულის გაუქმების შესახებ. ბიზნეს ორგანიზაციებმა (ვისაც ეს ეხებოდათ) სავარაუდოდ გადასცეს მოთხოვნილი დოკუმენტი,[34] მაგრამ თვითონ ფეისბუქს არ შეუმოწმებია მათი განადგურების პროცესი.[35]

შემდეგ, დადგა 2018 წლის მარტი, როდესაც პრესაში დაიბეჭდა ფაქტების დამდგენი სტატიები, რომელთა მიხედვით *ქრისტოფერ უაილი* — ყოფილი თანამშრომელი, რომელიც პრესაში განცხადებებს აკეთებდა, ამტკიცებდა, რომ კემბრიჯ ანალიტიკამ კი არ გაანადგურა უკანონოდ დამუშავებული პერსონალური მონაცემები, არამედ მათი გამოყენებით, 2016 წლის აშშ-ის საპრეზიდენტო არჩევნებში საკუთარი პოლიტიკური რეკლამებისთვის მიზანში ამოიღო გარკვეული შთაგონებადი ამომრჩევლების ჯგუფები, წინასწარ შექმნილი მათი ფსიქოლოგიური პროფილის საფუძველზე. ამის შედეგად, მათ წარმატებით მოახერხეს ზეგავლენა მოეხდინათ ამ ამომრჩევლებზე ე. წ. „მერყევ" ("Swing") საარჩევნო ოლქებში *დონალდ ტრამპის* (რესპუბლიკელების საპრეზიდენტო კანდიდატი) მხარდასაჭერად, რომ საყოველთაო არჩევნებში ხმა მისთვის მიეცათ. იმავე წელს, რეკლამების საშუალებით და ფსიქოლოგიური მეთოდების გამოყენებით, კომპანიამ ზეგავლენა მოახდინა ევროკავშირის წევრობასთან დაკავშირებით გაერთიანებული სამეფოს რეფერენდუმზეც („ბრექსიტ რეფერენდუმი"). *უაილის* აზრით, ამ კამპანიების პროცესში კემბრიჯ ანალიტიკამ ფეისბუქის დაახლოებით 87 მილიონი მომხმარებლის მონაცემი დაამუშავა.[36]

ბრიტანეთის ანალიტიკის სკანდალის გამო, დიდი ბრიტანეთის საინფორმაციო კომისრის ოფისმა ("ICO"), გაერთიანებული სამეფოს მონაცემთა დაცვის ორგანომ, მას მაქსიმალური ჯარიმა (GBP 500,000)[37] დააკისრა, რაც განსაზღვრულია მონაცემთა დაცვის

---

[33] Facebook Platform Policy, II. point 4, <https://bit.ly/3rioTYH> [28.11.2022].

[34] *Németh S.,* A közösségi oldalak szolgáltatóinak jogi felelőssége. PhD értekezés (műhelyvitára benyújtott változat), 2021, 119, <https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf> [28.11.2022].

[35] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 123.

[36] იხ.: <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> [28.11.2022].

[37] იხ.: <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf> [20.01.2023].

რეგულაციით, რომელიც ძალაში იყო 2018 წლის 24 ოქტომბერს, ფეისბუქში უფლებების დარღვევის მომენტისთვის.[38] 2019 წლის ივლისში, აშშ-ის ფედერალური ვაჭრობის კომისიის კონკურენციის ბიურომ გამოძიების შედეგად, რომელიც კემბრიჯ ანალიტის საქმის გამო დაიწყო, ფეისბუქს 5 მილიარდი აშშ დოლარის ჯარიმა დააკისრა.[39]

9. „კემბრიჯ ანალიტიკას“ საქმის მოკლე შეფასება ალგორითმის გამჭირვალობის თვალსაზრისით

მონაცემთა დაცვის კანონმდებლობის თვალსაზრისით, ზემოხსენებულ სკანდალთან დაკავშირებით პირველ რიგში საჭიროა მივმართოთ „მიკრო-თარგეთინგის“ (მიზნების დასახვა) კონცეფციას, რომლის არსი მდგომარეობის იმაში, რომ შესაძლებელია კონკრეტული სამიზნე ჯგუფის ან პიროვნების ინტერესების დადგენა მომხმარებლის პროფილის საფუძველზე, რომელიც შექმნილია პიროვნების შესახებ შეგროვებული მონაცემების (მაგალითად, ჩვევების მოძებნა, ნანახი ან მოწონებული მასალა, სოციალური მედიის კომუნიკაციები) გამოყენებით და მათთვის პერსონალური მესიჯის/მასალის გაგზავნა ინტერნეტის საშუალებით.

„მიკრო-თარგეთინგისათვის“ მონაცემთა ანალიზი და პროფილირება თითქმის სრულიად ავტომატურია. ამ პროცესში, მონაცემთა სუბიექტზე მონაცემების შეგროვების საფუძველზე ავტომატური გადაწყვეტილების მიღების ალგორითმი აკონკრეტებს, თუ რა სახის მასალის გაგზავნა და რა სიხშირით არის საჭირო გავლენის მოხდენა მომხმარებლებზე ან პოლიტიკურ გადაწყვეტილებებსა და ჩვევებზე. იმ შემთხვევაში, თუ, მაგალითად, ვინმეს მოსწონს პროდუქციის კონკრეტული ასორტიმენტი, უსმენს კონკრეტული მუსიკალური სტილის შემსრულებლებს ან მიმდევარია იმ საზოგადოებრივ მოღვაწეთა აქტივობებისა, რომლებიც მოძღვრავენ კონკრეტულ პოლიტიკურ იდეოლოგიას, მაშინ ალგორითმი ამგვარ და მსგავს მასალას უჩვენებს მათ მომავალში.[40]

„მიკრო თარგეთინგის“ მეთოდი მჭიდროდაა დაკავშირებული *რიჩარდ ტალერის არჩევანის არქიტექტურისა* და *ბიძგის* (“nudge”) *თეორიასთან*, რაც გულისხმობს არჩევანის წინაშე მდგომი პიროვნების განწყობასა და გარკვეული მიმართულებით

[38] იხ.: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/> [28.11.2022].

[39] იხ.: <https://www.bbc.com/news/world-us-canada-48972327> [28.11.2022].

[40] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.)*, 2021, 122.

წაყვანას არაპირდაპირი მეთოდების მეშვეობით. ტალერის მიხედვით, ბიძგი არ ნიშნავს მანიპულირებას, ეს არის მხოლოდ „მსუბუქი ორიენტირება“.[41]

ზემოხსენებულ ცნებებს განსაკუთრებული მნიშვნელობა ენიჭება კემბრიჯ ანალიტიკის საქმეში, რადგან ფეისბუქზე შედგენილი “TIYDL” მომხმარებლების (და მათი მეგობრების) პერსონალური პროფილები გამოყენებული იყო ზუსტად ასეთი ავტომატური “მიკრო-თარგეთული” პოლიტიკური რეკლამების გასაგზავნად, რათა კონკრეტული გადაწყვეტილებების მისაღებად მონაცემთა სუბიექტების ორიენტირებით არაპირდაპირი ზეგავლენა მოეხდინათ არჩევნების შედეგებზე.

მონაცემთა უკანონო დამუშავების ზუსტი დროის ინტერვალის განსაზღვრა შეუძლებელია ხელმისაწვდომი ინფორმაციის საფუძველზე. თუმცა ცხადია, რომ ეს ხდებოდა 2018 წლის მაისამდე, მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) ძალაში შესვლამდე: პერსონალური მონაცემები დამუშავებული იქნა 2010 და 2015 წლებს შორის პერიოდში, ხოლო ამომრჩევლებზე გამიზნული მასალით ზემოქმედება მოხდა 2016 წელს. თუმცა მონაცემთა დაცვის ზოგადი რეგულაციის მიღებამდე მონაცემთა დამუშავებისთვის აუცილებელი იურიდიული საფუძვლის არსებობის მტკიცებულება, დამუშავების გამჭირვალობის მოთხოვნა და მონაცემთა დამუშავებასთან დაკავშირებით წინასწარი შეტყობინების გაგზავნა აუცილებელი იყო ორივე — უნგრეთის[42] მანამდე მოქმედი მონაცემთა დაცვის რეგულაციისა და საერთაშორისო მონაცემთა დაცვის სტანდარტების მიხედვით. გამჭვირვალობის მოთხოვნა მკაფიოდ არის განსაზღვრული მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 5(1)(ა) მუხლით, რომლის მიხედვით, მონაცემთა სუბიექტთან მიმართებით პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და *გამჭირვალედ*.

მომხმარებლებმა აირჩიეს აპლიკაციის გამოყენება და თანხმობის წინასწარ გაცემა, რათა აპლიკაციასა და მის „ოპერატორს“ წვდომა ჰქონოდათ რეგისტრაციის პროცესში თავად მომხმარებლის მიერ მიწოდებულ პერსონალურ მონაცემებზე. ასე რომ, მომხმარებლის მონაცემთა დამუშავების თვალსაზრისით, აპლიკაციის ფუნქციონირება კანონიერადაც კი შეიძლება იქნეს მიჩნეული. მაგრამ ფაქტი, რომ აპლიკაციის ოპერატორისთვის ასევე ხელმისაწვდომი იყო აპლიკაციის მომხმარებლის გარდა მონაცემთა სუბიექტების სხვა ჯგუფის (მომხმარებლის მეგობრების) პერსონალური მონაცემები, არ შეიძლება იქნეს მიჩნეული კანონიერად. ამის მიზეზია ის, რომ მომხმარებლის მეგობრებს არ მიუციათ თანხმობა მათი მონაცემების ამ მიზნის დამუშავებაზე და მათ საერთოდ არ მიუღიათ ინფორმაცია აღნიშნულის შესახებ.

[41] *Deli G., Kocsis B., Muhari N.,* Akarva-akaratlanul – az adatvédelem és az akaratszabadság dilemmái. In: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 237-238.

[42] Version of Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information, in force prior to the application of GDPR.

ამგვარად, ამ მხრივ დამუშავების გამჭვირვალობა და კანონიერება საფრთხის ქვეშ დადგა. არაკანონიერია ისიც, რომ არც მომხმარებელმა და არც მისმა მეგობრებმა იცოდნენ, რომ მათი მონაცემები მესამე პირისთვის გახდა ცნობილი.

"TIYDL"-ის მომსახურების მიმწოდებლისა და ფეისბუქის წარუმატებლობასთან მიმართებით ხაზი უნდა გაესვას გამჭვირვალობის ნაკლებობას, რაც წლების განმავლობაში სოციალური მედია-ვებგვერდების კრიტიკის საფუძველი იყო: დამუშავების შიდა წესები და ინფორმაციული ტექნოლოგიის სტრუქტურა უბრალოდ არ არის ცნობილი საზოგადოებისათვის და მათთვის, ვისაც აღნიშნული კანონი შეეხებათ, როგორიცაა, მაგალითად, გამიზნული რეკლამების გამანაწილებელი ალგორითმების ოპერირება.[43] თავად პერსონალურ მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) ცდილობს ამ პრობლემის გადაჭრას ავტომატური გადაწყვეტილების მიღებისა და პროფილირების მიმართ გამჭვირვალობისა და ინფორმაციის კონკრეტული მოთხოვნების განსაზღვრით.

შესაბამისად, რეგულაცია დამმუშავებლისგან მოითხოვს ინფორმაციის მიწოდებას იმ გადაწყვეტილების მიღებასთან დაკავშირებით, რომელსაც მხოლოდ ურიდიული ძალის ან ანალოგიური მნიშვნელობის მქონე მონაცემთა ავტომატური დამუშავება უდევს საფუძვლად. რეგულაცია მოიცავს პროფილირებას, რომლის საფუძველია ამ კატეგორიის მონაცემთა დამუშავება[44] და რომლის შესაბამისად, მონაცემთა სუბიექტს უნდა მიეწოდოს შემდეგი სამი სახის ინფორმაცია:

1) მას უნდა ეცნობოს ასეთი მონაცემების დამუშავების ფაქტის შესახებ;
2) მას უნდა მიეწოდოს ინფორმაცია, რომელიც გასაგებად ახსნის გამოყენებულ ლოგიკას;
3) დაბოლოს, იგი უნდა იყოს ინფორმირებული მონაცემთა დამუშავების მნიშვნელობისა და მონაცემთა სუბიექტისათვის მისი მოსალოდნელი შედეგების შესახებ.[45]

ავტომატური ინდივიდუალური გადაწყვეტილების მიღების თაობაზე შეტყობინება შედარებით მარტივი მოთხოვნაა; საკმარისია, დამმუშავებლის მიერ მხოლოდ მონაცემთა დამუშავების თაობაზე ინფორმაციის მიწოდება. მნიშვნელოვანია ისიც, რომ მონაცემთა სუბიექტმა ასევე იცოდეს, ავტომატური ინდივიდუალური გადაწყვეტილებების მიღება გულისხმობს თუ არა პროფილირებას.

გამოყენებული ლოგიკის მიხედვით, ინფორმაციით უზრუნველყოფის ფორმა წამოჭრის რამდენიმე საკითხს. ეს შესაძლოა მნიშვნელოვან გამოწვევას უქმნიდეს

[43] *Klein T., Tóth A. (Eds.),* Technológia jog – Robotjog – Cyberjog, 2018, 50.

[44] 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 L 119, 4/5/2016, 1–88,* მუხლი 15(1)(h).

[45] იქვე, მუხლი 13(2)(f).

დამმუშავებელს ზემოხსენებული მანქანური სწავლების მეთოდების შემთხვევაში, რადგანაც, ხშირად, იგი ეფუძნება კომპლექსურ მონაცემთა დამუშავების პროცესებს, რომელთა განხილვა ძალიან ძნელია.

„მრავლისმეტყველი ინფორმაცია“, მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) შესაბამისად, მონაცემთა დამმუშავებლებმა გამოყენებულ ლოგიკასთან დაკავშირებით უნდა გადმოსცენ გასაგები და მარტივი ენით. თუ მონაცემთა დამმუშავებელი წარადგენს მხოლოდ ზოგად შეტყობინებას, რომ, მაგალითად, იგი ამუშავებს სისტემას ნერვული ქსელის საფუძველზე, იგი საკმარისი არ იქნება, რადგან მონაცემთა სუბიექტს ძალიან მცირე წარმოდგენა შეექმნება იმაზე, თუ რა ელის მის პერსონალურ მონაცემებს დამუშავების პროცესში.[46]

„მრავლისმეტყველი ინფორმაცია“ არ ნიშნავს, რომ დამმუშავებელმა უნდა გასცეს რთული ახსნა-განმარტება გამოყენებული ალგორითმის შესახებ ან სრულად წარადგინოს ალგორითმი. ტექნოლოგიის დეტალური პრეზენტაცია, უმეტეს შემთხვევაში, ართულებს ინფორმაციის გაგებას და ხელს უშლის მის აღქმას.[47] გარდა ამისა, თვითონ რეგულაცია აცხადებს, რომ ინფორმაცია გამოყენებული ლოგიკის შესახებ ზეგავლენას არ ახდენს ბიზნესის საიდუმლოსა ან ინტელექტუალურ საკუთრებაზე, პროგრამული უზრუნველყოფის დაცვის გარანტორი საავტორო უფლების ჩათვლით.[48] ბუნებრივია, ტექნოლოგიის სირთულე არ შეიძლება იყოს ინფორმაციით უზრუნველყოფის თავიდან არიდების გამამართლებელი მიზეზი.

მონაცემთა იმ დამმუშავებლებისაგან, რომლებიც ავტომატური გადაწყვეტილების მიღების საფუძველზე იყენებენ პროფილირებას, მათ შორის, საიტებს „მიკრო-თარგეთინგის“ გამოიყენებით რეკლამების საჩვენებლად, ზოგადი რეგულაციის (GDPR) აღნიშნული დებულებები მოითხოვს ინფორმაციის გამჭვირვალობის უზრუნველყოფას ამ ტიპის დამუშავების თაობაზე. ამ დებულების დაცვა ზოგადი რეგულაციის (GDPR) სამართლებრივი რეჟიმის მთავარ საკვანძო საკითხს წარმოადგენს: კანონმდებელმა აღიარა ის მნიშვნელოვანი ზეგავლენა, რომელსაც აღნიშნული მეთოდი კონფიდენციალურობაზე ახდენს. იმედი უნდა ვიქონიოთ, რომ ეს მოთხოვნები მხოლოდ „საჩვენებელი კანონმდებლობა“ კი არ იქნება, არამედ მონაცემთა დამმუშავებლები ნამდვილად დაიცავენ მათ პროფილირების პროცესში.

ასეთი და ამის მსგავსი სისტემების შემუშავება და ფუნქციონირება არ წარმოადგენს ერთადერთ საკითხს მონაცემთა დაცვისა და დამუშავებისთვის, რომლებიც ასევე აღიარებულია ევროკავშირის კანონმდებლების მიერ. ევროპის კომისიის რეგლამენტის პროექტი, რომელიც გამოქვეყნდა 2021 წლის 21 აპრილს, ასახავს ხელოვნურ ინტელექტზე დაფუძნებული სისტემების რეგულირებას, რომლის მოკლე განხილვა წარმოდგენილია მომდევნო ნაწილში.

[46] *Eszteri D.,* Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat, Magyar Jog, 12, 2019, 679-680.
[47] *Péterfalvi A., Révész B., Buzás P. (ed.),* Magyarázat a GDPR-ról, 2018, 158.
[48] 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 L 119, 4/5/2016, 1–88,* პრეამბულა (63).

10. ხელოვნური ინტელექტის ახალი რეგულაციის პროექტი

ევროპის კომისიის მიერ გამოქვეყნებული რეგულაციის პროექტი, რომელიც მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) მსგავსად პირდაპირი მოქმედების ძალის მქონეა, მოაწესრიგებს ხელოვნური ინტელექტის განვითარებას, როგორც ევროკავშირის ყველა წევრ ქვეყანაში სავალდებულო ძალის მქონე რეგულაცია.

კომისიის პრეს-რელიზის მიხედვით, გამოქვეყნებული პროექტის მიზანია ევროპის გადაქცევა ხელოვნური ინტელექტის სანდო გლობალურ ცენტრად. ხელოვნურ ინტელექტად კლასიფიცირებისათვის პროექტი სამი პირობის ერთდროულად დაკმაყოფილებას მოითხოვს. პირველი, ხელოვნურმა ინტელექტმა უნდა გამოიყენოს კონკრეტული ტექნოლოგია; მეორე, მან დამოუკიდებლად უნდა მიაღწიოს ადამიანის მიერ დასახულ მიზნებს; და ბოლოს, მან უნდა მიიღოს შედეგი, რომელიც „ზეგავლენას“ მოახდენს გარემოზე. *ზოლტ ზოდის* შესაბამისი ნაშრომის მიხედვით, ეს უკანასკნელი ორი კრიტერიუმი წარმოადგენს „ავტონომიის“ ზუსტი განმარტების მცდელობას. იმ სისტემების გარდა, რომლებსაც საფუძვლად მანქანური სწავლება უდევთ, ახალი კოდექსის პროექტი გამიზნულია მის ფარგლებში მყოფ ორ დამატებით ჯგუფზე. ესენია ისთი სისტემები, რომლებსაც საფუძვლად უდევთ ცოდნის ასახვა და სტატისტიკურ სისტემები. *ზოდის* მიხედვით, ეს ხდება იმიტომ, რომ აღნიშნული სისტემები შეიძლება შეიქმნას იმგვარად, რომ მათი კომპლექსურობისა და დამუშავებული მონაცემების რაოდენობის გამო, შედეგები არ იყოს განმსაზღვრელი.[49]

გარდა ამისა, ხელოვნური ინტელექტის კლასიფიკაციისათვის კოდექსი გამოიყენებს რისკზე დაფუძნებულ მიდგომას, რათა სისტემა დაიყოს ოთხ მთავარ კატეგორიად:

ა) პირველი რისკის კატეგორია მოიცავს სისტემებს, რომლებიც კლასიფიცირდება როგორც დაუშვებლად მაღალი რისკის მქონე. ესენია ის ხელოვნური ინტელექტები, რომლებიც ადამიანთა უსაფრთხოებას, საარსებო სახსრებსა და უფლებებს აშკარად უქმნის საფრთხეს. ამაში შედიან, მაგალითად, სისტემები ან აპლიკაციები, რომლებიც მანიპულირებენ ადამიანთა ქცევით იმ განზრახვით, რომ „გვერდი აუარონ მომხმარებელთა თავისუფალ ნებას“ და ასევე სისტემები, რომელთა მეშვეობით შესაძლებელია მთავრობის მიერ „საზოგადოების შეფასება“.[50]

პროფილირებასა და „მიკრო-თარგეთინგზე“ დაფუძნებული მონაცემთა დამუშავება, რომელიც განხორციელდა კემბრიჯ ანალიტიკის მიერ, შეიძლება მიეკუთვნოს პირველ კატეგორიას, რადგანაც მომხმარებლებმა არ იცოდნენ მათი მონაცემების საფუძველზე

[49] *Ződi Z.,* A mesterséges intelligencia jogi fogalma, Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/itkiblog/2021/06/18/a-mesterseges-intelligencia-jogi-fogalma/> [28.11.2022].
[50] *European Commission,* A Digitális korra felkészült Európa: A Bizottság új szabályokat és intézkedéseket javasol a kiválóságra és bizalomra épülő mesterséges intelligencia terén, Sajtóközlemény, 2021, <https://ec.europa.eu/commission/presscorner/detail/hu/IP_21_1682> [28.11.2022].

შექმნილი პროფილების გამოყენებით მათზე პოლიტიკური ზეგავლენის მოხდენის მცდელობების შესახებ. ეს უკანასკნელი, როგორც კატეგორია, რომელიც მოითხოვს აკრძალვას, ინსპირირებული იყო ე. წ. სოციალური კრედიტის სისტემით, რომელიც შეიქმნა და გამოცდილ იქნა ჩინეთის სახალხო რესპუბლიკაში.[51]

ბ) კოდექსის პროექტი მეორე ან მაღალი რისკის მქონე კატეგორიაში აერთიანებს ხელოვნური ინტელექტის იმ ტექნოლოგიებს, რომლებიც გამოიყენებიან სულ ცხრა სფეროში ან/და წარმოადგენს მაღალ რისკს ადამიანთა ზოგიერთი ძირითადი უფლებების მიმართ. ეს სფეროებია:

- კრიტიკული ინფრასტრუქტურა (მაგალითად, ტრანსპორტირება);
- განათლება და პროფესიული ტრენინგი (მაგალითად, გამოცდის შედეგების შეფასება);
- აპარატურა, რომელიც უზრუნველყოფს ზოგიერთი პროდუქტის უსაფრთხოებას (მაგალითად, რობოტოქირურგია);
- დასაქმება და დასაქმებულთა მართვა (მაგალითად, სამსახურში აყვანისათვის ავტობიოგრაფიების (CV) შერჩევა);
- ძირითადი კერძო და საჯარო მომსახურება (მაგალითად, საკრედიტო რანჟირება);
- სამართალდამცავი ორგანოები, სამართალდამცავი ქმედება (მაგალითად, მტკიცებულების სანდოობის შეფასება);
- თავშესაფრის უზრუნველყოფასთან დაკავშირებული საქმეები და საზღვრის კონტროლი (მაგალითად, სამოგზაურო დოკუმენტაციის აუთენტურობის შემოწმება);
- სამართლისა და დემოკრატიული პროცესების ადმინისტრირება (მაგალითად, კანონის გამოყენება საქმის კონკრეტულ ფაქტებთან დაკავშირებით);
- ბოლოს, კოდექსის პროექტის მიხედვით, ყველა დისტანციური ბიომეტრული იდენტიფიკაციის სისტემა კვალიფიცირდება როგორც მაღალი რისკის შემცველი. როგორც მთავარი წესი, კანონის პრაქტიკაში გატარების მიზნით მათი საჯარო ადგილებში და რეალურ დროში გამოყენება იკრძალება. რეგულაციური კონცეფცია ამ აკრძალვიდან გამონაკლისის დაშვების შესაძლებლობას იძლევა მხოლოდ რამდენიმე სერიოზული დანაშაულებრივი ქმედების შემთხვევაში (მაგალითად, დაკარგული ბავშვის პოვნა, ტერორიზმის პირდაპირი საფრთხის ან სერიოზული კრიმინალური ქმედების თავიდან აცილება), ასევე, რომელიც

[51] *Kollár C.,* Kína és a társadalmi kreditrendszere, Hadtudomány, 2, 2020, <https://www.mhtt.eu/hadtudomany/2020/2020_2szam/079-097_Kollar.pdf> [28.11.2022].

ექვემდებარება მოსამართლის ან სხვა დამოუკიდებელი ორგანოს ნებართვასაც კი.[52]

ამ კატეგორიების ხელოვნური ინტელექტის სისტემებმა სამოქალაქო ბრუნვაში გაშვებამდე უნდა შეასრულონ მკაცრი ვალდებულებები. პროექტი მოითხოვს, რომ ჩამოყალიბების ეტაპზევე ყველა ასეთმა სისტემამ გაიაროს შესაბამისი რისკების შეფასებისა და შემცირების პროცესები. მონაცემთა ერთობლიობა, რომლებიც გამოიყენება ხელოვნური ინტელექტის შექმნაში, უნდა იყოს უმაღლესი ხარისხის, ხოლო ყოველი აქტივობა — რეგისტრირებული, რათა უზრუნველყოფილ იქნას შედეგების მიკვლევადობა; გარდა ამისა, ხელმისაწვდომი უნდა იყოს მოთხოვნასთან შესაბამისობის შეფასების დეტალური დოკუმენტაცია. პროექტი ასევე მოითხოვს მომხმარებელთათვის გასაგები და ყოვლისმომცველი ინფორმაციის მიწოდებას ადამიანის ზედამხედველობის საჭიროების შესახებ და ასევე, პრინციპულად მოითხოვს სანდოობის, სიზუსტისა და სისტემის უსაფრთხო ფუნქციონირების აუცილებლობას.[53]

გ) პროექტის თანახმად, ხელოვნური ინტელექტის სისტემები შეზღუდული რისკების შემცველად კლასიფიცირდება, რომელიც საჭიროებს, რომ მომხმარებლებმა იცოდნენ, რომ მათ მანქანასთან აქვთ კომუნიკაცია და არა — ადამიანთან (მაგალითად, „ჩეთბოტები“). სავარაუდოდ, გამჭვირვალობის მოთხოვნა აუცილებელია, რათა პროგრამის მიერ მომხმარებლები არ იყვნენ შეცდომაში შეყვანილნი და რომ გაცნობიერებული ჰქონდეთ ის ფაქტი, რომ „მონიტორის მეორე მხარეს“ არ ზის ადამიანი.

დ) ბოლოს, პროექტის მიხედვით, მინიმალური რისკის კატეგორიას მიეკუთვნება სისტემა, რომელიც წარმოადგენს ხელოვნური ინტელექტის დიდ უმრავლესობას და რომელთა გამოყენება თითქმის არანაირ რისკს უქმნის მომხმარებელთა უფლებებსა და უსაფრთხოებას. კოდექსი იძლევა ამ სისტემების თავისუფალი გამოყენების საშუალებას და მათ მიმართ არ შეიცავს ჩარევის რაიმე ღონისძიებებს, ამიტომ ისინი პრაქტიკულად არ თავსდებიან მის ფარგლებში. ასეთი ხელოვნური ინტელექტის მაგალითებია სპამის ფილტრები ან ვიდეო თამაშები.

ახლახანს, ევროპის მონაცემთა დაცვის საბჭომ (EDPB) და ევროპის მონაცემთა დაცვის ზედამხედველმა (EDPS) გამოხატეს საკუთარი ერთობლივი მოსაზრება, რომლის თანახმად, ისინი მიესალმებიან ასეთ პროექტს. თუმცა ზოგიერთ სფეროში, მაგალითად, დისტანციური ბიომეტრული იდენტიფიკაციის დარგში, ევროპის მონაცემთა დაცვის საბჭომ (EDPB) გაამკაცრა წესები. მისი აზრით, როგორც წესი, იკრძალებოდა დისტანციური ბიომეტრული იდენტიფიკაციის სისტემა, რომელსაც შეუძლია მონაცემთა

[52] *European Commission,* A Digitális korra felkészült Európa: A Bizottság új szabályokat és intézkedéseket javasol a kiválóságra és bizalomra épülő mesterséges intelligencia terén. Sajtóközlemény, 2021, <https://ec.europa.eu/commission/presscorner/detail/hu/IP_21_1682> [28.11.2022].
[53] იქვე.

სუბიექტების კლასიფიცირება კატეგორიებად ზოგიერთი ისეთი მახასიათებლის საფუძველზე, როგორიცაა წარმომავლობა, სქესი ან სექსუალური ორიენტაცია, რადგან ამან შეიძლება, გამოიწვიოს დისკრიმინაცია.[54]

გარდა ზემოხსენებულისა, ევროპის საბჭო ასევე მიესალმა ამ სფეროს რეგულირებას. თუმცა პოლონეთისა და ჩეხეთის სენატებმა ასევე გამოთქვეს შეშფოთება ბიომეტრული იდენტიფიკაციის სისტემების საჯარო ადგილებში გამოყენების შესახებ, რაც ნებადართულია პროექტით. შესაბამისად, ისინიც, ევროპის მონაცემთა დაცვის საბჭოს (EDPB) პოზიციის მსგავსად, კომისიისადმი გაგზავნილ წერილში მოუწოდებენ უფრო მკაცრი მიდგომისაკენ.[55]

უახლოეს პერიოდში რეგულაციის პროექტი ხშირად გახდება პრაქტიკული და სამეცნიერო განხილვის საგანი, ვიდრე სრულად არ იქნება იგი ევროკავშირის მიერ აღიარებული. ზოგადად, შეიძლება ითქვას, რომ რისკზე დაფუძნებული მიდგომა და იმ სისტემების შედარებით ვიწრო სპექტრი, რომლებიც აკრძალულია და კლასიფიცირებულია როგორც მაღალი რისკის შემცველი, გვთავაზობს პროგრესულ და საკმაოდ მოქნილ რეგულაციას.

11. დასკვნა

ხელოვნური ინტელექტის და მონაცემებზე დაფუძნებული მანქანური სწავლების განვითარებამ გვიჩვენა, რომ პროგრამული უზრუნველყოფით და მათი ქცევით მიღებული გადაწყვეტილებები დამოკიდებულია მონაცემთა ერთობლიობაზე, რომელიც მათ შესასწავლად გამოიყენება. ამიტომ, პროგრამული უზრუნველყოფის დეველოპერი და სისტემის ოპერატორი აღნიშნული სისტემების მიმართ უდიდესი პასუხისმგებლობის მატარებელნი არიან. ყველა ფაქტორის გათვალისწინებით, ევროკავშირის ხელოვნური ინტელექტის რეგულაციის ახალი პროექტიდან გამომდინარე, მომავალში ეს სფერო უფრო მეტად ემპათიურიც უნდა გახდეს.

ავტომატური გადაწყვეტილებების მიღებასა და პროფილირებაში მეტად მნიშვნელოვანია, რომ მონაცემთა ერთობლიობა, რომელიც გამოიყენება სწავლებისთვის, იყოს სათანადო ხარისხის, რისი მიღწევაც შესაძლებელია მონაცემთა ბაზის ფრთხილი, წინასწარი შერჩევითა და მონაცემთა შესაბამისი მარკირებით. ამიტომ შეხედულება, რომ რაც უფრო მეტ მონაცემებს გამოიყენებს მანქანური სწავლების

[54] *European Data Protection Board*, *European Data Protection Supervisor*, Joint opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2021, <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> [28.11.2022].

[55] *Pethő M.,* Aranyérem a szabályozásban? Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/messzelato/2021/12/08/aranyerem-szabalyozasban/> [28.11.2022].

ალგორითმი, მით უფრო ნაყოფიერად ფუნქციონირებს და შესაბამის გადაწყვეტილებებს მიიღებს, ფუნდამენტურად მცდარია.[56] ჩვეულებრივ, მონაცემთა ერთობლიობის ფრთხილი, წინასწარი შერჩევა და მათი აუცილებელ რაოდენობამდე შემცირება, შედეგად მოგვცემს უფრო ეფექტიანი გადაწყვეტილების მიმღებ სისტემებს; ეს დასტურდება არსებული სამეცნიერო შეხედულებით; და ევროკავშირის რეგულაციის ახალი პროექტი მას, როგორც პრინციპულ საკითხს, ძირითად მოთხოვნად განსაზღვრავს. როგორც ნათქვამია, ნაკლები, ხშირად, უკეთესი შედეგის მომტანია...

გარდა ზემოხსენებულისა, პერსონალური მონაცემთა დამუშავებისას, სისტემების უშუალოდ რეალურ დროში ოპერირების პროცესში აუცილებელია, ვაჩვენოთ დამუშავებისათვის შესაფერისი იურიდიული საფუძველი, გავითვალისწინოთ მონაცემების მინიმალიზაციის პრინციპი და უზრუნველვყოთ სისტემის გამჭვირვალე და ხელმისაწვდომი ფუნქციონირება, სადაც გამოყენებული ლოგიკის შესახებ ინფორმაცია მთავარ საკვანძო ელემენტს წარმოადგენს.

ამრიგად, შეიძლება ითქვას, რომ ზოგადი რეგულირების თვალსაზრისით, ხელოვნური ინტელექტისა და მონაცემებით მართული ავტომატური გადაწყვეტილების მიღება განვითარების ჯერ კიდევ საწყის ეტაპზეა; თუმცა, ბოლო პერიოდში ჩამოყალიბებული კონკრეტული რეგულაციური კონცეფციები შორსმჭვრეტია. მომავალ წლებში მთავარი საკითხი იქნება რეგულაციის პრაქტიკული და ეფექტიანი გამოყენება. რაც შეგვეხება ჩვენ, მოუთმენლად ველით ახალ ეტაპებს სამართლებრივ პრაქტიკაში.

ბიბლიოგრაფია:

1. 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 L 119, 4/5/2016, 1–88.
2. Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information of Hungary, 2011.
3. *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 8, 10, 22, 23, 24, 25, <https://naih.hu/files/wp251rev01_hu.pdf>, [28.11.2022].

[56]*Datatilsynet*, Artificial Intelligence and Privacy, Report, 2018, 11. <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].

4. *Article 29 Data Protection Working Party,* Guidance on the Consent according to Regulation (EU) 2016/679 (WP259rev.01.), 2018, 20-22, <http://naih.hu/files/wp259-rev-0_1_HU.PDF> [28.11.2022].
5. *Barthelmess U., Furbach U.,* Do We Need Asimov's Laws? In: Lecture Notes in Informatics. Bonn, Gesellschaft für Informatik, 2014, 5.
6. *Deli G., Kocsis B., Muhari N.,* Akarva-akaratlanul – az adatvédelem és az akaratszabadság dilemmái. In: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 237-238.
7. *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 119-120, 121, 122, 123.
8. *Datatilsynet,* Artificial Intelligence and Privacy, Report, 2018, 7, 10, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].
9. *European Data Protection Board*, *European Data Protection Supervisor*, Joint opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2021, <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> [28.11.2022].
10. *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 189, 190, 191, 193, 199-200.
11. *Eszteri D.,* Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat, Magyar Jog, 12, 2019, 679-680.
12. *Goertzel B., Pitt J.,* Nine Ways to Bias Open-Source AGI Toward Friendliness, Journal of Evolution and Technology, Vol. 22, 2011.
13. *Karvalics L. Z.,* Mesterséges intelligencia – a diskurzusok újratervezésének kora, Információs Társadalom, Vol. 15, 2015, 13, 14.
14. *Klein T., Tóth A. (Eds.),* Technológia jog – Robotjog – Cyberjog, 2018, 50.
15. *Kollár C.,* Kína és a társadalmi kreditrendszere, Hadtudomány, 2, 2020, <https://www.mhtt.eu/hadtudomany/2020/2020_2szam/079-097_Kollar.pdf> [28.11.2022].
16. *Kurzweil R.,* A szingularitás küszöbén, 2014, in: *Marosán G.,* Mi vár ránk a szingularitáson túl? Népszava, 2019, 12, 15.
17. *Lacan J.,* A tükör-stádium mint az én funkciójának kialakítója, ahogyan ezt a pszichoanalitikus tapasztalat feltárja a számunkra, Thalassa, Vol. 4, 1993, 2.
18. *Masahiro M., The Uncanny Valley, In: IEEE Robotics and Automation, Vol. 19, 2012, 2.*
19. *Marosán G.,* Mi vár ránk a szingularitáson túl? Népszava, 2019, 12, 15.

20. *Németh S.,* A közösségi oldalak szolgáltatóinak jogi felelőssége, PhD értekezés (műhelyvitára benyújtott változat), 2021, 119, <https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf> [28.11.2022].
21. *Pethő M.,* Aranyérem a szabályozásban? Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/messzelato/2021/12/08/aranyerem-szabalyozasban/> [28.11.2022].
22. *Péterfalvi A., Révész B., Buzás P. (ed.),* Magyarázat a GDPR-ról, 2018, 158.
23. *Pokol B.,* A mesterséges intelligencia társadalma, 2018, 55-56.
24. *Russell St. J., Norvig P.,* Mesterséges Intelligencia – Modern megközelítésben, Budapest, Panem, 2000, Ch. 26.
25. *Szathmáry Z., Barna M.,* Büntetőjogi kérdések az információk korában (mesterséges intelligencia, big data, profilozás), Budapest, HVG Orac, 2018, 44.
26. *Szepesvári C.*, Gépi tanulás – rövid bevezetés, 2005, 22, <http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf> [28.11.2022].
27. *Veale M., Edwards L.,* Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision Making and Profiling. Computer, Law and Security Review, Vol. 34, 2018, 2, 400, 401.
28. *Ződi Z.,* A mesterséges intelligencia jogi fogalma, Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/itkiblog/2021/06/18/a-mesterseges-intelligencia-jogi-fogalma/> [28.11.2022].
29. Facebook Platform Policy, II. point 4, <https://bit.ly/3rioTYH> [28.11.2022].
30. <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> [28.11.2022].
31. <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf> [28.11.2022].
32. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/> [28.11.2022].
33. <https://www.bbc.com/news/world-us-canada-48972327> [28.11.2022].

კახაბერ გოშაძე*

პერსონალურ მონაცემთა დაცვის პოლიტიკა, როგორც მონაცემთა დამუშავების გამჭვირვალობის ინდიკატორი

პერსონალურ მონაცემთა დამუშავება ნებისმიერი კერძო თუ საჯარო ორგანიზაციის საქმიანობის განუყოფელი ნაწილია. დამუშავების პროცესი ექვემდებარება ამა თუ იმ ორგანიზაციაში არსებულ მოთხოვნებს, რაც განსხვავებულია ფორმისა და მეთოდების მხრივ. მონაცემთა დამუშავებისას მნიშვნელოვანია გავაცნობიეროთ, რომ ეს პროცესი უნდა ხასიათდებოდეს გამჭვირვალობით, რათა ნებისმიერი ფიზიკური პირისთვის წინასწარ ცნობილი იყოს თუ რა სახის პერსონალური მონაცემები შეიძლება დამუშავდეს. ამ მიზნებისთვის გადამწყვეტი მნიშვნელობის მქონეა პერსონალურ მონაცემთა დაცვის პოლიტიკა, რომელიც ორგანიზაციამ საჯაროდ უნდა განათავსოს. მისი შემუშავებისა და ფორმირების ერთიანი და საყოველთაოდ შეთანხმებული სტანდარტი არ არსებობს, თუმცა განსაკუთრებით მნიშვნელოვანია, რომ პოლიტიკა იწერებოდეს ფიზიკური პირებისთვის გასაგებ ენაზე. ამდენად, წინამდებარე სტატია ეხება მონაცემთა დაცვის პოლიტიკის მნიშვნელობას, მის საჯაროობას, ფუნქციასა და ფორმირების თავისებურებებს.

საკვანძო სიტყვები: *პერსონალურ მონაცემთა დაცვა, მონაცემთა დაცვის პოლიტიკა, მონაცემთა დამუშავების გამჭვირვალობა.*

* ევროპის უნივერსიტეტის ასოცირებული პროფესორი, სამართლის დოქტორი; საქართველოს პარლამენტის ადამიანის უფლებათა დაცვისა და სამოქალაქო ინტეგრაციის კომიტეტის აპარატის წამყვანი სპეციალისტი.

1. შესავალი

პერსონალურ მონაცემთა დაცვის კონცეფცია რამდენიმე ათწლეულია არ კარგავს აქტუალობას. მეტიც, მონაცემთა დაცვისკენ მიმართული სამართლებრივი რეგულირების დახვეწა განსაკუთრებული ყურადღების საგანია ევროკავშირისა და ევროპის საბჭოს ფარგლებში, ხაზგასასმელია უკანასკნელ წლებში მიღებული სამართლებრივი აქტები.[1] საკითხის აქტუალობის ფონზე, ცალკე ყურადღების საგანია პერსონალურ მონაცემთა დაცვის უფლების უპირველესი ბენეფიციარების – მონაცემთა სუბიექტების[2] წინაშე გამჭვირვალობის უზრუნველყოფა. ეს შესაძლებელია სხვადასხვა მიმართულებით განხორციელდეს, თუმცა მოცემული სტატიის ფარგლებში ორგანიზაციის მიერ მონაცემთა დამუშავების გამჭვირვალობის სტანდარტის დაცვაზე იქნება საუბარი.

პერსონალურ მონაცემთა დაცვის პოლიტიკის შემუშავება და მისი საჯაროდ განთავსება, შესაძლოა მონაცემთა დამუშავების გამჭვირვალობის მნიშვნელოვანი ინდიკატორი იყოს. მეორე მხრივ, მხოლოდ მისი შემუშავება ვერ იქნება ორგანიზაციის მიერ კანონით დადგენილი მოთხოვნების შესრულების მაჩვენებელი. ასევე, როდესაც საუბარია მონაცემთა დაცვის პოლიტიკაზე, აქ არ იგულისხმება ერთი, კომპლექსური, ყოვლისმომცველი ფორმისა და შინაარსის დოკუმენტი, ვინაიდან მონაცემთა დაცვის წესების აღნუსხვა არ შეიძლება შემოიფარგლებოდეს მხოლოდ ერთი დოკუმენტის შექმნით, არამედ, საჭიროების შესაბამისად, ორგანიზაციას შესაძლებელია ჰქონდეს მონაცემთა დაცვის სხვადასხვა მარეგულირებელი წესი.[3] მონაცემთა დაცვის პოლიტიკის შემუშავება უკავშირდება მონაცემთა უსაფრთხოების უზრუნველსაყოფად გასატარებელ ღონისძიებებს, ვინაიდან ის უნდა განსაზღვრავდეს დამუშავების უსაფრთხოების ზომებსა და პროცედურებს,[4] თუმცა, ეს არ გამორიცხავს პოლიტიკის, როგორც გამჭვირვალობის ინდიკატორის მნიშვნელობას.

---

[1] 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 L 119, 4.5.2016, 1–88*; Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), *OJ L 119, 4.5.2016, 89–131*; Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18.05.2018.

[2] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (5669-რს, 28/12/2011) მე-2 მუხლის „ვ“ პუნქტის თანახმად, მონაცემთა სუბიექტად ითვლება ნებისმიერი ფიზიკური პირი, რომლის შესახებაც მუშავდება მონაცემი.

[3] მაგალითად, ორგანიზაციაში შესაძლოა, ასევე, იყოს შემუშავებული ე. წ. “cookie” პოლიტიკა, ვებგვერდის მეშვეობით მონაცემთა დამუშავების გამჭვირვალობის უზრუნველყოფისთვის.

[4] *სახელმწიფო ინსპექტორის სამსახური,* თვითშეფასების კითხვარი, 2021, 7, 13.

მეტი სიცხადისთვის, უნდა აღინიშნოს, რომ წინამდებარე სტატიაში საუბარია იმ ინფორმაციაზე, რომელიც ორგანიზაციის ვებგვერდზე საჯაროდ არის განთავსებული, ხელმისაწვდომია ნებისმიერი დაინტერესებული პირისთვის და ასახავს პერსონალურ მონაცემთა დამუშავების პირობებს. თუმცა ეს არ გამორიცხავს ორგანიზაციის შიგნით დამუშავების დეტალური წესებისა და პროცედურების შემცველი დოკუმენტების არსებობას. მეტიც, ამგვარი შიდაორგანიზაციული დოკუმენტების შემუშავება, თითოეული ორგანიზაციის ვალდებულებაა. კანონმდებლობით შესაძლებელია, დაწესდეს მონაცემთა დაცვის პოლიტიკის საჯაროდ განთავსების ვალდებულებაც, თუმცა, ასეთ შემთხვევაში, რთული იქნება შეთანხმება იმ დეტალებზე, რაც უნდა აისახოს დოკუმენტში, ვინაიდან ორგანიზაციები ერთმანეთისგან ძალიან განსხვავდებიან, როგორც ორგანიზაციულ-სამართლებრივი ფორმის, ისე საქმიანობის მიხედვით.

ასევე, საყურადღებოა, რომ საქართველოში მონაცემთა დაცვის პოლიტიკის ფორმირებისადმი ყურადღება სათანადოდ არაა გამახვილებული. ეს კომპლექსური გამოწვევაა და არ უკავშირდება მხოლოდ იმას, რომ კანონმდებლობით არ არის დაწესებული მსგავსი საჯარო პოლიტიკის შემუშავების მოთხოვნა, არამედ, ეს ასევე განპირობებულია ამ სფეროსადმი საზოგადოების მცირე ინტერესითა და ორგანიზაციების მხრიდან იმის გაუაზრებლობით, რომ მონაცემთა დამუშავების გამართული პროცესის დანერგვა და მისი საჯაროდ დემონსტრირება, ორგანიზაციის ერთ-ერთ ძლიერ მხარედ შეიძლება წარმოჩინდეს. არსებული ვითარების გათვალისწინებით, საქართველოს კონტექსტში, ორგანიზაციების მიერ მონაცემთა დაცვის პოლიტიკის შემუშავება, აუცილებლობაც კი არის.

ამდენად, სტატიის პირველი პარაგრაფი განიხილავს მონაცემთა დაცვის პოლიტიკის ადგილს პერსონალურ მონაცემთა დაცვის კონცეფციაში. მეორე პარაგრაფი ეთმობა პერსონალურ მონაცემთა დაცვის პოლიტიკას, სადაც განხილული იქნება რეგულირების ზოგადი სამართლებრივი ჩარჩო და პოლიტიკის არსი. მესამე პარაგრაფი ეხება პოლიტიკის დოკუმენტის შემუშავებისა და ამოქმედების ასპექტებს, ხოლო მეოთხე პარაგრაფი განიხილავს პოლიტიკის შესაძლო შინაარსს ზოგიერთი კომპანიის მაგალითზე. დასკვნაში კი, განხილული საკითხების შეჯამების მიზნით, შემოთავაზებულია რიგი საკითხების რეზიუმირება და ზოგადი რეკომენდაციები.

2. მონაცემთა დაცვის პოლიტიკის ადგილი პერსონალურ მონაცემთა დაცვის კონცეფციაში

პერსონალურ მონაცემთა დაცვის უფლება ადამიანის ძირითად უფლებათა კატეგორიას მიეკუთვნება.[5] მისი წარმოშობა პირადი ცხოვრების ხელშეუხებლობის უფლების განვითარების შედეგია. პერსონალურ მონაცემთა დაცვის კონცეფციის ძირითადი არსი მდგომარეობს იმაში, რომ განსაზღვროს მონაცემთა გამოყენების კანონით დადგენილი გზები, ასევე, უზრუნველყოს მონაცემთა სუბიექტების უფლებათა დაცვა. პერსონალურ მონაცემთა დაცვის მარეგულირებელი ნორმები თანაბრად ვრცელდება საჯარო და კერძო იურიდიულ პირებზე, ასევე, ნებისმიერ პირზე, რომელიც რაიმე ფორმით არის ჩართული მონაცემთა დამუშავების პროცესში.[6] შესაბამისად, პერსონალურ მონაცემთა დაცვის კონცეფციის მიზანია, უზრუნველყოს მონაცემთა უკანონო დამუშავების პრევენცია.

ამ პროცესში დიდი მნიშვნელობა ენიჭება მონაცემთა სუბიექტის (ფიზიკური პირის) ინფორმირების ხარისხს, რაც საბოლოოდ საშუალებას აძლევს მას, წარმოდგენა ჰქონდეს დამუშავების პროცესსა და მის უფლებებზე. პერსონალურ მონაცემთა დამუშავება დაფუძნებულია გარკვეულ პრინციპებზე, რომელთა განუხრელი დაცვა განაპირობებს ამ უფლებაში ჩარევის კანონიერებას. ეს პრინციპები ჯერ კიდევ 1981 წელს აისახა ევროპის საბჭოს 108-ე კონვენციაში,[7] რაც შემდგომ დამკვიდრდა როგორც

[5] *Hert P. D., Gutwirth S.,* Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action, 2009, 7.

[6] მონაცემთა დამუშავების პროცესში მთავარი მოქმედი პირები არიან მონაცემთა დამმუშავებელი და უფლებამოსილი პირი. იმისთვის, რათა პირს „დამმუშავებლის“ სტატუსი მიენიჭოს, აუცილებელია ორი პირობის კუმულაციური დაკმაყოფილება, კერძოდ, პირი უნდა განსაზღვრავდეს დამუშავების მიზანსა და იმავდროულად საშუალებას („პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მუხლი 2(„ი“)). უფლებამოსილი პირის შემთხვევაში, ის ერთგვარი „დამხმარე“ ფუნქციის მატარებელია, კერძოდ, პირი „უფლებამოსილად“ მიიჩნევა მხოლოდ იმ შემთხვევაში, თუ დამუშავების პროცესი ადმინისტრირებულია დამმუშავებლის მიერ და იმავდროულად, ეს უკანასკნელი დამუშავების პროცესში რთავს „დამხმარე“ (უფლებამოსილ) პირს, რომელზეც გასცემს დავალებებს („პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მუხლი 2(„კ“)). შესაბამისად, უფლებამოსილი პირი უნდა მოქმედებდეს მხოლოდ დამმუშავებლის მითითებების შესაბამისად და დაწესებულ ფარგლებში. აქედან გამომდინარე, ლოგიკურია, რომ დამუშავების პროცესში თუ წარმოდგენილია უფლებამოსილი პირი, ეს აუცილებლად ნიშნავს იმას, რომ პროცესი ადმინისტრირებულია დამმუშავებლის მიერ. აქვე უნდა აღინიშნოს ისიც, რომ ხშირ შემთხვევაში, ხდება უფლებამოსილი პირის სტატუსის არასწორი აღქმა და მაგალითად, ორგანიზაციაში, შრომითი ხელშეკრულებით დასაქმებული პირის მიჩნევა „უფლებამოსილად“, რაც არ არის სწორი, ვინაიდან უფლებამოსილი პირი, როგორც წესი, არის დამმუშავებლისგან ორგანიზაციული ფორმით დისტანცირებული, დამოუკიდებელი იურიდიული პირი. აღნიშნული ბუნდოვანების აღმოფხვრა გათვალისწინებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტის ინიციირებული ვერსიის (07-3/353/9; 22/05/2019) მე-3 მუხლის „ჟ“ პუნქტით, სადაც აღნიშნულია, რომ „უფლებამოსილ პირად არ მიიჩნევა მონაცემთა დამმუშავებელთან შრომით ურთიერთობაში მყოფი ფიზიკური პირი“.

მონაცემთა დამუშავების საყოველთაო სტანდარტი.[8] ეს პრინციპებია: 1. მონაცემთა სამართლიანი და კანონიერი დამუშავება; 2. მონაცემთა მიზნობრივი დამუშავება; 3. მონაცემთა პროპორციული დამუშავება; 4. სწორი და უტყუარი მონაცემების დამუშავება; 5. მონაცემთა განსაზღვრული ვადით დამუშავება.

აღსანიშნავია, რომ სუბიექტის წინაშე მონაცემთა დამუშავების გამჭვირვალობის უზრუნველყოფა მოაზრებულია პირველ პრინციპში, ხოლო მონაცემთა დაცვის საერთო რეგულაციითა (GDPR) და ევროპის საბჭოს მოდერნიზებული 108+ კონვენციით, გამჭვირვალედ დამუშავების მოთხოვნა პრინციპად არის გაწერილი.[9]

დამუშავების გამჭვირვალობა სხვადასხვა გზით შეიძლება უზრუნველვყოთ, დამუშავების პროცესის დაწყებისას ან დაწყებამდე.[10] შესაბამისად, პერსონალურ მონაცემთა გამჭვირვალე დამუშავება მოითხოვს სუბიექტის გათვალისწინებას, მათ შორის, დამუშავების პროცესის შესახებ სუბიექტის ინფორმირებას მისთვის გასაგები ფორმით. ბუნებრივია, აქ მეტწილად საუბარია წერილობით ფორმაზე, სუბიექტისთვის გასაგები ენის გამოყენებასა და დამუშავების პროცესის იმგვარ აღწერაზე, რაც არ გამოიწვევს გაუგებრობას მისი გაცნობის შემდეგ.

მხედველობაში უნდა მივიღოთ ისიც, რომ პერსონალურ მონაცემთა ავტომატიზებული სისტემებით დამუშავების თაობაზე სათანადო გამჭვირვალობის უზრუნველყოფა საკვანძო მნიშვნელობის იყო პერსონალურ მონაცემთა დაცვის, ჯერ კიდევ, პირველი თაობის ევროპულ კანონმდებლობებში. მაგალითად, საფრანგეთის კანონი, 1978 წლიდან, ანიჭებდა პირს უფლებას, სცოდნოდა ინფორმაცია მის შესახებ დამუშავებული მონაცემების თაობაზე.[11]

როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობა განსაკუთრებულ ყურადღებას უთმობს დამმუშავებლის მხრიდან სუბიექტის ინფორმირებას. ევროპის საბჭოს 108+ მოდერნიზებული კონვენციის მე-8 მუხლით გაწერილია დამმუშავებლის ვალდებულება, უზრუნველყოს დამუშავების პროცესის გამჭვირვალობა, რაც გამოიხატება შემდეგი სახის ინფორმაციის მიწოდებაში: დამმუშავებლის ვინაობა, ოპერირების ან დაფუძნების ადგილი; დამუშავების სამართლებრივი საფუძველი და მიზანი; დამუშავებულ მონაცემთა კატეგორიები; მონაცემთა მიმღებები; სუბიექტის უფლებების რეალიზაციის საშუალებები; ასევე, სხვა ნებისმიერი დამატებითი

[8] მონაცემთა დაცვის საერთო რეგულაციის (GDPR) მიხედვით, ამ პრინციპების ჩამონათვალს დაემატა გამჭვირვალობისა და უსაფრთხოების პრინციპები, რითაც, ევროკავშირის ფარგლებში, დამუშავების სტანდარტი ამაღლდა.

[9] მონაცემთა დაცვის საერთო რეგულაცია (GDPR), მუხლი 5(1)(a); 108+ კონვენცია, მუხლი 5(4)(a).

[10] *Kuner C., Bygrave L. A., Docksey C. (eds),* The EU General Data Protection Regulation (GDPR) Commentary, Oxford University Press, 2020, 415.

[11] იქვე, 416.

ინფორმაცია, რაც საჭიროა მონაცემთა სამართლიანი და გამჭვირვალე დამუშავებისთვის.[12]

ანალოგიურად, მონაცემთა დაცვის საერთო რეგულაციაც (GDPR) აკისრებს დამმუშავებლებს ინფორმირების ვალდებულებას, თუმცა მისაწოდებელი ინფორმაცია უფრო დეტალიზებულია. რეგულაციის მე-13 მუხლის თანახმად, დამმუშავებელი ვალდებულია სუბიექტს მიაწოდოს ინფორმაცია, რომელიც ეხება: დამმუშავებლის ვინაობას, საკონტაქტო ინფორმაციას; მონაცემთა დაცვის ოფიცრის შესახებ ინფორმაციას, არსებობის შემთხვევაში; დამუშავების მიზანსა და სამართლებრივ საფუძველს; დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების საფუძველზე დამუშავებას, ასეთის არსებობისას; მონაცემთა მიმღებს ან მათ კატეგორიებს; საერთაშორისო გადაცემასა და მასთან დაკავშირებულ დეტალებს.[13] გარდა ამისა, რეგულაცია დამატებით მოითხოვს დამმუშავებლისგან ინფორმაციის მიწოდებას უშუალოდ მონაცემთა შეგროვებისას, რათა უზრუნველყოფილ იქნეს სამართლიანი და გამჭვირვალე დამუშავება, კერძოდ: მონაცემთა შენახვის პერიოდი ან, შეუძლებლობის შემთხვევაში, კრიტერიუმი, რომელიც გამოიყენება პერიოდის განსაზღვრისთვის; მონაცემთა წვდომის, შეცვლის, წაშლისა და დამუშავების შეზღუდვის უფლების შესახებ, ასევე, მონაცემთა პორტირების უფლების შესახებ; თანხმობის გამოხმობის უფლების და მასთან დაკავშირებული დეტალების შესახებ; საზედამხედველო ორგანოში საჩივრის შეტანის უფლების შესახებ; მონაცემთა წარდგენის სავალდებულო შემთხვევების შესახებ და წარუდგენლობის შედეგების თაობაზე; ავტომატიზებული მონაცემთა დამუშავების, მათ შორის, პროფილირების შესახებ, კერძოდ, გამოყენებული ლოგიკის და იმ შედეგების შესახებ, რაც შეიძლება დადგეს სუბიექტისთვის დამუშავების შედეგად.[14]

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი აკისრებს დამმუშავებელს გარკვეული ინფორმაციის მიწოდების ვალდებულებას სუბიექტისთვის, თუმცა, რეგულაციისგან განსხვავებით, სუბიექტისთვის წარსადგენი ინფორმაციის ჩამონათვალი არ არის ყოვლისმომცველი და იგი უდავოდ საჭიროებს დეტალიზებას. მიუხედავად ამისა, კანონი მაინც აწესებს იმ მინიმუმს, რის მიხედვითაც სუბიექტი შეიძლება ჩაითვალოს ინფორმირებულად დამუშავებასთან დაკავშირებული ზოგადი საკითხების ირგვლივ. კანონით განსაზღვრული ვალდებულება მოიცავს ინფორმაციის მიწოდების მოთხოვნას შემდეგ მონაცემებთან მიმართებით: მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ვინაობა და მისამართი; დამუშავების მიზანი; სავალდებულოა თუ ნებაყოფლობითი მონაცემთა მიწოდება და სავალდებულოობის შემთხვევაში – მასზე უარის თქმის სამართლებრივი შედეგები;

[12] 108+ კონვენცია, მუხლი 8(1).
[13] მონაცემთა დაცვის საერთო რეგულაცია (GDPR), მუხლი 13(1).
[14] იქვე, მუხლი 13(2).

მონაცემთა სუბიექტის უფლება – მიიღოს ინფორმაცია მის შესახებ დამუშავებული მონაცემების თაობაზე, მოითხოვოს მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა და განადგურება.[15]

3. პერსონალურ მონაცემთა დაცვის პოლიტიკა

3.1. ზოგადი სამართლებრივი ჩარჩო

პერსონალურ მონაცემთა დაცვის პოლიტიკის მარეგულირებელი წესები ჩნდება 1990-იანი წლებიდან, როდესაც ინტერნეტის გამოყენებამ წარმოშვა კითხვები პირადი ცხოვრების პატივისცემის წინაშე არსებული რისკების მიმართ.[16] როგორც აღინიშნა, პერსონალურ მონაცემთა დაცვის პოლიტიკა, ორგანიზაციის მიერ წარმოებული დამუშავების პროცესის გამჭვირვალობის მნიშვნელოვანი ინდიკატორია, თუმცა, მაგალითად, ევროკავშირის ფარგლებში, პოლიტიკის შემუშავების სამართლებრივად გაწერილი პირდაპირი ვალდებულება მკაფიოდ და სიტყვასიტყვით დღემდე არ გვხვდება. მიუხედავად ამისა, პერსონალურ მონაცემთა დაცვის საერთაშორისო და შიდაეროვნული კანონმდებლობით დადგენილი მოთხოვნებიდან გამომდინარე, პოლიტიკის ფორმირების აუცილებლობაც კი არსებობს.

მონაცემთა დაცვის საერთო რეგულაციის (GDPR) პრეამბულის 78-ე პუნქტის თანახმად, მასთან შესაბამისობის დემონსტრირების მიზნით, დამმუშავებელმა უნდა შეიმუშაოს შიდა პოლიტიკა, რომელიც შესაბამისი იქნება “Privacy by Design” და “Privacy by Default” პრინციპებთან. ამდენად, შიდაორგანიზაციულ დონეზე მიღებული პოლიტიკა შეიძლება, წარმოადგენდეს ერთგვარ სახელმძღვანელოს მონაცემთა დაცვის საჯარო პოლიტიკის ფორმირებისთვის. ამასთან, შიდაორგანიზაციულ პოლიტიკაზე მითითებას შეიცავს, ასევე, რეგულაციის 24-ე მუხლის მე-2 პუნქტი, სადაც აღნიშნულია ტექნიკური და ორგანიზაციული ზომების იმპლემენტირების თაობაზე.

საქართველოს კონტექსტში, პოლიტიკის შემუშავების პირდაპირი ვალდებულება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი არ არის. ამისგან განსხვავებით, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი შეიცავს ჩანაწერს, რის მიხედვითაც „კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია მიიღოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, რომელიც ემსახურება ამ კანონის დებულებათა აღსრულებას და

[15] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მუხლი 15(1).
[16] *Waldman A. E.,* Privacy, Notice and Design, Stanford Technology Law Review, 2018, 80.

განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას.“[17] ამ შემთხვევაშიც, შიდაორგანიზაციული მოხმარების დოკუმენტი შეიძლება, წარმოადგენდეს ერთგვარ სახელმძღვანელოს მონაცემთა დაცვის საჯარო პოლიტიკის ფორმირებისთვის. თუმცა შენიშვნის სახით უნდა ითქვას ისიც, რომ ამ დოკუმენტის შედგენის ვალდებულება ვრცელდება მხოლოდ სახელმწიფო ან მუნიციპალიტეტის ორგანოზე ან დაწესებულებაზე, თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტზე, იურიდიულ პირზე, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.[18]

ევროკავშირისგან განსხვავებით, ამერიკის შეერთებულ შტატებში არ მოქმედებს საყოველთაო, ფედერალური კანონმდებლობა პერსონალურ მონაცემთა დაცვის შესახებ. ამის ნაცვლად, აშშ-ში გვხვდება ე. წ. „სექტორული“ კანონმდებლობა, რომელიც არეგულირებს პირადი ცხოვრების ამა თუ იმ სფეროს.[19] შესაბამისად, სრულიად განსხვავებულ მიდგომას შეიცავს, მაგალითად, კალიფორნიის შტატის კანონმდებლობა, სადაც პირადი ცხოვრების დაცვის პოლიტიკის (“Privacy Policy”) შემუშავება ვალდებულებას წარმოადგენს. ვალდებულების თანახმად, კომერციული ვებგვერდის ან ონლაინ მომსახურების ოპერატორი, რომელიც აგროვებს პერსონალურ მონაცემებს ინტერნეტის საშუალებით კალიფორნიაში მცხოვრები ინდივიდუალური მომხმარებლების შესახებ, რომლებიც იყენებენ ან სტუმრობენ ორგანიზაციის კომერციულ ვებგვერდს ან სარგებლობენ ონლაინ მომსახურებით, საჯაროდ უნდა განათავსონ თავიანთი პირადი ცხოვრების დაცვის პოლიტიკა ვებგვერდზე.[20] მეტიც, გარდა პოლიტიკის სავალდებულო საჯაროობისა, კანონი განსაზღვრავს პოლიტიკის შინაარსის შემადგენელ ნაწილებს, ესენია: პერსონალური მონაცემების კატეგორიები და იმ მესამე პირთა კატეგორიები, ვისაც შეიძლება გადაეცეს მონაცემები; პერსონალურ მონაცემთა წვდომასთან და ცვლილებებთან დაკავშირებული პროცესის აღწერა; პოლიტიკაში ცვლილების შეტანისას მომხმარებლის შეტყობინების პროცედურის აღწერა; პოლიტიკის მოქმედების პერიოდი; “do not track” ან სხვა მექანიზმებზე რეაგირების ფორმების განმარტება, რომელიც უზრუნველყოფს მომხმარებლების ონლაინ აქტივობის მონაცემთა შეგროვებისას შესაგროვებელ მონაცემთა არჩევის შესაძლებლობას; შემთხვევებს, როდესაც სხვა პირები შეიძლება, აგროვებდნენ მონაცემებს მომხმარებლის აქტივობის შესახებ.[21]

[17] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი (6391-Iს; 05.06.2012), მუხლი 4(1).
[18] მუხლი 2(„ზ“).
[19] *Waldman A. E.,* Privacy, Notice and Design, Stanford Technology Law Review, 2018, 90.
[20] CalOPPA, Business and Professions Code – BPC, 01/01/2014, Division 8, Ch. 22, 22575(a).
[21] იქვე, 22575(b).

როგორც აღინიშნა, პოლიტიკის შემუშავებაზე პირდაპირ მითითებას არც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი აკეთებს. კანონი განსაზღვრავს პერსონალურ მონაცემთა სამართლიანი დამუშავების ვალდებულებას,[22] ასევე, ადგენს სუბიექტისთვის ზოგადი ინფორმაციის მიწოდების ვალდებულებას, როგორიცაა: დამმუშავებლის და უფლებამოსილი პირის ვინაობა და მისამართი; დამუშავების მიზანი; დამუშავების სავალდებულო ან ნებაყოფლობითი ხასიათი; სუბიექტის ხელთ არსებული უფლებები.[23]

3.2. პოლიტიკის არსი

მიუხედავად იმისა, თუ რა საშუალებაა გამოყენებული პერსონალური მონაცემების დამუშავებისთვის, დამმუშავებელს გააჩნია რიგი ვალდებულებები მომხმარებლების (მონაცემთა სუბიექტების) წინაშე. უპირატესად ეს ვალდებულება მოიცავს მოთხოვნას, რომ მონაცემები უსაფრთხოდ იყოს შენახული, მომხმარებლის პირადი ცხოვრება იყოს დაცული და დამუშავების თაობაზე პოლიტიკის საშუალებით მოხდეს სუბიექტების ინფორმირება.[24]

გამჭვირვალობის დემონსტრირებისა და დამმუშავებლის მხრიდან ინფორმირების კუთხით არსებული ვალდებულებების შესრულების უპირველესი და ყველაზე მოხერხებული გზაა პერსონალურ მონაცემთა დამუშავების შესახებ საჯარო შეტყობინების (პოლიტიკის) განთავსება. ეს შეტყობინება, თავისი არსით, წარმოადგენს ერთგვარ ინფორმაციის წარმდგენ დოკუმენტს. როგორც წესი, მსგავსი დოკუმენტები საჯაროდ არის განთავსებული ორგანიზაციების ვებგვერდებზე. სახელწოდების მხრივ, მისი ინგლისურენოვანი შესატყვისი არის “Privacy Policy”, ხოლო ქართულ კონტექსტში,

[22] მუხლი 4(ა). მონაცემთა სამართლიანი დამუშავების მოთხოვნა, მათ შორის, მოიაზრებს სუბიექტის წინაშე გამჭვირვალობის უზრუნველყოფასაც, ვინაიდან დამუშავების პროცესის სამართლიანობის უზრუნველყოფა, ასევე, გულისხმობს იმას, რომ ინფორმაციის გამოთხოვისას დამმუშავებელი უნდა აწვდიდეს ინფორმაციას თავის მხრივ.

[23] მუხლი 15(1). აქვე უნდა აღინიშნოს, მიუხედავად იმისა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტის ინიციირებული ვარიანტი არ განსაზღვრავს მონაცემთა დაცვის პოლიტიკის შექმნის ვალდებულებას, სუბიექტის ინფორმირების ნაწილში ის, იზიარებს მონაცემთა დაცვის საერთო რეგულაციის (GDPR) მიდგომას და მოქმედი კანონისგან განსხვავებით, შეიცავს დამატებით მოთხოვნებს გამჭვირვალობის პრინციპისა და ინფორმირების უფლების უკეთ უზრუნველყოფისთვის. კერძოდ, განსაზღვრულია მონაცემთა დამუშავების გამჭვირვალობის, სუბიექტის დეტალური ინფორმირების ვალდებულება, როდესაც მონაცემები უშუალოდ მისგან ან სხვა წყაროდან არის შეგროვებული. იხ. მუხლები 13, 14, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი და თანმდევი საკანონმდებლო აქტების პროექტები, № 07-3/353/9, 22/05/2019, <www.parliament.ge> [20.01.2023].

[24] *Pirzada M.,* Sample Privacy Policy Template, 2022, <https://www.privacypolicies.com/blog/privacy-policy-template/#Examples_Of_Useful_Clauses_For_Your_Privacy_Policy> [20.01.2023].

მას „პერსონალურ მონაცემთა ან პირადი ცხოვრების დაცვის პოლიტიკა“ შეიძლება ეწოდოს.

თავისი არსით, პერსონალურ მონაცემთა დაცვის პოლიტიკა, შეიძლება აღქმულ იქნეს, როგორც სამართლებრივი მოთხოვნის რეალიზების, ისე პრაქტიკული დანიშნულების დოკუმენტად. ცალსახაა, რომ პოლიტიკის მიზანს მონაცემთა სუბიექტის ინფორმირება წარმოადგენს, ეს დამუშავების გამჭვირვალობის უპირველეს მოთხოვნად შეიძლება ჩაითვალოს. მიზეზი, რის გამოც გამჭვირვალობა არის მოთხოვნილი ისაა, რომ მონაცემთა დაცვა მოკლებული იქნება ეფექტიანობას, თუ მონაცემთა სუბიექტს არ ექნება ინფორმაცია დამუშავების მიმდინარე პროცესზე, იმ მონაცემებზე, რაც გამოყენებულია, ვინ ამუშავებს მონაცემებს, რა მიზნით და ვის აქვს მათზე წვდომა.[25]

მომხმარებლების შესაძლებლობა, დააფიქსირონ გარკვეული მოთხოვნები თავიანთი პერსონალური მონაცემების გამოყენების თაობაზე, საკვანძოდაა დამოკიდებული პოლიტიკაზე, რომელიც უნდა იყოს ღია და გამჭვირვალე.[26] პოლიტიკის საჯაროდ განთავსება ყველაზე გავრცელებული გზაა საზოგადოების ინფორმირებისთვის იმის შესახებ, თუ როგორ ხდება მათი მონაცემების დამუშავება, თუმცა ზოგიერთი მომხმარებლისთვის მაინც უცნობია, თუ რა სახის მონაცემების გამოყენება ხდება და რა ფარგლებში.[27] ამდენად, გამჭვირვალობის მოთხოვნა მნიშვნელოვნად არის მხედველობაში მისაღები.

თუმცა ეს ერთადერთი მიზანი ვერ იქნება. მაგალითად, პოლიტიკის შემუშავებით, ორგანიზაცია, ერთი მხრივ, მზაობას გამოთქვამს დამუშავების პროცესის გამჭვირვალობაზე, მეორე მხრივ, არაპირდაპირ ხაზს უსვამს იმას, რომ მონაცემთა დამუშავების მოთხოვნებთან შესაბამისობა მისი ერთ-ერთი მთავარი პრიორიტეტული მიმართულებაა. გარდა ამისა, პოლიტიკის მიზანი შეიძლება იყოს ორგანიზაციაში მომსახურე პერსონალისთვის მონაცემთა დაცვის მნიშვნელობისა და ამ საკითხებისადმი ყურადღების გამახვილება, ეს, თავის მხრივ, ცნობიერების ასამაღლებელ ბერკეტადაც კი შეიძლება ჩაითვალოს. დამატებით, ხაზი უნდა გაესვას იმ გარემოებასაც, რომ მაგალითად, ვებგვერდზე პოლიტიკის დოკუმენტის ასახვით, დადებითი გავლენა ჩნდება მომხმარებლების წარმოდგენებზე, რომ მათი პირადი ცხოვრება არის დაცული.[28] ამდენად, მთლიანობაში პოლიტიკის დოკუმენტის შედგენა, ერთგვარი უპირატესობაა ორგანიზაციის მხრიდან.

---

[25] *Kuner C., Bygrave L. A., Docksey C. (eds),* The EU General Data Protection Regulation (GDPR) Commentary, Oxford University Press, 2020, 415-416.

[26] *Tavani H.,* Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy, 2007, 17.

[27] *Mulder T., Tudorica M.,* Privacy Policies, Cross-Border Health Data and the GDPR, Information & Communications Technology Law, 2019, 5, <https://doi.org/10.1080/13600834.2019.1644068> [20.01.2023].

[28] *Ermakova T., Baumann A., Benjamin F., Krasnova H.,* Privacy Policies and Users' Trust: Does Reliability Matter?, 2014, 2, <https://www.researchgate.net/publication/262563357> [01.20.2023].

პოლიტიკის მიზნებიდან გამომდინარე, შესაძლებელია შეთანხმება მასში ასასახი ინფორმაციის კატეგორიებზე. ეჭვგარეშეა, რომ პოლიტიკა უნდა ქმნიდეს წარმოდგენას, სულ მცირე, შემდეგ საკითხებზე: 1. დამმუშავებლის ვინაობისა და საქმიანობის შესახებ ინფორმაცია; 2. დამმუშავებლის მიერ განსაზღვრული საქმიანობიდან გამომდინარე მონაცემთა შეგროვებისა და გამოყენების მიზნობრიობა; 3. შეგროვებულ მონაცემთა სახეობის და კატეგორიების შესახებ ინფორმაცია; 4. სუბიექტის უფლებებისა და მათი რეალიზაციის გზების შესახებ ინფორმაცია. მაგალითად, ერთ-ერთი რეკომენდაციის თანახმად, პოლიტიკა უნდა ასახავდეს შემდეგ ინფორმაციას მაინც, კერძოდ: რა ინფორმაცია მუშავდება და როგორ; როგორ ხდება მონაცემთა გამოყენება; როგორ ხდება მონაცემთა შენახვა და დაცვა; ორგანიზაციის საკონტაქტო ინფორმაცია; მზა ფაილების – ე. წ. "cookies" („ქუქი") გამოყენების, მონაცემთა ლოგირებისა და მიდევნების სისტემის ("tracking") გამოყენების თაობაზე; მონაცემთა დამუშავებაზე გაცემული თანხმობის უკან გამოხმობის შესახებ არსებული პროცედურა.[29]

სუბიექტის უფლებების დაცვის ნაწილში, სახელმწიფო ინსპექტორის სამსახურმა აღნიშნა, რომ ორგანიზაციაში მონაცემთა სუბიექტის უფლებების რეალიზების უზრუნველსაყოფად მიღებული ზომების შეფასებისას უნდა იყოს გათვალისწინებული: 1. თუ რა პროცესს გადის მონაცემთა სუბიექტის მიერ წარდგენილი განცხადება, რომელიც მის უფლებებს ეხება და არის თუ არა განსაზღვრული პასუხისმგებელი პირი; 2. დადგენილია თუ არა ამგვარ განცხადებაზე რეაგირების წესი წერილობით; 3. ხდება თუ არა განცხადებების პერიოდული ანალიზი და სხვა.[30] შესაბამისად, შესაძლებელია ითქვას, რომ ამ ინფორმაციის პოლიტიკის დოკუმენტში განთავსება დამატებითი ინდიკატორი იქნება იმისა, რომ ორგანიზაციის ერთ-ერთ პრიორიტეტს წარმოადგენს სუბიექტის უფლებებზე ორიენტირება. თუმცა ზემოჩამოთვლილი ნაწილები, რაც შეიძლება იქნეს ასახული პოლიტიკაში, ბუნებრივია, არ გამორიცხავს სხვა დამატებითი ინფორმაციის მითითების შესაძლებლობას, თუ ეს აუცილებელია ორგანიზაციის საქმიანობის სპეციფიკიდან გამომდინარე, ხოლო საზომი ერთეული იმისა, თუ რამდენად ეფექტიანად ასახა ორგანიზაციამ საჭირო ინფორმაცია პოლიტიკაში, არის ერთგვარი თვითშეფასების ტესტი, რომელიც აფასებდეს პოლიტიკას გარეშე პირის პერსპექტივიდან.

დამატებით, მომხმარებლებს ხშირად ესაჭიროებათ საშუალოზე მაღალი ცნობიერების დონე და გარკვევა სამართლებრივ ტერმინოლოგიაში, რათა აღიქვან პოლიტიკით წარმოდგენილი ტექსტი.[31] ამდენად, გასაგები და ცხადი ენით

[29] *Pirzada M.,* Sample Privacy Policy Template, 2022, <https://www.privacypolicies.com/blog/privacy-policy-template/#Examples_Of_Useful_Clauses_For_Your_Privacy_Policy> [20.01.2023].
[30] *სახელმწიფო ინსპექტორის სამსახური,* თვითშეფასების კითხვარი, 2021, 8.
[31] *Ermakova T., Baumann A., Benjamin F., Krasnova H.,* Privacy Policies and Users' Trust: Does Reliability Matter?, 2014, 1, <https://www.researchgate.net/publication/262563357> [01.20.2023].

ფორმულირება ერთ-ერთი პრიორიტეტული მოთხოვნაა. ამასთან კავშირშია, ასევე, ისიც, რომ გარკვეული პროდუქტის თუ მომსახურების მომხმარებელი, შესაძლებელია, ასევე, იყოს არასრულწლოვანი პირი, რომელსაც გონებრივი განვითარებიდან გამომდინარე, არ გააჩნია ინფორმაციის აღქმის სრულყოფილი უნარი. ამდენად, მონაცემთა დამუშავების შესახებ ინფორმაცია, უნდა იყოს მიწოდებული მეტად ადაპტირებული ფორმით, მაგალითად, ორგანიზაციამ შესაძლოა, შესთავაზოს მომხმარებელს პოლიტიკის სტანდარტული და ადაპტირებული ვერსიები. ამასთან დაკავშირებით, საფრანგეთის პერსონალურ მონაცემთა სახელმწიფო საზედამხედველო ორგანოს (CNIL) რეკომენდაციის თანახმად, არასრულწლოვანთა ინფორმირების უფლების გაძლიერების მიზნით, ონლაინ მომსახურების მიმწოდებლები უნდა აწვდიდნენ პოლიტიკას და მომსახურების პირობებს იმგვარად, რომ იგი შესაბამისი იყოს არასრულწლოვანთათვის (სიცხადე, სიმარტივე, მიმზიდველობა). მონაცემთა დაცვის კუთხით გადაწყვეტილების მიღების მარტივად შეთავაზების პირობა და გარკვეული სერვისების გათიშვის შესაძლებლობა, როგორიცაა ადგილმდებარეობის მონაცემთა დამუშავება, უნდა იყოს დანერგილი.[32]

4. პოლიტიკის დოკუმენტის შემუშავებისა და ამოქმედების ასპექტები

პოლიტიკა ნებისმიერი ორგანიზაციის აუცილებლად დასამტკიცებელ წესთა სიას უნდა მიეკუთვნებოდეს, იქნება ეს საჯარო თუ კერძო დაწესებულება, საქმიანობის განხორციელების მიუხედავად. პოლიტიკა უნდა ასახავდეს ორგანიზაციაში არსებულ მიმდინარე პროცესებს. აქედან გამომდინარე, პოლიტიკის დოკუმენტის ფორმირების შემდეგ, ის მუდმივი განახლების ციკლს ექვემდებარება, რომელიც შემდეგი თანმიმდევრობით ვლინდება: ინფორმაციის შეგროვება დამუშავების პროცესების თაობაზე, შეგროვებულ მონაცემთა ანალიზი, პოლიტიკის პირველადი ვერსიის შემუშავება და შიდაორგანიზაციული კონსულტირებები, პოლიტიკის დამტკიცება, მისი შესრულება და პერიოდული რევიზია.

4.1. ინფორმაციის შეგროვება და ანალიზი

თავდაპირველად, პოლიტიკის დოკუმენტის ფორმირების მიზნით, უნდა იდენტიფიცირდეს ორგანიზაციაში არსებული დამუშავების ყველა მიზანი და შეგროვებულ მონაცემთა სახეობები, ასევე, კატეგორიები. მათი იდენტიფიცირებისთვის, აუცილებელია, თითოეული სტრუქტურული ერთეულის ფარგლებში მოხდეს დამუშავების მიზნებისა და შეგროვებული მონაცემების ანალიზი. ასევე,

[32] *CNIL,* Recommandation 6: renforcer l'information et les droits des mineurs par le design, 2021, <https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design> [20.01.2023].

მნიშვნელოვანია, რომ ერთმანეთისგან გაიმიჯნოს ძირითადი და ე. წ. „გამომდინარე მიზნები“, რომელიც, თავის მხრივ, შესაძლოა არ საჭიროებდეს დოკუმენტში ასახვას, ვინაიდან, ძირითადი მიზნები მოიცავს მათ. ორგანიზაციამ უნდა აღწეროს მასთან არსებული ყველა ელექტრონული სისტემა, პროცესი, რომლის მეშვეობითაც ხდება მონაცემთა დამუშავება, ასევე, უნდა გაკეთდეს, ელექტრონულ სისტემაში დამუშავებული მონაცემების აღნუსხვა, მონაცემთა შეგროვების წყაროთა იდენტიფიცირება.[33]

ასევე, მნიშვნელოვანია, რომ იდენტიფიცირებული მიზნების ასახვა პოლიტიკაში არ მოხდეს ზოგადად და ბუნდოვნად. მეორე მხრივ, არც უკიდურესი დეტალიზება იქნება გამართლებული, ვინაიდან, როგორც აღინიშნა, პოლიტიკის დოკუმენტის მიზანი არის წარმოდგენის შექმნა არსებული პროცესების თაობაზე და არა დამუშავების პროცესის დეტალური აღწერა. ამასთანავე, რაც მეტად დამოკიდებულია ორგანიზაციის საქმიანობა პერსონალურ მონაცემთა დამუშავებაზე, მით მეტად არის აუცილებელი დამუშავების პროცესის ამა თუ იმ ასპექტების მითითება.

ინფორმაციის შეგროვების მიზნებისთვის, შესაძლებელია სხვადასხვა მეთოდის გამოყენება, მაგალითად, თითოეული სტრუქტურული ერთეულისთვის საგანგებოდ შედგენილი კითხვარის მიწოდება, მათი შემდგომი შევსების მიზნით. აქვე, გასათვალისწინებელია ისიც, რომ ეს კითხვარი არ უნდა იყოს შედგენილი რთული ტერმინოლოგიის ან იურიდიული ლექსიკის გამოყენებით, ვინაიდან, ეს შესაძლოა შემაფერხებელი ფაქტორი აღმოჩნდეს მათთვის, ვისაც არ გააჩნია შესაბამისი პროფესიული ცოდნა, რაც, თავის მხრივ, გამოიწვევს არასასურველ შედეგს პოლიტიკის შედგენაზე პასუხისმგებელი პირისთვის.

კითხვარის შედეგად მოპოვებული ინფორმაციის შემდგომ, უნდა მოხდეს მათი ანალიზი, რაც მოიცავს ასახული ინფორმაციის ვარგისიანობის შეფასებას, მათი ხარისხის შემოწმების გზით. თუ კითხვარი შეიცავს ზოგად ინფორმაციას, მიზანშეწონილია, მოხდეს მათი დაზუსტება ან დეტალიზება, რათა საბოლოო პოლიტიკისთვის იყოს გამოსადეგი. მიუხედავად იმისა, რომ პოლიტიკაში პროცესები არ უნდა აღიწეროს დეტალურად, უშუალოდ კითხვარის შევსებისას, მიზანშეწონილია გამოყენებულ იქნას რაც შეიძლება დეტალიზებული ენა, რათა შემდგომ პოლიტიკის შედგენაზე პასუხისმგებელმა პირმა, განასხვაოს პირველხარისხოვანი, მეორეხარისხოვანი და არარელევანტური ინფორმაცია.

[33] *სახელმწიფო ინსპექტორის სამსახური,* თვითშეფასების კითხვარი, 2021, 2.

4.2. პოლიტიკის დოკუმენტის დამტკიცება

როგორც წესი, პოლიტიკის დამტკიცების პროცედურა რაიმე განსხვავებულ მოთხოვნას არ შეიცავს. ის, როგორც ნებისმიერი დოკუმენტი, რომელიც მიღებულია ორგანიზაციაში, საჭიროებს შიდაორგანიზაციული პროცედურების შესაბამისად დამტკიცებას. თუმცა დამტკიცების პროცედურამდე, მნიშვნელოვანია, რომ პოლიტიკის ე. წ. პირველადი, სამუშაო ვერსია მაქსიმალურად გაზიარდეს შიდაორგანიზაციულად, გაცნობისა და შენიშვნების თანდართვის მიზნით. გარდა ამისა, მნიშვნელოვანია, პოლიტიკის შემუშავების პროცესი ადმინისტრირებული იყოს ცენტრალიზებულად, სხვა სიტყვებით, შესაბამისი პასუხისმგებელი პირის მიერ, რომელიც იქნება სათანადო კომპეტენციის მქონე პოლიტიკის შედგენის მხრივ.

დამტკიცების შემდგომ, აუცილებელია, პოლიტიკის საჯაროდ გაზიარება, ვინაიდან ეს აუცილებელი პირობაა გამჭვირვალობის მოთხოვნის დასაკმაყოფილებლად. ასევე, გასათვალისწინებელია ვებგვერდზე გასაჯაროების ისეთი დეტალური საკითხები, როგორიცაა მარტივად ხელმისაწვდომ ადგილზე განთავსება და თუ ვებგვერდი მომხმარებელს სთავაზობს სხვადასხვაენოვან მომსახურებას, პოლიტიკის შესაბამისი თარგმანის გასაჯაროებაც. აქვე, უნდა აღინიშნოს, მცდარია წარმოდგენა იმის შესახებ, რომ თუ პოლიტიკა თავსდება ვებგვერდზე, ის მხოლოდ ვებგვერდის მეშვეობით მონაცემთა დამუშავებას უნდა ეხებოდეს.

4.3. პოლიტიკის შესრულება და რევიზია

მას შემდეგ, რაც პოლიტიკა დამტკიცდება, მნიშვნელოვანია მასში ასახული დებულებების გათვალისწინება და დაცვა. ზოგადად, პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები გამოირჩევა სპეციფიკურობით, ამდენად, მნიშვნელოვანია, რომ პერსონალურ მონაცემთა დაცვის პოლიტიკის ადმინისტრირება მოხდეს შესაბამისი პასუხისმგებელი პირის მიერ. როგორც წესი, ამ პირს ეწოდება პერსონალურ მონაცემთა დაცვის ოფიცერი, რომლის სავალდებულო დანიშვნის/განსაზღვრის პირობა, რიგ შემთხვევებში, გათვალისწინებულია მონაცემთა დაცვის საერთო რეგულაციით (GDPR).[34] გარდა ამისა, გამართლებულია, რომ პოლიტიკის შესრულებაზე კონტროლი არ მოხდეს სხვადასხვა პირის მიერ, რამდენადაც ამან შესაძლოა, გავლენა იქონიოს მისი აღსრულების ეფექტიანობაზე. ამდენად, ორგანიზაციაში პერსონალურ მონაცემთა დაცვის ოფიცრის განსაზღვრა პოზიტიური შედეგების მომტანია საბოლოო მიზნებისთვის.

როგორც საჯაროდ განთავსებული, ისე მონაცემთა დაცვის შიდაორგანიზაციული სტანდარტების რევიზია, მიზანშეწონილია, მოხდეს რეგულარულად. რევიზიის პირველ ეტაპზე აუცილებელია დამუშავების არსებული მიდგომებისა და რისკების შეფასება,

[34] იხ. მონაცემთა დაცვის საერთო რეგულაცია (GDPR), მუხლი 37.

რასაც პერსონალურ მონაცემთა დაცვის სფეროში, ეწოდება "DPIA" ("Data Protection Impact Assessment").[35] თავისი არსით, "DPIA" არის პროცესი, რომელიც ეხმარება ორგანიზაციას მონაცემთა დამუშავების მიმდინარეობისას არსებული რისკების იდენტიფიცირებასა და აღმოფხვრაში.

პოლიტიკის რევიზიის მიზნებიდან გამომდინარე, პირველ რიგში, უნდა მოხდეს დამუშავების არსებული პროცესის აღწერა და ამ მიზნით, შესაბამის სტრუქტურულ ერთეულებთან კონსულტაციის საჭიროების დადგენა. შემდეგ ეტაპზე პერსონალურ მონაცემთა დაცვის ოფიცრის მიერ უნდა შეფასდეს დამუშავების საშუალებებისა და ფორმების თავსებადობა მისაღწევ მიზნებთან, ასევე, შეგროვებულ მონაცემთა პროპორციულობა და ადეკვატურობა. პარალელურად, აუცილებელია საკანონმდებლო სიახლეებთან თავსებადობის უზრუნველყოფა, რაც საშუალებას მისცემს ორგანიზაციას დამუშავების პროცესი გახადოს თავსებადი შეცვლილ საკანონმდებლო მოთხოვნებთან. ამ პროცესის შემდგომი განვითარების ეტაპია არსებული ცვლილებების ინტეგრირება დამუშავების პროცესებსა და უშუალოდ, მარეგულირებელ დოკუმენტებში, მათ შორის, პოლიტიკაში.

5. პოლიტიკის სავარაუდო შინაარსი ზოგიერთი კომპანიის მაგალითზე

როგორც აღინიშნა, პოლიტიკა უკიდურესად მოქნილი სტრუქტურის მქონე უნდა იყოს. მისი შინაარსი დამოკიდებულია ორგანიზაციის წინაშე არსებულ გამოწვევებსა და საჭიროებებზე, ასევე, შესაბამის სახელმწიფოში დადგენილ სამართლებრივ მოთხოვნებზე.

იმისთვის, რათა თვალსაჩინო იყოს, თუ როგორია უცხო ქვეყნებში დაფუძნებული კომპანიების პოლიტიკის დოკუმენტები, წინამდებარე თავში განხილულია რამდენიმე ორგანიზაცია, დაფუძნებული როგორც ევროკავშირის, ისე ამერიკის შეერთებული შტატების ტერიტორიაზე. მაგალითები ეყრდნობა შემდეგ კომპანიებს: "Telefónica", "Deutsche Bank", "Bank of America" და "Google". ეს კომპანიები შერჩეულია როგორც ცნობადობის, ისე საქმიანობის განსხვავებული სპეციფიკიდან გამომდინარე, ასევე, სამართლებრივი რეგულირების თავისებურებათა გათვალისწინებით. სტატიის ფორმატიდან გამომდინარე, ამ დოკუმენტების დეტალური განხილვა ვერ მოხდება, არამედ აქცენტი გაკეთდება მხოლოდ საკვანძო მნიშვნელობის დანაწესებზე.

თავდაპირველად უნდა აღინიშნოს, რომ თითოეული ზემოხსენებული კომპანიის პოლიტიკა გამოირჩევა სიცხადით, მარტივი ენითა და აკმაყოფილებს დამუშავების გამჭვირვალობისთვის დადგენილ მოთხოვნას. აღსანიშნავია, რომ გამჭვირვალობა,

[35] იხ. მონაცემთა დაცვის საერთო რეგულაცია (GDPR), მუხლი 35.

აუცილებელი წესით, არ მოითხოვს ამ დოკუმენტში თითოეული პროცესის დეტალურ გაწერას, არამედ, აქ მთავარი აქცენტი კეთდება იმაზე, თუ რამდენად აძლევს პოლიტიკა სუბიექტს იმის საშუალებას, რომ წარმოდგენა ჰქონდეს დამუშავების ყველა შესაძლო ასპექტზე.

“Telefónica” კომპანია დაფუძნებულია ევროკავშირში, კერძოდ, ესპანეთში. ის სატელეკომუნიკაციო და მობილური კავშირგაბმულობის მომსახურებას ახორციელებს. კომპანიის პოლიტიკის დოკუმენტი[36] იწყება პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის მიმართ კომპანიის მიერ განსაკუთრებული მნიშვნელობის ხაზგასმით, ხოლო ვებგვერდზე შესვლისთანავე, ჩნდება ცალკე ფანჯარა, სადაც მითითებულია ე. წ. “cookie” ფაილების დამუშავების თაობაზე და სუბიექტისთვის შეთავაზებულია ამ მონაცემთა დამუშავების არჩევის შესაძლებლობა.

პოლიტიკის შემდეგი ნაწილები ეთმობა გამჭვირვალობასა და დამუშავების უსაფრთხოებაზე ხაზგასმას. ასევე, მოცემულია განმარტებები, როგორიცაა: თუ ვინ არის დამმუშავებელი, რა მონაცემები მუშავდება, მათ შორის, სუბიექტთა განაცხადების დამუშავებისთვის, ბიზნეს საქმიანობისთვის, სიახლეების შეტყობინებისთვის, სოციალური გვერდის მეშვეობით კომუნიკაციისთვის, მონაცემთა ანალიტიკისთვის, ვებგვერდის მეშვეობით მონაცემთა დამუშავებისთვის. პოლიტიკა, ასევე, შეიცავს ინფორმაციას მონაცემთა შენახვის ვადების, მონაცემთა მიმღებებისა და საერთაშორისო გადაცემის თაობაზე. რაც შეეხება უფლებებს, დოკუმენტში მოცემულია ინფორმაცია თანხმობის გამოხმობის, წვდომის უფლების, შეცვლის მოთხოვნის უფლების, წაშლის უფლების, დაბლოკვის უფლების, გასაჩივრების, პორტირებისა და ავტომატიზებული გადაწყვეტილების გასაჩივრების უფლების შესახებ.

“Deutsche Bank” კომპანია დაფუძნებულია გერმანიაში, მისი საქმიანობა მოიცავს საბანკო-საფინანსო სექტორს. კომპანიის ვებგვერდზე შესვლისას, ჩნდება ფანჯარა, რომელიც მომხმარებელს აცნობს ე. წ. “cookie” ფაილების გამოყენების თაობაზე და სთავაზობს არჩევანს ამ მიმართულებით მონაცემთა დამუშავების კუთხით. აღსანიშნავია, რომ მომხმარებლისთვის ე. წ. “cookie” ფაილების დამუშავების თვალსაზრისით არჩევანის მიცემის შესაძლებლობა განსაკუთრებით მნიშვნელოვანი გახდა მას შემდეგ, რაც ამოქმედდა მონაცემთა დაცვის საერთო რეგულაცია (GDPR).

კომპანიის მონაცემთა დაცვის პოლიტიკა[37] მსგავსად, შეიცავს განაცხადს, სადაც ხაზგასმულია, თუ როგორი მნიშვნელოვანია კომპანიისთვის მონაცემთა დაცვა და როგორ ზრუნავს იგი მონაცემთა უსაფრთხოებაზე.

[36] <https://www.telefonica.com/en/privacy-policy/> [12.01.2023].

[37]<https://www.db.com/legal-resources/privacy-notice#:~:text=We%20collect%2C%20process%2C%20and%20use,information%20and%20online%20banking%20applications> [12.01.2023].

პოლიტიკის ძირითადი პუნქტები ეთმობა მონაცემთა ე. წ. „თრექინგს“, რომელიც, ძირითადად, ეხება ვებგვერდის მეშვეობით მონაცემთა დამუშავებას, ასევე, მონაცემთა შენახვის საკითხებს, ფსევდონიმიზაციას, ადგილმდებარეობის შესახებ მონაცემებს.

აღსანიშნავია, რომ პოლიტიკა ცალკე განმარტებას აკეთებს სისტემის ფუნქციონირების შესახებ ინფორმაციაზე, რის მიხედვითაც განმარტებულია, რომ კომპანია ამუშავებს მონაცემებს იმ სისტემის თაობაზე, რომლითაც განხორციელდა ვებგვერდზე წვდომა, მათ შორისაა: ეკრანის გაფართოება, ოპერაციული სისტემა და ინტერნეტბრაუზერი, ქსელისა და კავშირის შესახებ ინფორმაცია, გამოყენებული მოწყობილობა, “cookie”-ს შესახებ ინფორმაცია, ენა, დომეინი, IP მისამართი. გარდა ამისა, ბანკი აღნიშნავს, რომ ვებგვერდი შეიცავს ბმულებს სოციალურ ქსელებთან, როგორიცაა: “Facebook”, “Instagram”, “LinkedIn”.

აღსანიშნავია ისიც, რომ დოკუმენტი შეიცავს დეტალურ ჩანაწერებს “cookie” ფაილებთან მიმართებით, მათ შორის, აღწერილია, თუ რომელი ფაილია გამოყენებული, რა მიზანს ემსახურება თითოეული მათგანი და რამდენად აუცილებელია მათი დამუშავება. დამატებით, მოცემულია ინფორმაცია ამ ფაილების დამუშავების კონტროლთან დაკავშირებით სუბიექტის მიერ.

“Bank of America” კომპანია დაფუძნებულია ამერიკის შეერთებულ შტატებში, ხოლო მისი საქმიანობა მოიცავს საბანკო-საფინანსო სექტორს. განსხვავებით განხილული ორი კომპანიისგან, ამ ორგანიზაციის ვებგვერდზე შესვლისას, ის მომხმარებელს არ სთავაზობს “cookie” ფაილებთან დაკავშირებულ ინფორმაციას პროაქტიულად, ასევე, არჩევანის შესაძლებლობას, თუ რომელი მათგანი დამუშავდეს. ეს გასაგებიცაა, ვინაიდან აშშ-ის მასშტაბით არ არსებობს მსგავსი ინფორმაციის პროაქტიულად წარდგენის ვალდებულება.

მიუხედავად იმისა, რომ ამ კომპანიაზე არ ვრცელდება მონაცემთა დაცვის საერთო რეგულაცია (GDPR), მისი პოლიტიკის დოკუმენტი, შეიძლება ითქვას, რეგულაციით დადგენილი მოთხოვნების შესაბამისად აწვდის მომხმარებელს ინფორმაციას. დოკუმენტი საკმარისად ინფორმაციულია და შეიცავს მონაცემებს იმის თაობაზე, თუ რომელ სოციალურ მედია პლატფორმებს იყენებს ორგანიზაცია მონაცემთა დამუშავებისას (“Facebook”, “Twitter”, “YouTube”, “LinkedIn”), როგორია დაცვისა და უსაფრთხოების ზომები, როგორ ხდება მონაცემთა შეგროვება, რა მონაცემები გროვდება, როგორ გამოიყენება, ვისთან ხდება მონაცემთა გაზიარება. ასევე, ცალკე არის გაკეთებული ჩანართი ფიზიკური პირის ჯანმრთელობასთან დაკავშირებული მონაცემების თაობაზე. გარდა ამისა, ცალკე ჩანაწერი ეთმობა მიზნობრივ რეკლამირებას, სადაც განმარტებულია, თუ როგორ ხდება რეკლამებისთვის სამიზნე აუდიტორიის განსაზღვრა და როგორ არის შესაძლებელი სარეკლამო შეტყობინებების მიღების მომსახურებაზე უარის თქმა.

“Google” კომპანია რეგისტრირებულია ამერიკის შეერთებულ შტატებში, ხოლო მისი საქმიანობა მოიცავს ინტერნეტზე დაფუძნებულ მომსახურებებს. უპირველესად, უნდა ითქვას, რომ განსხვავებით განხილული პოლიტიკის დოკუმენტებისგან, ამ კომპანიის მონაცემთა დაცვის პოლიტიკა[38] გამოირჩევა მოცულობითა და დეტალიზაციით. ეს მარტივად გასაგებიცაა, ვინაიდან ამ კომპანიის მიერ, მომსახურებების მიწოდებისას, პერსონალური მონაცემების დამუშავება განსაკუთრებული სიხშირითა და მოცულობით ხდება. ასევე, ხაზგასასმელია ისიც, რომ თავად პოლიტიკაში არის არაერთი გადამისამართება სხვა წყაროებზე, რომელიც დამატებით ინფორმაციას აწვდიან სუბიექტს მონაცემთა დამუშავების თაობაზე, მაგალითად, როგორიცაა ინტერნეტბრაუზერთან დაკავშირებული უნიკალური იდენტიფიკატორები, აპლიკაციების ე. წ. „ქეშირებული მონაცემები“ და ა. შ.

სხვა მხრივ, დოკუმენტი შეიცავს ინფორმაციას სუბიექტის მიერ მიწოდებული მონაცემების თაობაზე, როგორიცაა: ნანახი ვიდეოების, ხმის, შესყიდვების შესახებ, იმ ადამიანების შესახებ ინფორმაცია, რომლებთანაც ხდება კონტენტის გაზიარება, ვებგვერდზე ვიზიტების ისტორია, რომელიც სინქრონიზებულია “Google”-ის ანგარიშთან, შეტყობინებებისა და ზარების სახეობები და მოცულობა. მნიშვნელოვანია აღინიშნოს, რომ მეტი თვალსაჩინოებისთვის, დოკუმენტში მოცემულია კონკრეტული მაგალითები, რათა დამუშავების შესახებ ინფორმაცია გახადოს მეტად აღქმადი.

შეგროვებული ინფორმაციის გარდა, მითითებაა გაკეთებული იმაზე, თუ რატომ გროვდება ინფორმაცია და რა მიზნებისთვის. ცალკე ხაზგასმულია გარემოებები, რის დროსაც “Google” არ უზიარებს მესამე პირებს ინფორმაციას. პოლიტიკის დოკუმენტის თანახმად, ის მომხმარებლებს არ სთავაზობს პერსონიფიცირებულ რეკლამებს, რომელიც დაფუძნებულია განსაკუთრებული კატეგორიის მონაცემებზე, როგორიცაა: რასა, რელიგია, სექსუალური ორიენტაცია ან ჯანმრთელობა. ასევე, პერსონიფიცირებული რეკლამები არ ფორმირდება იმ კონტენტიდან გამომდინარე, რომელიც ატვირთულია მომხმარებლის ღრუბლოვან სისტემაში, ელფოსტასა ან ფოტოებში. ასევე, პოლიტიკაში აღნიშნულია, რომ “Google” არ აზიარებს ინფორმაციას რეკლამის განმახორციელებლებთან იმგვარად, რომ პირი იყოს იდენტიფიცირებული, გარდა იმ შემთხვევისა, როდესაც თავად მომხმარებელი ითხოვს ამას.

განხილული პოლიტიკების შეჯამებისას, შეიძლება ითქვას, რომ როგორც ამერიკაში, ისე ევროპაში დაფუძნებული კომპანიები სათანადო ყურადღებას უთმობენ მომხმარებლის ინფორმირებას და აწვდიან მას ყველა ინფორმაციას, რომელიც აუცილებელია სუბიექტისთვის. სხვა საკითხია, თუ რამდენად გამართულია, მაგალითად, “Google”-ის ან სხვა განხილული კომპანიის პოლიტიკა რეგულაციის დებულებებთან

[38] <https://policies.google.com/privacy?hl=en-US> [12.01.2023].

მიმართებით, თუმცა ეს დამოუკიდებელი კვლევის საგანია, რომელსაც, ბუნებრივია, ამ სტატიაში ვერ შევეხებით.

6. დასკვნა

წინამდებარე სტატიაში განხილული საკითხებიდან გამომდინარე, აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის პოლიტიკა საყურადღებო და მნიშვნელოვანია ნებისმიერი კომპანიისთვის. როგორც არაერთხელ აღინიშნა, მონაცემთა სუბიექტის წინაშე დამუშავების პროცესის გამჭვირვალობის უზრუნველყოფის მოთხოვნა, მათ შორის, მოიცავს მონაცემთა დაცვის პოლიტიკის შემუშავებასა და მის საჯაროდ განთავსებას.

პოლიტიკაში ასასახი ინფორმაცია განსხვავებულია თითოეული კომპანიის საქმიანობის სპეციფიკიდან გამომდინარე, შესაბამისად, არ არსებობს საყოველთაოდ შეთანხმებული, ერთიანი სტრუქტურა, რის შესაბამისადაც უნდა ჩამოყალიბდეს პოლიტიკა.

ამისგან განსხვავებით, პოლიტიკის შედგენის მიზნით ინფორმაციის შეგროვების პროცესი შეიძლება მსგავსი იყოს სხვადასხვა ორგანიზაციაში, იმ გაგებით, რომ მონაცემთა დამუშავების პროცესის იდენტიფიცირების გზები და ეტაპები მეტ-ნაკლებად თანაბარ მიდგომას შეიძლება ეფუძნებოდეს, როგორიცაა, შესაბამისი კითხვარების გამოყენება ინფორმაციის შეგროვებისთვის, კონსულტირება და ა. შ.

პოლიტიკის შემუშავებისა და მის შესაბამისად მონაცემთა დამუშავების წარმოებაზე დადებითი გავლენა უდავოდ ექნება პერსონალურ მონაცემთა დაცვის ოფიცერს, რომელიც ცენტრალიზებული ფორმით უზრუნველყოფს კომპანიაში არსებული საკითხების მართვას. შესაბამისად, მისი მონაწილეობა პოლიტიკის შემუშავებაში საკვანძო მნიშვნელობის მქონეა.

როგორც აღინიშნა, პოლიტიკის შემუშავებისთვის განსაზღვრული პირდაპირი საკანონმდებლო მოთხოვნა არ არსებობს. მიუხედავად ამისა, რიგი ნორმები არაპირდაპირ განსაზღვრავს პოლიტიკის დამტკიცების ვალდებულებას. ამავდროულად, პოლიტიკის შემუშავების მიმართულებით წამახალისებელი ნაბიჯები შეიძლება გადაიდგას პერსონალურ მონაცემთა დაცვის სამსახურის მიერ, მაგალითად, ამ საკითხის პოპულარიზების მიზნით კამპანიის გამართვის გზით.

მეორე მხრივ, შეიძლება გარკვეული საკანონმდებლო ცვლილებების შემუშავებაც, რის მიხედვითაც გარკვეული კატეგორიის კომპანიებისთვის პოლიტიკის შემუშავება და საჯაროდ განთავსება სავალდებულო იქნება. ასევე, დაწესდება ვალდებულება, რომ რიგი კომპანიების რეგისტრაციისთვის, მარეგისტრირებელ ორგანოში სავალდებულო

გახდეს პოლიტიკის წარდგენა, რომლის გარეშეც, რეგისტრაციის განაცხადი ხარვეზიანად მიიჩნევა, ხოლო პოლიტიკაში მისათითებელი ინფორმაცია კი, შეიძლება საკანონმდებლო აქტით ან პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანების საფუძველზე დადგინდეს.

ბიბლიოგრაფია:

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, 6391-Iს, 05/06/2012.
2. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
3. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი, № 07-3/353/9, 22/05/2019.
4. *სახელმწიფო ინსპექტორის სამსახური,* თვითშეფასების კითხვარი, 2021, 2, 7, 8, 13.
5. CalOPPA, Business and Professions Code – BPC 22575, 01/01/2014.
6. Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
7. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), *OJ L 119, 4/5/2016, 89–131.*
8. 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 L 119, 4/5/2016, 1–88.*
9. *Ermakova T., Baumann A., Benjamin F., Krasnova H.,* Privacy Policies and Users' Trust: Does Reliability Matter?, 2014, 1, 2, <https://www.researchgate.net/publication/262563357> [01.20.2023].
10. *Hert P. D., Gutwirth S.,* Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action, 2009, 7.
11. *Kuner C., Bygrave L. A., Docksey C. (eds),* The EU General Data Protection Regulation (GDPR) Commentary, Oxford University Press, 2020, 415, 416.

12. *Mulder T., Tudorica M.,* Privacy Policies, Cross-Border Health Data and the GDPR, Information & Communications Technology Law, 2019, 5, <https://doi.org/10.1080/13600834.2019.1644068> [20.01.2023].
13. *Pirzada M.,* Sample Privacy Policy Template, 2022, <https://www.privacypolicies.com/blog/privacy-policy-template/#Examples_Of_Useful_Clauses_For_Your_Privacy_Policy> [20.01.2023].
14. *Tavani H.,* Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy, 2007, 17.
15. *Waldman A. E.,* Privacy, Notice and Design, Stanford Technology Law Review, 2018, 80, 90.
16. *CNIL,* Recommandation 6: renforcer l'information et les droits des mineurs par le design, 2021, <https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design> [20.01.2023].
17. <https://www.telefonica.com/en/privacy-policy/> [12.01.2023].
18. <https://www.db.com/legal-resources/privacy-notice#:~:text=We%20collect%2C%20process%2C%20and%20use,information%20and%20online%20banking%20applications> [12.01.2023].
19. <https://policies.google.com/privacy?hl=en-US> [12.01.2023].

თამარ შუდრა*

ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში

ყველა ბავშვს აქვს მისი ძირითადი უფლებებისა და თავისუფლებების დაცვისა და პატივისცემის უფლება როგორც ჩვეულებრივ, ასევე ციფრულ გარემოში. შესაბამისად, ასაკისა და დამუშავების პლატფორმის მიუხედავად, დაცული უნდა იყოს მათი პირადი ცხოვრების ხელშეუხებლობა და პერსონალური მონაცემები.

ევროპული და ამერიკული საკანონმდებლო ნორმები (ზოგ შემთხვევაში, ასევე სასამართლო პრაქტიკა) ბავშვის პირადი ცხოვრების დაცვის მთავარ ფიგურად მშობელს მოიაზრებს, რადგან მას აქვს ბავშვის ინფორმაციის დამუშავებაზე ექსკლუზიური კონტროლის უფლება. საკანონმდებლო ნორმები, როგორც წესი, არ არეგულირებს მშობლების მიერ შვილის პერსონალური მონაცემების დამუშავების სამართლებრივ ასპექტებს მშობლის მხრიდან შვილის უფლებების შეზღუდვის ჭრილში. აღნიშნული ნაწილობრივ გამოწვეულია საზოგადოებაში დამკვიდრებული შეხედულებით, რომ მშობლის მოქმედებები ყოველთვის განპირობებულია ბავშვის საუკეთესო ინტერესით, ასევე იმ ფაქტორით, რომ „გაციფრულებული ბავშვები“ ჯერ კიდევ პატარები არიან და იურიდიულ წრეებში ციფრულ გარემოში მშობლების მიმართ მათი უფლებების დაცვის საკითხებზე მსჯელობა ჯერ არ დაწყებულა.

სასამართლო პრაქტიკა ადასტურებს, რომ „მშობლის თვალით“ დანახული ბავშვის საუკეთესო ინტერესი ყოველთვის არ არის თანხვედრაში „შვილის თვალით“ აღქმულ საუკეთესო ინტერესთან. შესაბამისად, თანამედროვე ეპოქაში გამოიკვეთა მშობლებისა და არასრულწლოვანი შვილების განსხვავებული მოლოდინები და შეხედულებები ციფრულ გარემოში არასრულწლოვანთა პერსონალური

* ნიუ ვიჟენ უნივერსიტეტის სამართლის სკოლის დოქტორანტი; შავი ზღვის საერთაშორისო უნივერსიტეტის მოწვეული ლექტორი, იურიდიული სამსახურის უფროსი.

მონაცემების დაცულობის ასპექტში. წინამდებარე კვლევა მიზნად ისახავს იმგვარი მექანიზმების განხილვას, რომლებიც არასრულწლოვანთა პერსონალური მონაცემების დაცვის გზით უზრუნველყოფს ციფრულ გარემოში მშობლებისა და არასრულწლოვანი შვილების მოლოდინების მართებულ ფორმირებას.

საკვანძო სიტყვები: *პერსონალური მონაცემები, არასრულ წლოვანი, ციფრული გარემო, თანხმობა.*

1. შესავალი

პერსონალური მონაცემი თანამედროვე ეპოქის ახალი ვალუტაა. მისი მონეტარული ღირებულება მზარდია და მრავალი კომპანიისათვის მნიშვნელოვან აქტივს წარმოადგენს.[1] დღევანდელ ეპოქაში პერსონალური მონაცემი ნავთობსაც კი შეედრება – იგი ღირებულია, თუმცა გადამუშავების გარეშე გამოუსადეგარი.[2]

სწორედ ამ „ნავთობის“ მოპოვებაზე ორიენტირებული კომპანიების „ობიექტებს“ წარმოადგენს ინდივიდი და მისი არასრულწლოვანი შვილი, რომელთა პრივატულობის საკითხი, განსაკუთრებით კი ტექნოლოგიურ შესაძლებლობების განვითარების ფონზე, კითხვის ნიშნის ქვეშ დგას. სიტუაციას კიდევ უფრო ამძაფრებს არასრულწლოვანთა მხრიდან საინფორმაციო ტექნოლოგიების გამოყენების მაღალი ამპლიტუდა[3] და ამ მიმართულებით საგანგაშო სტატისტიკა.[4]

რამდენადაც ყველა ბავშვს აქვს მისი (ადამიანის) ძირითადი უფლებებისა და თავისუფლების დაცვისა და პატივისცემის უფლება როგორც ჩვეულებრივ, ასევე

[1] *Schwartz P. M.,* Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2004, 2056, <https://www.jstor.org/stable/4093335> [27.06.2022].

[2] *Joshua N.,* Why do People Still Think Data is the New Oil? Center for Data Innovation, 2018, <https://www.datainnovation.org/2018/01/why-do-people-still-think-data-is-the-new-oil/> [27.06.2022].

[3] მსოფლიოს მასშტაბით, ყოველი სამი ინტერნეტ მომხმარებლიდან ერთი არასრულწლოვანია. იხ. *Macenaite M., Kosta E.,* Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?, Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, Netherlands, 146, 2017, <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096> [27.06.2022].

[4] *Office for Children's Commissioner for England*, Children's Commissioner's Report Calls on Internet Giants and Toy Manufacturers to be Transparent About Collection of Children's Data, 2018, <https://www.childrenscommissioner.gov.uk/2018/11/08/childrens-commissioners-report-calls-on-internet-giants-and-toy-manufacturers-to-be-transparent-about-collection-of-childrens-data/#:~:text=The%20report%20calls%20on%20companies,collected%20and%20for%20what%20purposes> [27.06.2022].

ციფრულ გარემოში,[5] ასაკის და დამუშავების პლატფორმის მიუხედავად, დაცული უნდა იყოს მათი პირადი ცხოვრების ხელშეუხებლობა და პერსონალური მონაცემები.[6]

როგორც ევროპული[7], ასევე ამერიკული[8] საკანონმდებლო ნორმები ბავშვის პირადი ცხოვრების დაცვის მთავარ ფიგურად მშობელს მოიაზრებს.[9] თუმცა საკანონმდებლო დონეზე, როგორც წესი, არ არის მოწესრიგებული მშობლების მიერ შვილის პერსონალური მონაცემების დამუშავების სამართლებრივი ასპექტები მშობლის მხრიდან შვილის უფლებების შეზღუდვის ჭრილში. სასამართლო პრაქტიკა[10] ადასტურებს, რომ „მშობლის თვალით“ დანახული ბავშვის საუკეთესო ინტერესი ყოველთვის არ არის თანხვედრაში ,,შვილის თვალით“ დანახულ მის (ბავშვის) საუკეთესო ინტერესთან. შესაბამისად, თანამედროვე ეპოქაში გამოიკვეთა მშობლებისა და არასრულწლოვანი შვილების განსხვავებული მოლოდინები და შეხედულებები ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცულობის ასპექტში.

წინამდებარე კვლევის ფარგლებში, მშობლისა და მისი არასრულწლოვანი შვილის მოლოდინები განხილული იქნება მშობლების მიერ არასრულწლოვანი

---

[5] *Council of Europe,* Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html> [27.06.2022].

[6] პირადი ცხოვრების ხელშეუხებლობის უფლებისა და პერსონალური მონაცემების დაცვის უფლების ურთიერთკავშირზე დეტალურად იხ.: *საგინაშვილი ნ.,* პერსონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა, ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე, სტატიათა კრებული, *კორკელია კ. (რედ.),* 2015, 166-19, <http://ewmi-prolog.org/images/files/7110HRStandardsImpact.pdf> [27.06.2022]; ასევე *Hustinx P.,* EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013, 2, <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en;> [27.06.2022]; *European Union Agency for Fundamental Rights and Council of Europe*, Handbook on European Data Protection Law, 2018, 20, <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [27.06.2022].

[7] *Gligorijevi´C J.,* Children's Privacy: The Role of Parental Control and Consent, Human Rights Law Review, 2019, 19, 201–229, <https://academic.oup.com/hrlr/article/19/2/201/5522387?login=true> [27.06.2022].

[8] *Steinberg S. B.*, Sharenting: Children's Privacy in the Age of Social Media, 66 Emory L.J. 839, 2017, 861, <https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/> [27.06.2022].

[9] ანალოგიური მოწესრიგებაა ეროვნულ კანონმდებლობაშიც. იხ. ,,ბავშვის უფლებათა კოდექსის“ (5004-Iს, 20/09/2019) 24-ე მუხლის მე-3 ნაწილი. ასევე, საქართველოს სამოქალაქო კოდექსის (საქართველოს პარლამენტის უწყებანი, 31, 24/07/1997) 1198-ე მუხლის მე-6 ნაწილი.

[10] ,,2017 წელს, 16 წლის არასრულწლოვანმა მიმართა სასამართლოს, მშობლის მიერ სოციალურ ქსელში მისი ფოტოს თანხმობის გარეშე განთავსების გამო. სასამართლომ მშობელს დაავალა ფოტოს წაშლა, წინააღმდეგ შემთხვევაში სანქციის სახით განუსაზღვრა ჯარიმა 10 000 ევროს ოდენობით. 2016 წელს ავსტრალიელმა თინეიჯერმა სარჩელი შეიტანა მშობლების წინააღმდეგ სასამართლოში, რომლებმაც ბოლო 7 წლის განმავლობაში განათავსეს 500-მდე ,,სამარცხვინო“ ფოტოები სოციალურ ქსელში, შვილის თანხმობის გარეშე“. იხილეთ ციტირება: *Goshadze K.,* Legal Implications of "Shattering", International Journal of Law: "Law And World", №15, Vol. 6, Issue 2, 2020, 5.

შვილების პერსონალური მონაცემების სოციალურ ქსელებში სისტემატური განთავსების („შარენტინგის“[11]) კონტექსტში. აღნიშნული საფრთხის ქვეშ აყენებს არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობის უფლებასა და ამ ჭრილში მათი პერსონალური მონაცემების დაცვას. ამ პროცესში, მშობლის ვარაუდი მისი ქმედების ,,უვნებელი“ ხასიათის შესახებ არ არის თანხვედრაში შვილის შეხედულებებთან და ინფორმაციის გავრცელების ობიექტურ საჭიროებებთან. მშობელი ვერ (არ) ამართლებს არასრულწლოვნის მიერ ჩამოყალიბებულ პერსონალურ მონაცემების დაცვის მოლოდინს.

კვლევის ფარგლებში, წარმოჩენილია საკითხის მნიშვნელობა, შეფასებულია ,,შარენტინგის“ უარყოფითი შედეგები და გავლენა არასრულწლოვნის უფლებრივ მდგომარეობაზე, იდენტიფიცირებულია პრობლემის გადაჭრის შესაძლო სამართლებრივი მექანიზმები.

კვლევა ეფუძნება შედარებითსამართლებრივ მეთოდს. ეროვნულ მოწესრიგებასთან ერთად, გაანალიზებულია პერსონალურ მონაცემთა დაცვის საკითხების მარეგულირებელი საერთაშორისო აქტები, ოფიციალური გზამკვლევები, რეკომენდაციები და მოსაზრებები, ასევე საერთაშორისო სასამართლო პრაქტიკა. მსჯელობის ფარგლებში, ცალკეულ საკითხებზე ასევე გაანალიზებულია ევროპის კავშირის წევრი ქვეყნების კანონმდებლობა და სასამართლო პრაქტიკა.

2. „შარენტინგი“ – მშობლის მიერ შექმნილი თანამედროვე საფრთხე არასრულწლოვნის პერსონალური მონაცემებისათვის

მშობლის მიერ სოციალურ ქსელში მისი არასრულწლოვანი შვილის შესახებ ინფორმაციის სისტემატური განთავსება, ბავშვის[12] ყოველდღიური ცხოვრების აღწერა ფოტოების, ვიდეოებისა და ბლოგების წარმოების ფორმით დღევანდელი ცხოვრების ჩვეული ნაწილია.[13] აღნიშნული, როგორც წესი, წარმოადგენს მშობლის სტატუსთან

[11] სიტყვა “Sharenting“ გამომდინარეობს სიტყვების “parent” (მშობელი) და “share” (გაზიარება) კომბინაციიდან. მითითებულია: *Goshadze K.,* დასახელებული ნაშრომი, 1.

[12] „ბავშვის უფლებათა კოდექსის“ მიხედვით, ბავშვად მიიჩნევა პირი 18 წლის ასაკის მიღწევამდე (იხ. მე-3 მუხლის ,,ა“ ქვეპუნქტი). შესაბამისად, წინამდებარე კვლევაში თანაბარმნიშვნელოვნად არის გამოყენებული ტერმინები ,,ბავშვი“ და ,,არასრულწლოვანი“.

[13] *Siibak A.,* Educating 21st Century Children, Chapter 6, Digital parenting and the Datafied Child, Institute of Social Studies, University of Tartu, Estonia, 2019, <https://www.oecd-ilibrary.org/sites/313a9b21-en/index.html?itemId=/content/component/313a9b21-en> [28.06.2022]. “Google”-ის ყოფილი დირექტორის, *ერიკ შმიდტის* განმარტებით, როგორც პირადი მიზეზით, ასევე მშობლების დამსახურებით, გარკვეული დროის შემდეგ ჩვენ მივაღწევთ ისეთ წერტილს, როდესაც თითოეულ ადამიანს ექნება სამარცხვინო ინფორმაცია და ფოტოები განთავსებული სოციალურ ქსელში. იხ. *Steinberg S. B.*, დასახელებული ნაშრომი, 855.

დაკავშირებული დადებითი ემოციების გაზიარების, ბავშვის აღზრდასთან დაკავშირებული გამოწვევების გამოხატვისა და ცალკეულ საკითხებზე რჩევებისა და რეკომენდაციების მიღების საშუალებას.[14;15]

„შარენტინგის“ მასშტაბები საკმაოდ ფართოა[16] და ზოგ შემთხვევაში ის ჯერ კიდევ ბავშვის დაბადებამდე იწყება.[17] კვლევები ცხადყოფს, რომ არასრულწლოვნები, ასაკის მატებასთან ერთად, განიცდიან დისკომფორტს მშობლების მიერ მათი პერსონალური მონაცემების გასაჯაროების გამო.[18] თუმცა იმის გათვალისწინებით, რომ ამ პრაქტიკის ,,მსხვერპლი“ არასრულწლოვნები ჯერ კიდევ პატარები არიან[19] და აკადემიურ წრეებში ამ საკითხებზე საუბარი ჯერ არ დაწყებულა,[20] საკითხი სამართლებრივად მოწესრიგებული არ არის.

ციფრულ გარემოში მონაცემების განთავსებისას მშობლები, როგორც წესი, ინფორმაციას კონკრეტულ აუდიტორიას უზიარებენ, თუმცა გადაზიარების ფუნქციის საშუალებით, მისი ფართო აუდიტორიისათვის ხელმისაწვდომობა მარტივად შესაძლებელია. ასევე, საძიებო სისტემების „ქეშირების“ ფუნქცია საშუალებას იძლევა განუსაზღვრელი ვადის შემდეგ მოხდეს ერთხელ გასაჯაროებული ინფორმაციის მოძიება.[21] ამდენად, ჩვენს მიერ სოციალურ ქსელში განთავსებული ინფორმაცია ,,უკიდეგანო“ არეალში იკარგება, რაც ზრდის არასრულწლოვნების პერსონალური მონაცემების შელახვის რიკებს.

---

[14] *Siibak A.,* დასახელებული ნაშრომი.

[15] ზოგიერთი მკვლევრის მოსაზრებით (მაგ. *Lazard L. et al.,* Sharenting: Pride, Affect and the Day-to-Day Politics of Digital Mothering, Social and Personality Psychology Compass, Vol. 13/4, 2019, e12443,) მსგავსი ქმედებები „კარგი მშობლის“ სამაგალითო ფსიქოლოგიურ ტრენდადაც იქცა.

[16] მიჩიგანის უნივერსიტეტის მიერ ჩატარებული კვლევის მიხედვით, მშობლების 56% პოტენციურად სამარცხვინო ინფორმაციას აქვეყნებდა, 51%-ის მიერ განთავსებული ინფორმაცია ახდენდა ბავშვის ადგილმდებარეობის იდენტიფიკაციას კონკრეტული მომენტისათვის, ხოლო 27% აქვეყნებდა შეუფერებელ ფოტოებს. იხ. “Sharenting” Trends: Do Parents Share Too Much About Their Kids on Social Media? C.S. Mott Children’s Hospital, Mar. 16, 2015, მითითებულია: *Steinberg S. B.*, დასახელებული ნაშრომი, 848.

[17] ორსული დედების ¼, ბავშვის დაბადებამდე ათავსებს ექოსკოპიის ფოტოს სოციალურ ქსელში. იხ.: *Steinberg S. B.*, დასახელებული ნაშრომი, 849.

[18] გაერთიანებულ სამეფოში, 2017 წელს ჩატარებული კვლევის მიხედვით, 12-16 ასაკობრივი კატეგორიის 1000 მოზარდიდან, 71.3 % მიიჩნევდა, რომ მშობლები პატივს არ სცემდნენ მათ პირადი ცხოვრების ხელშეუხებლობას ციფრულ გარემოში, ხოლო 39.8% თვლიდა, რომ მშობლებმა სამარცხვინო ფოტოები განათავსეს სოციალურ ქსელებში. იხ. *Levy E.,* Parenting in the Digital Age: How Are We Doing?, Parent Zone: Making the Internet Work for Families, 2017, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://parentzone.org.uk/sites/default/files/2021-12/PZ_Parenting_in_the_Digital_Age_2017.pdf> [26.06.2022].

[19] დღევანდელი ბავშვები არიან ,,გაციფრულებული ბავშვების“ პირველი თაობა. *United Nations Children’s Fund (UNICEF)*, Children’s Online Privacy and Freedom of Expression: Industry Toolkit, 2018, 4, <https://www.coursehero.com/file/95867628/UNICEF-Childrens-Online-Privacy-and-Freedom-of-Expression1pdf/> [28.06.2022].

[20] *Siibak A.,* დასახელებული ნაშრომი.

[21] *Steinberg S. B.*, დასახელებული ნაშრომი, 844, 850.

პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევის გამო ფსიქოლოგიური და ემოციური დისკომფორტის[22] გარდა, ,,შარენტინგს“ ასევე შესაძლოა მოჰყვეს კონკრეტული უარყოფითი შედეგები პიროვნების ,,ციფრული გატაცების“,[23] პედოფილიისა[24] და კრიმინალური ქმედებების[25] სახითაც.

2.1. სამართლებრივი მოწესრიგება

არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობის უფლება დაცულია არაერთი სამართლებრივი აქტით, როგორც ეროვნულ,[26] ასევე საერთაშორისო დონეზე.[27] პერსონალური მონაცემების დაცვის კონტექსტში, არასრულწლოვნის უფლებების დაცულობას ეროვნულ დონეზე უზრუნველყოფს ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (შემდგომში – ,,პერსონალურ მონაცემთა დაცვის კანონი“),[28] ხოლო საერთაშორისო დონეზე „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს 1981 წლის 28 იანვრის №108 კონვენცია (შემდგომში – ,,108-ე კონვენცია“).

მონაცემთა დაცვის ეროვნული კანონმდებლობა თავის მხრივ ეფუძნება ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის პერსონალურ მონაცემთა დაცვასა და ასეთი ტიპის მონაცემთა თავისუფალ გადაადგილებასთან მიმართებით ინდივიდების დაცვის თაობაზე დირექტივას (95/46/EC) (შემდგომში – ,,1995 წლის დირექტივა“). ეროვნულ დონეზე დღეს მოქმედი საკანონმდებლო ნორმების უმეტესი ნაწილი სწორედ 1995 წლის დირექტივის ტექსტს ეფუძნება. 2018 წელს, დირექტივა

[22] ,,შატრერინგიდან“ გამომდინარე ფსიქოლოგიური და ემოციური დისკომფორტის შესახებ დაწვრილებით იხ. *Siibak A., Lipu M.,* 'Take it down!': Estonian Parents' and Pre-teens' Opinions and Experiences with Sharenting, Media International Australia Incorporating Culture and Policy, 2019, 1–11, 4, 7, <https://www.researchgate.net/publication/331411236_'Take_it_down'_Estonian_parents'_and_pre-teens'_opinions_and_experiences_with_sharenting> [18.05.2022], აგრეთვე: *Goshadze K.*, დასახელებული ნაშრომი, 3.

[23] ციფრული გატაცების (“digital kidnapping”) შესახებ, დაწვრილებით იხ. *Siibak A.,* დასახელებული ნაშრომი; ასევე *Steinberg S. B.*, დასახელებული ნაშრომი, 854.

[24] იხ. *Battersby L.,* Millions of Social Media Photos Found on Child Exploitation Sharing Sites, Sydney Morning Herald, Vol. 30, 2015, <http://www.smh.com.au/national/millions-of-socialmedia-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html> [28.06.2022].

[25] იხ.: *Donovan S.*, “Sharenting”: The Forgotten Children of the GDPR, Peace Human Rights Governance, 4(1), 2020, 42, <http://phrg.padovauniversitypress.it/2020/1/2> [28.06.2022].

[26] საქართველოს კონსტიტუციის მე-15 მუხლი (საქართველოს პარლამენტის უწყებები, 31-33, 24/08/199); ბავშვის უფლებათა კოდექსის მე-9 მუხლი.

[27] ბავშვის უფლებების შესახებ კონვენციის (02/07/1994, ვებგვერდი) მე-16 მუხლი; ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის (20/05/1999, 16/11/1999, 1950) მე-8 მუხლი.

[28] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.

ჩაანაცვლა მონაცემთა დაცვის ზოგადმა რეგულაციამ[29] (შემდგომში – ,,ზოგადი რეგულაცია"),[30] ხოლო რეგულაციასთან ეროვნული კანონმდებლობის შესაბამისობაში მოყვანის მიზნით, პარლამენტში წარდგენილ იქნა ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის ახალი პროექტი.[31]

შესაბამისად, ,,შარენტინგის" სამართლებრივი მოწესრიგების ჭრილში საკითხის განხილვისათვის, გაანალიზებული იქნება ეროვნული კანონმდებლობის, ეროვნულ დონეზე ინიციირებული ცვლილებისა და ზოგადი რეგულაციის შესაბამისი ნორმები.

,,პერსონალურ მონაცემთა დაცვის კანონის" შესაბამისად, კანონის მოქმედების სფერო არ ვრცელდება ,,ფიზიკური პირის მიერ მონაცემთა აშკარად პირადი მიზნებისათვის დამუშავებაზე, როდესაც მათი დამუშავება დაკავშირებული არ არის მის სამეწარმეო ან პროფესიულ საქმიანობასთან;"[32] მსგავსი ფორმულირება არის წარმოდგენილი ზოგადი რეგულაციითაც, მათ შორის პირადი მიზნების განმარტების ნაწილში უშუალოდ ,,სოციალურ ქსელებში მოღვაწეობისა" და ,,ინტერნეტ აქტივობის" დაკონკრეტებით. [33]

შესაბამისად, ზემოაღნიშნული ფორმულირებების სიტყვა-სიტყვითი განმარტებიდან გამომდინარე, მშობლების მიერ არასრულწლოვანი შვილების პერსონალური მონაცემების ციფრულ გარემოში განთავსება[34] წარმოადგენს პირადი მიზნებისათვის მონაცემების დამუშავებას და მასზე არ ვრცელდება მონაცემთა დაცვის სამართლის ნორმები არც ეროვნული[35] და არც საერთაშორისო[36] მოწესრიგებით.

---

[29] General Data Protection Regulation (GDPR). რეგულაციის ოფიციალური ქართულენოვანი თარგმანი იხ. <https://personaldata.ge/ka/legislation> [28.06.2022].

[30] ქართულ იურიდიულ წრეებში აღნიშნულ დოკუმენტს ასევე მოიხსენიებენ *მონაცემთა დაცვის საერთო რეგულაციის* სახელწოდებით, თუმცა წინამდებარე ნაშრომის მიზნებისათვის, გამოყენებული იქნება სახელმწიფო ინსპექტორის სამსახურის მიერ მომზადებულ ოფიციალურ თარგმანში გამოყენებულია სახელწოდება ,,მონაცემთა დაცვის ზოგადი რეგულაცია".

[31] რეგ. N07-3/353/9, თარიღი 22.05.2019.

[32] კანონის მე-3 მუხლის 3 ,,ა" ქვეპუნქტი. პირადი მიზნებით დამუშავებას ასევე გამორიცხავდა 1995 წლის დირექტივა და 108-ე მოდერნიზებული კონვენციის 3.2 მუხლი.

[33] ,,...პირადი და ოჯახური საქმიანობა შეიძლება მოიცავდეს მიმოწერას და მისამართების შენახვას, *სოციალურ ქსელებში მოღვაწეობას და ინტერნეტ აქტივობას*, რომელიც ასეთი საქმიანობის კონტექსტში ხორციელდება" . ზოგადი რეგულაციის პრეამბულის მე-18 პარაგრაფი.

[34] მით უფრო რეგულაციის ნორმის ფორმულირებაში ,,სოციალურ ქსელებში მოღვაწეობას და ინტერნეტ აქტივობას"-ზე მითითების შემდეგ. ამასთან, 1995 წლის დირექტივის ტექსტი პირდაპირ მითითებას არ აკეთებდა სოციალურ ქსელში მოღვაწეობასა და ინტერნეტ აქტივობაზე.

[35] „პერსონალურ მონაცემთა დაცვის შესახებ" კანონის მე-3 მუხლის ,,ა" პუნქტი.

[36] ,,2016 წელს მონაცემთა დაცვის ზოგადი რეგულაცია შემუშავდა იმ სულისკვეთებით, რომ დაცვის მაღალი სტანდარტი დაეწესებინა ინდივიდების (განსაკუთრებით ბავშვების) პერსონალური მონაცემების დაცვისათვის. თუმცა, რეგულაცია მცირეწლოვნების ,,ციფრულ პრივატულობას" (digital privacy) ტოვებს მშობლების ხელში, მათი ციფრული კომპეტენციების მიუხედავად." „ ..... რეგულაცია ნაკლებ ყურადღებას ამახვილებს პატარა ბავშვების პრივატულობის დაცვაზე, რომელთა პრივატულობაც ღიაა მშობლების მიერ ონლაინ პოსტების გათავისების პირობებში". იხილეთ ციტირება: *Donovan S.*, დასახელებული ნაშრომი, 35, 36.

აღსანიშნავია, რომ მონაცემთა დაცვის ზოგადი რეგულაცია, განსაკუთრებულ ყურადღებას ამახვილებს ბავშვებზე[37] და მსგავსი განმარტებით, მონაცემთა დაცვის სამართლის ნორმების გაუვრცელებლობით, მშობლებისაგან დაუცველ მდგომარეობაში ხვდებიან „შარენტინგი“-ს მსხვერპლი არასრულწლოვანი შვილები,[38] რაც მონაცემთა დაცვის სამართლის პრინციპებიდან გამომდინარე, აზრს მოკლებულია.

ზოგადად, პირადი და საოჯახო მიზნებით დამუშავების კონტექსტში, მონაცემთა დაცვის სამართლის მოქმედების გაუვრცელებლობა განპირობებულია ჟურნალისტიკის, სახელოვნებო და ლიტერატურული გამოხატულების ხელშეწყობის ისტორიული პრაქტიკით[39] და მიზნად ისახავს ინდივიდის გამოხატვის თავისუფლების დაცვას.[40] მეორე მხრივ, გამოხატვის თავისუფლების დაცვის სანაცვლოდ, არსებობს ინდივიდუალური ოჯახის წევრების პერსონალური მონაცემების დარღვევის რისკი.[41] შედეგად, სახეზე გვაქვს ამ ორი უფლების ურთიერთდაპირისპირება.[42]

ადამიანის უფლებების დაცვის ჭრილში, ერთი მხრივ დაცული უნდა იყოს გამოხატვის თავისუფლება, ხოლო მეორე მხრივ ოჯახის ცალკეული წევრის (ინდივიდის) უფლებები, მათი პირადი ცხოვრების ხელშეუხებლობისა და კონკრეტულად კი პერსონალური მონაცემების დაცულობის კონტექსტში. სამართლიანი ბალანსის დადგენისათვის, მართლმსაჯულების ევროპული სასამართლოს პრაქტიკით ,,პირადი და საოჯახო მიზნით დამუშავება“ მაქსიმალურად ვიწროდ განიმარტება.[43] ასეთი ვიწრო განმარტების სასამართლო პრაქტიკა არსებობდა როგორც 1995 წლის დირექტივის მოქმედების პერიოდში,[44] ასევე რეგულაციის არსებობის დროსაც.[45] სასამართლოს შეფასებით,

[37] იხ. ზოგადი რეგულაციის პრეამბულის 38-ე პარაგრაფი.

[38] *Donovan S.*, დასახელებული ნაშრომი, 39.

[39] *WP 29,* Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 1-2, <https://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm> [28.06.2022]. WP29-ე სამუშაო ჯგუფის უფლებამოსილებთან და მნიშვნელობასთან დაკავშირებით იხ.: *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2019, 15.

[40] ამასთან, კერძო ინდივიდის მიერ განხორციელებული ყველა ქმედება ონლაინ სივრცეში არ წარმოადგენს ჟურნალისტიკის, სახელოვნებო ან ლიტერატურულ გამოხატულებას.

[41] *Donovan S.*, დასახელებული ნაშრომი, 39.

[42] *WP 29,* Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 1-2.

[43] რეგულაციაშიც ასევე პირადი და საოჯახო მიზნით დამუშავების ვიწრო განმარტებას ემსახურება ნორმის ფორმულირების ტექსტში გამოყენებულია ტერმინი ,,წმინდა“ [“purely”]. იხ. რეგულაციის პრეამბულის მე-18 ნაწილი.

[44] იხ. “Bodil Lindqvist” საქმე (სქოლიო 47). ამ საქმის განხილვა მოხდა 1995 წლის დირექტივის საფუძველზე, რომლის ტექსტში პირდაპირ არ იყო მითითებული სოციალური მედიის ფარგლებში საქმიანობა, როგორც პირადი მიზნებით საქმიანობის ერთ-ერთი სახე (იხ. დირექტივის მე-3 მუხლის მე-2 ნაწილი).

[45] “Sergejs Buivids v. the Augstākā Tiesa”-ის საქმე, იხ. სქოლიო 49. რეგულაციის ფორმულირებაში ფორმულირებაში პირდაპირ არის მითითებული სოციალური მედია. (იხ. რეგულაციის პრეამბულის მე-18 ნაწილი).

ვიწრო განმარტების საჭიროება გამომდინარეობს ევროპის კავშირის ძირითად უფლებათა ქარტიიდან.[46]

მართლმსაჯულების ევროპული სასამართლოს პრაქტიკით, ვიწრო განმარტების ერთ-ერთი მთავარი საკვანძო კრიტერიუმია მონაცემების გავრცელების ფარგლები. სასამართლომ "Lindqvist"[47]-ის საქმეზე დაადგინა, რომ „ბლოგის" ტიპის ვებგვერდის გზით მონაცემების პირთა განუსაზღვრელი წრისათვის გავრცელება არ წარმოადგენს ,,აშკარად პირადი მიზნებით დამუშავებას"[48] და შესაბამისად ხვდება 1995 წლის დირექტივის მოქმედების ფარგლებში. ასევე "Sergejs Buivids"-ის[49] საქმეზე, სასამართლომ დაადასტურა ასეთი ვიწრო ინტერპრეტაცია.[50] მსგავსი განმარტება შენარჩუნდა მონაცემთა დაცვის ზოგადი რეგულაციის ძალაში შესვლის შემდეგაც – ნიდერლანდების პირველი ინსტანციის სასამართლომ,[51] არ ჩათვალა ბებიის (მოპასუხე) მიერ შვილიშვილის ფოტოსურათის "Facebook" და "Pinterest" გვერდებზე განთავსება აშკარად პირადი მიზნებით დამუშავებად, რადგანაც: ა) სახეზე არ იყო მცირეწლოვანი ბავშვის მშობლის (მოსარჩელის) თანხმობა და ბ) ბებიის "Facebook" და "Pinterest" გვერდებით გაზიარებული ინფორმაცია შესაძლებელია მოხვედრილიყო მესამე პირთა ხელში.[52] აღნიშნული გადაწყვეტილებით, სასამართლო პრაქტიკით, კიდევ ერთხელ დადასტურდა, ,,პირადი და საოჯახო მიზნებით დამუშავების" ვიწრო ინტერპრეტაცია.

ონლაინ სივრცეში არასრულწლოვნის ინფორმაციის ციფრულ გარემოში გავრცელებისას პირადი მიზნებით დამუშავების ,,გამონაკლისიდან" ,,გამოყვანას" განამტკიცებს ასევე ზოგიერთი ქვეყნის საკანონმდებლო მოწესრიგებაც.[53]

სასამართლო პრაქტიკისგან განსხვავებით, 29-ე სამუშაო ჯგუფი[54] პირადი მიზნებით დამუშავების ,,გამონაკლისის" შეფასებისას უფრო ფართო განმარტებას აკეთებს და მხოლოდ გავრცელების ფარგლების კრიტერიუმს არ ეფუძნება. აღნიშნულმა ორგანომ განსაზღვრა კრიტერიუმები, რომელთა კომბინაციითაც, შეიძლება იდენტიფიცირება, რამდენად ხვდება კონკრეტული დამუშავება პირადი მიზნებით დამუშავების

[46] მართლმსაჯულების ევროპულმა სასამართლომ საქმეზე CJEU, Case C- 212/ 13, *Ryneš* [2014] განმარტა, რომ ,,ქარტიის მე-7 მუხლის შესაბამისად, გადახვევები და შეზღუდვები პერსონალური მონაცემების დაცულობის კონტექსტში უნდა იყოს გამოყენებული მხოლოდ მაშინ, როცა ის მკაცრად საჭიროა". იხ. გადაწყვეტილების §48.

[47] CJEU, Case C-101/01, *Bodil Lindqvist*, [2003].

[48] გადაწყვეტილების §31.

[49] CJEU, C-345/17 – *Buivids*, [2019].

[50] იხ. გადაწყვეტილების §43**.**

[51] 2020 წლის 13 მაისის გადაწყვეტილება.

[52] მოპასუხეს არ ჰქონდა დაყენებული უსაფრთხოების შესაბამისი პარამეტრები. საქმის დეტალები იხ:. *Fenech Farrugia Fiott Legal,* <https://www.fff-legal.com/the-household-exemption-in-gdpr/> [01.07.2022].

[53] მაგ., დანიის კანონმდებლობით, 16 წლამდე არასრულწლოვნის ფოტოების ინტერნეტსივრცეში განთავსებამდე, სავალდებულოა მისი კანონიერი წარმომადგენლ(ებ)ის თანხმობა. იხ. *Fenech Farrugia Fiott Legal,* <https://www.fff-legal.com/the-household-exemption-in-gdpr/> [01.07.2022].

[54] *WP29*, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 4.

,,გამონაკლისის“ ფარგლებში. ამ კრიტერიუმებს შორის, გავრცელების პირთა წრე ერთ-ერთი პარამეტრია,[55] თუმცა არა განმსაზღვრელი. 29-ე სამუშაო ჯგუფის შეფასებით, მხოლოდ გავრცელების ფარგლების კრიტერიუმზე დაყრდნობა არ შეიძლება, რადგანაც დაპირისპირებული უფლებების (დამმუშავებლის მხარეზე – გამოხატვის თავისუფლება, ხოლო მონაცემთა სუბიექტის მხარეს – პერსონალური მონაცემების დაცვა (ავტ.)) შეფასების კუთხით, ასევე ლოგისტიკური კუთხით, სოციალური ქსელების მომხმარებლებისა და ბლოგერების მონაცემთა დაცვის სამართლის მოქმედების სფეროში სრული მოცულობით შეყვანა შეუძლებელია.[56] მხოლოდ გავრცელების ფარგლების კრიტერიუმზე დაყრდნობით, ასეთი კატეგორიის დამუშავებაც მოხვდება მონაცემთა დაცვის სამართლის ნორმების მოქმედების სფეროში, რაც გაართულებს მონაცემთა დაცვის სამართლის პრინციპებისა და ნორმების იმპლემენტაციასა და საზედამხედველო ორგანოების მიერ მათ შესრულებაზე კონტროლს.

შესაბამისად, გამოხატვის თავისუფლების უფლებასა და ოჯახის წევრების პირადი ცხოვრების ხელშეუხებლობის უფლებებს შორის სამართლიანი ბალანსის დადგენისათვის, 29-ე სამუშაო ჯგუფმა განსაზღვრა პირადი მიზნებით დამუშავებისას ზოგადი რეგულაციის გავრცელების შემდეგი შესაძლებლობები:

ა) რეგულაციის საბაზო უსაფრთხოების მოთხოვნების დაცვა ,,მსუბუქი“ ფორმით;

ბ) სხვა ინდივიდის წვდომის,[57] გასწორებისა[58] და დავიწყების უფლებების[59] პატივისცემა;[60]

გ) დამუშავებისას მონაცემთა დაცვის პრინციპების დაცვა (მონაცემების სანდოობა და სიახლე);

დ) დამუშავების საფუძვლის არსებობა;

ე) სხვა პირების ინფორმირება, მათი მონაცემების განთავსების შესახებ, რათა მათ ჰქონდეთ მონაცემების წაშლის მოთხოვნის შესაძლებლობა.[61]

---

[55] გამონაკლისის შეფასებისათვის, გავრცელების პირთა წრესთან ერთად, 29-ე სამუშაო ჯგუფი ადგენს სხვა პარამეტრებსაც, როგორიცაა ,,ეკუთვნის თუ არა პერსონალური მონაცემები ისეთ პირს, ვისაც არ აქვს პირადი ან საოჯახო ურთიერთობა დამმუშავებელთან“; ,,განთავსების სიხშირე და მასშტაბი ხომ არ ქმნის პროფესიული ან სრული დატვირთვის საქმიანობის ვარაუდს“, ,,არის თუ არა სახეზე ინდივიდზე პოტენციური გავლენის მოხდენის შესაძლებლობა, მათ შორის პრივატულობაში ჩარევის ფორმით“. იხ.: *WP29*, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 4.

[56] იქვე.

[57] Right to Access. იხ. მონაცემთა დაცვის ზოგადი რეგულაციის მე-14 მუხლი, პერსონალურ მონაცემთა დაცვის შესახებ კანონის 22-ე მუხლი.

[58] Right to Rectification. იხ. მონაცემთა დაცვის ზოგადი რეგულაციის მე-16 მუხლი, მუხლი, პერსონალურ მონაცემთა დაცვის შესახებ კანონის 22-ე მუხლი.

[59] Right to erasure (“right to be forgotten”) იხ. მონაცემთა დაცვის ზოგადი რეგულაციის მე-17 მუხლი, მუხლი, პერსონალურ მონაცემთა დაცვის შესახებ კანონის 22-ე მუხლი.

[60] მაგალითად, მეგობარმა მოგთხოვათ სოციალური ქსელიდან ფოტოს ჩამოხსნა. *Donovan S.*, დასახელებული ნაშრომი, 36.

[61] *WP 29,* Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 5. ასევე, 29-ე სამუშაო ჯგუფის მოსაზრებით, საზედამხედველო ორგანოებს უნდა ჰქონდეთ მოკვლევის ჩატარების

ზემოაღნიშნულიდან გამომდინარე, მონაცემთა დაცვის სამართალი „სრული მოცულობით“ ვერ გავრცელდება „შარენტინგის“ შემთხვევებზე პირადი მიზნებით დამუშავების გამონაკლისის არსებობის გამო. ამასთან, მისი გაუვრცელებლობა აშკარად შელახავს არასრულწლოვნების პერსონალური მონაცემების დაცვის უფლებას. შესაბამისად, „შარენტინგი“ არ უნდა განიმარტოს, როგორც პირადი მიზნებით დამუშავება (ვიწრო განმარტების შესაბამისად) იმ შემთხვევაში, როცა ინფორმაციის მიმღები პირთა წრე განუსაზღვრელი ან ძალიან ფართეა.

თუმცა ამ შემთხვევაშიც, მონაცემთა დაცვის სამართალი უნდა გავრცელდეს არა სრულად,[62] არამედ მხოლოდ ,,მსუბუქი“ ფორმით – კონკრეტულ სამართლებრივ მექანიზმებზე დაყრდნობით.

2.2. პრევენციის სამართლებრივი მექანიზმები

წინამდებარე კვლევის ფარგლებში წარმოდგენილია „შარენტინგის“ პრევენციის სამი სამართლებრივი მექანიზმი: ა) არასრულწლოვნის თანხმობა; ბ) არასრულწლოვნის მიერ ,,დავიწყების უფლების“ გამოყენება და გ) არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება. მექანიზმების განხილვისას, შეფასებულია მათი დადებითი და უარყოფითი მხარეები. კვლევაში მექანიზმები წარმოდგენილია მათი ეფექტიანობის პრიორიტეტულობით – ყველაზე ეფექტიანობიდან ნაკლებად ეფექტიანობისკენ.

2.2.1. არასრულწლოვნის თანხმობა

არასრულწლოვნებთან მიმართებით სამართლებრივი ურთიერთობის თითქმის ყველა სიბრტყეში, მშობელი (კანონიერი წარმომადგენელი) მოიაზრება არასრულწლოვნის საუკეთესო ინტერესის განმახორციელებლად. აღნიშნული

შესაძლებლობა, რათა განსაზღვრონ, მიეკუთვნება თუ არა დამუშავება პირადი მიზნებით დამუშავებას. ევროპის კავშირის არაერთი ქვეყნის კანონმდებლობით (მაგ. საფრანგეთი - the French Act No. 2018-493 of 20 June 2018, art.2.3 <https://www.dataguidance.com/notes/france-data-protection-overview> [05.05.2022]; გერმანია - Federal Data Protection Act of 30 June 2017, art. 2.3 <https://www.dataguidance.com/notes/germany-data-protection-overview> [05.05.2022]), პირადი და საოჯახო მიზნით მონაცემების დამუშავებაზე არ ვრცელდება მონაცემთა დაცვის ეროვნული სამართალი. თუმცა, ცალკეულ შემთხვევებში, ვრცელდება საზედამხედველო ორგანოს უფლებამოსილება მოკვლევის განხორციელების კონტექსტში. იხ. *WP 29,* Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 1.

[62] სრულ გავრცელებაში მოიაზრება ყველა პრინციპისა და საფუძვლის, ანგარიშვალდებულებისა და სხვა ყველა სავალდებულო მოთხოვნის დაცვა. სრული გავრცელება ფაქტობრივად შეუძლებელია და ვერ მოხდება მისი კონტროლი და სათანადო ლოჯისტიკა. შესაბამისად ნორმა იქნება უმოქმედო.

გარკვეულწილად ეფუძნება კერძო სამართლით განმტკიცებულ შეზღუდული ქმედუნარიანობის ინსტიტუტს, რაც კანონიერი წარმომადგენლის ნების გამოვლენას (წინასწარი თანხმობა ან შემდგომი მოწონება) უკავშირებს არასრულწლოვნის მიერ გამოვლენილი ნების ნამდვილობას.[63]

მსგავსი მოწესრიგება არის წარმოდგენილი არასრულწლოვნის პერსონალური მონაცემების დაცვის კონტექსტშიც.[64] ამასთან, ციფრულ გარემოში მშობლის უფლება გადაწყვიტოს და აკონტროლოს შვილის ინფორმაციის გავრცელების ფარგლები, უნდა დაექვემდებაროს გარკვეულ შეზღუდვებს. განსხვავებით სამოქალაქოსამართლებრივი ურთიერთობებისაგან, როცა არასრულწლოვნის ,,დამოუკიდებელმა" ნების გამოვლენამ, შესაძლოა ზიანი მიაყენოს როგორც თავად არასრულწლოვანს, ასევე სამოქალაქო ბრუნვის სხვა მონაწილეებს, ,,შარენტინგის" შემთხვევაში ასეთი ,,ზიანი" პრაქტიკულად არ არსებობს.[65]

კვლევები ცხადყოფს,[66] რომ მშობლებისა და შვილების შეხედულებებს შორის ციფრულ გარემოში ინფორმაციის განთავსებამდე მშობლის მიერ შვილის თანხმობის მოპოვების თვალსაზრისით, აზრთა დიდი სხვაობაა. მშობლები, როგორც წესი, არ იღებენ თანხმობას მათი შვილებისაგან, ხოლო შვილების მიერ პროტესტის გამოხატვის შემთხვევაში, არ ახდენენ მასზე რეაგირებას. აღნიშნული კი იწვევს „პრივატულობის საზღვრების ტურბულენტობას" მშობლებსა და შვილებს შორის. იქმნება ინტერესთა დისბალანსი, რაც იწვევს ურთიერთობის დაძაბულობას.

ავტორთა ნაწილი[67] მიიჩნევს რომ, მშობელმა სრულად უნდა დაიცვას შვილის პრივატულობა და არ უნდა გაამჟღავნოს მისი ინფორმაცია, მეორე ნაწილის[68] შეფასებით კი უპირატესობა უნდა მიენიჭოს ბავშვზე ორიენტირებული პერსპექტივიდან გამომდინარე მშობლის უფლებას,[69] რაც მოიაზრებს მშობლისათვის მინიჭებული უფლებამოსილების განხორციელებას შვილის საუკეთესო ინტერესების ჭრილში.

[63] იხ. საქართველოს სამოქალაქო კოდექსის 63-ე მუხლის პირველი ნაწილი.

[64] იხ. ზოგადი რეგულაციის პრეამბულის 38-ე ნაწილი და მე-8 მუხლი, ხოლო ეროვნულ დონეზე - ინიციირებული კანონპროექტის მე-7 მუხლი.

[65] ამასთან, სამოქალაქოსამართლებრივ ურთიერთობებშიც არსებობს გარკვეული ფარგლები, როდესაც არასრულწლოვნები თავისუფლები არიან თავის ნების გამოვლენაში (როდესაც პირი გარიგებით იღებს სარგებელს (მაგ. ჩუქების ხელშეკრულების დადებისას), ასევე ემანსიპაციის შემთხვევაში (იხ. საქართველოს სამოქალაქო კოდექსის 65-ე მუხლი).

[66] *Siibak A., Lipu M.,* დასახელებული ნაშრომი, 3.

[67] *Sorensen S.,* Protecting Children's Right To Privacy In The Digital Age: Parents as Trustees of Children's Rights. Children's Legal Rights Journal 36(3), 2016, 202–203. მითითებულია *Siibak A., Lipu M.,* დასახელებული ნაშრომი, 3.

[68] *Steinberg S. B.,* Sharenting: Children's Privacy in the Age of Social, Gainesville, FL: UF Law Scholarship Repository, University of Florida Levin College of Law, 2017, მითითებულია *Siibak A., Lipu M.,* დასახელებული ნაშრომი, 3.

[69] "Child-centred Perspective on Parents' Rights'. ციტირებულია: *Siibak A., Lipu M.,* დასახელებული ნაშრომი, 4.

კვლევის მიხედვით,[70] მშობლების ნაწილი (მიუხედავად იმისა, რომ ინფორმირებულები არიან შვილის პროტესტის შესახებ) კვლავ აგრძელებენ ,,შარენტინგის“ პრაქტიკას. მშობლების გარკვეული კატეგორიის აზრით, ბავშვები ჯერ ახალგაზრდები არიან და მათი აზრი მნიშვნელოვანი არ არის ,,შარენტინგის“ პროცესში. ასევე ზოგიერთი მიიჩნევს, რომ მათ როგორც მშობელს, აქვთ შვილის ინფორმაციაზე სრული კონტროლის უფლება[71] (შესაბამისად, თანხმობის მიღებაც არ არის საჭირო (ავტ.)) თუმცა, გარკვეული ნაწილი ცვლის საკუთარ პრაქტიკას შვილისაგან თანხმობის მიღების კონტექსტში[72] (და იღებს თანხმობას შვილისაგან (ავტ.)).

თანხმობის მიღების ვალდებულების ფორმირების შესაძლებლობას ამყარებს „ბავშვის უფლებების შესახებ“ კონვენციის მე-12 მუხლი, ასევე ბავშვის უფლებათა კოდექსის მე-14 მუხლი.

ბავშვის უფლებათა კოდექსის შესაბამისად, განსაზღვრულია ბავშვის საუკეთესო ინტერესი[73], შესაბამისად, ზემოაღნიშნული ნორმების საფუძველზე, შეიძლება დავასკვნათ, რომ ბავშვის პერსონალური მონაცემები დაცვა ასევე წარმოადგენს მისი ინტერესის საგანს, რომელიც უნდა დაცული იქნეს მშობლის მიერ ბავშვის მონაწილეობითა და მოსაზრებების გათვალისწინებით.[74];[75]

რამდენადაც, მშობელთა ნაწილი თანახმაა, რომ თანხმობა მიიღოს მისი შვილებისაგან, საზოგადოებრივი ცნობიერების ამაღლება (უარზე მყოფი მშობლების მიდგომების შეცვლის მიზნით) და საკანონმდებლო დონეზე არასრულწლოვნის

[70] იხ. სქოლიო 66.

[71] *Siibak A., Lipu M.,* დასახელებული ნაშრომი, 7.

[72] *Siibak A., Lipu M.,* დასახელებული ნაშრომი, 8.

[73] კოდექსის მე-3 მუხლის ,,თ“ პუნქტი.

[74] პერსონალური მონაცემების დამუშავების კონტექსტში, ბავშვის საუკეთესო ინტერესებზე აქცენტს აკეთებს ასევე, სახელმწიფო ინსპექტორის სამსახური. ,,ბავშვების მონაცემების დამმუშავებელმა პირებმა უპირველეს ყოვლისა უნდა გაითვალისწინონ ბავშვის საუკეთესო ინტერესები. ყველა საჯარო და კერძო დაწესებულება ვალდებულია უზრუნველყოს არასრულწლოვანთა პერსონალური მონაცემების კანონიერი დამუშავება და ისეთი დარღვევების პრევენცია, რომლებმაც შესაძლოა გამოიწვიოს ბავშვის ღირსების შელახვა, მისი სტიგმატიზაცია, ბულინგი, დისკრიმინაცია ან ნეგატიური გავლენა მის ემოციურ მდგომარეობასა და განვითარებაზე. ტექნოლოგიური პროგრესის პირობებში არასრულწლოვანთა პირადი ცხოვრების ხელშეუხებლობის უფლებამ კიდევ უფრო მეტი მნიშვნელობა შეიძინა, რადგან ახალ შესაძლებლობებთან ერთად იზრდება ამ უფლებაში გაუმართლებელი ჩარევის საფრთხეები“. ,,არასრულწლოვანთა პერსონალური მონაცემების დამუშავება“, სახელმწიფო ინსპექტორის გადაწყვეტილებები, 2020, 4 <https://personaldata.ge/> [03.07.2022].

[75] სწორედ ბავშვის საუკეთესო ინტერესებზე დაფუძნებით, მისთვის მშობლისაგან ,,ცალკე მდგომი“ უფლებების მინიჭება განხორციელდა 2012 წელს, ირლანდიის კონსტიტუციის 31-ე ცვლილებით. (ცვლილების შესახებ დაწვრილებით იხ.: *Donovan S.*, დასახელებული ნაშრომი, 2020, 39, 43).
ზოგიერთი ავტორი ასეთი უფლების მინიჭების შესაძლებლობას განსაზღვრას ასევე ინგლისური სამართლისთვისაც (მითითებულია: *Bessant C.,* Sharenting: Balancing the Conflicting Rights of Parents and Children, Journal of Communications Law, Vol. 23, 2018, 20, <https://www.researchgate.net/publication/325594690_Sharenting_Balancing_the_conflicting_rights_of_parents_and_children> [03.07.2022].

თანხმობის სავალდებულოების განსაზღვრა, საკითხის რეგულირებას ერთ-ერთ ყველაზე ეფექტიან მექანიზმს წარმოადგენს.

ამასთან, თანხმობის შესაბამისი ასაკის განსაზღვრისათვის, მნიშვნელოვანია რამდენიმე ფაქტორის მხედველობაში მიღება – მშობლების შეფასებით, მათ (მშობლებს) აქვთ შვილის ინფორმაციის კონტროლის უფლება, განსაკუთრებით კი როცა ბავშვი პატარაა. შესაბამისად, თანხმობის საჭიროება უნდა დადგეს იმ ასაკიდან, როდესაც ბავშვი საკმაოდ მომწიფებულია, რომ შეაფასოს მისი ინფორმაციის განთავსების ,,ბედი“, ხოლო ამავდროულად ,,საშუალო მშობელი“ უნდა მიიჩნევდეს, რომ მისი შვილი საკმაოდ დიდია, რათა მისგან მიიღოს თანხმობა მისი ინფორმაციის განთავსებაზე.[76] მომწიფებულობის დონეზე ყურადღებას ამახვილებს ასევე ბავშვის უფლებათა კოდექსი.[77]

ამასთან, სამართლებრივი ურთიერთობების სხვადასხვა სიბრტყეებში არის დადგენილი გამონაკლისები, არასრულწლოვნების მიმართ მშობლის უპირატესი უფლებისაგან. არასრულწლოვანს შეუძლია თავად მიიღოს გადაწყვეტილება სამართლებრივი ურთიერთობის სხვადასხვა საკითხებზე, კანონიერი წარმომადგენლის ჩარევის გარეშე.[78] მსგავსი გამონაკლისი არსებობს ელექტრონული მომსახურების შეთავაზების ეტაპზეც. მონაცემთა დაცვის ზოგადი რეგულაციით, 13-დან 16 წლამდე ასაკი განისაზღვრა პერიოდად, როცა ბავშვებს მინიჭებული აქვთ უფლება, პირდაპირ მიიღონ ელექტრონული მომსახურება კანონიერი წარმომადგენლის თანხმობის გარეშე.[79] კანონპროექტის მიხედვით, ეს ასაკი არის 14 წელი.

ზემოაღნიშნულიდან გამომდინარე, რაკი მონაცემთა დაცვის საერთაშორისო კანონმდებლობა 13 წლიდან მიიჩნევს არასრულწლოვანს სათანადოდ მომწიფებულად, რომ მისთვის შეთავაზებული ელექტრონული მომსახურებით ისარგებლოს კანონიერი წარმომადგენლის თანხმობის გარეშე, ანალოგიური მომწიფებულობის ხარისხი ივარაუდება, ციფრულ გარემოში მის შესახებ ინფორმაციის განთავსებაზე თანხმობის გამოხატვის ასაკადაც.[80] შესაბამისად, 13 წელი *შესაძლოა,* განისაზღვროს როგორც ზღვარი, რის შემდეგაც მშობელს წარმოეშობა ვალდებულება მიიღოს შვილისაგან

[76] მშობლის აზრის გათვალისწინება ერთ-ერთი მნიშვნელოვანი ფაქტორია. როგორც ზემოთ აღინიშნა, მშობლები მიიჩნევენ რომ მათ აქვთ არასრულწლოვანი შვილის ინფორმაციაზე სრული კონტროლის უფლება (იხ. სქოლიო 66).

[77] იხ. მე-5 მუხლის მე-2 ნაწილი.

[78] იხ.: ,,პაციენტის უფლებების შესახებ“ საქართველოს კანონის (სსმ, 19, 25/05/2000) მე-4 მუხლის მე-2 ნაწილის ,,ბ“ და ,,გ“ ქვეპუნქტები; საქართველოს სამოქალაქო კოდექსის 65-ე და 1196-ე მუხლები.

[79] ეს ასაკი ქვეყნების მიხედვით მერყეობს 13-დან 15 წლამდე მონაკვეთში. ევროპის ქვეყნების მიხედვით თანხმობის ასაკები იხ.: <https://euconsent.eu/digital-age-of-consent-under-the-gdpr/> [03.07.2022].

[80] წინამდებარე კვლევის საგანს წარმოადგენს არა კონკრეტული ასაკის დადგენა, არამედ არასრულწლოვნის სავალდებულო თანხმობის სახით სამართლებრივი მექანიზმის შეთავაზება ,,შარენტინგის“ უარყოფითი შედეგების თავიდან აცილებისათვის. კონკრეტული ასაკი უნდა განისაზღვროს დარგის სხვა სპეციალისტების მიერ.

თანხმობა მისი პერსონალური მონაცემების ციფრულ გარემოში განთავსების შესახებ, როცა ასეთი განთავსება განპირობებულია მხოლოდ მშობლის გამოხატვის თავისუფლებით.[81] აქვე აღსანიშნავია, რომ ბავშვისათვის მინიჭებული უფლება, თანხმობა განაცხადოს მშობლის მიერ მის შესახებ ინფორმაციის განთავსებაზე, დამოკიდებული უნდა იყოს როგორც ბავშვის ასაკზე, ასევე განთავსებული ინფორმაციის ხასიათზე. შესაბამისად, ინფორმაციის ხასიათის გათვალისწინებით (მაგალითად, სამედიცინო ხასიათის ინფორმაციის განთავსება ,,ბლოგის" ტიპის ვებგვერდზე) ბავშვის მიერ თანხმობის გაცემის ასაკი შესაძლოა დაიწყოს უფრო მცირე ასაკიდანაც (მაგალითად, 10 წლიდან),[82] რამეთუ მონაცემთა ბუნებიდან გამომდინარე,[83] ასეთი ტიპის ინფორმაციის გასაჯაროებამ შეიძლება, სერიოზულად დააზიანოს მისი ემოციური მდგომარეობა ან არასასურველი შედეგი გამოიწვიოს ბავშვის სამომავლო პროფესიული და პირადი ცხოვრებისათვის.

ბუნებრივია რომ, დაინტერესებული მხარეების[84] ჩართულობის გარეშე ეს ბერკეტი მხოლოდ საკანონმდებლო ცვლილებით (კონკრეტული ასაკის მითითებით) ვერ ამუშავდება.[85] ბავშვის საუკეთესო ინტერესებიდან გამომდინარე შექმნილი საზიარო პასუხისმგებლობის ფარგლებში, მშობელმა, კერძო და საჯარო ორგანიზაციებმა ერთად უნდა იკისრონ პასუხისმგებლობა ციფრულ გარემოში ბავშვის უფლებების დაცვისათვის.[86] საზოგადოების ცნობიერების ამაღლება[87] ამ საზიარო პასუხისმგებლობის გამოხატვის ერთ – ერთი ფორმაა. განსაკუთრებული აქცენტი უნდა გაკეთდეს შშმ პირებზე და სხვა მოწყვლად ჯგუფებს მიკუთვნებულ ბავშვებზე.[88]

---

[81] ამ შემთხვევაში სახეზე არ უნდა იყოს ბავშვის ინტერესებიდან გამომდინარე, სხვა აუცილებელი საჭიროება. მაგ. საკანონმდებლო ვალდებულების ან ბავშვის სასიცოცხლო ინტერესის საფუძვლით ინფორმაციის საჯაროდ განთავსება.

[82] ეროვნული კანონმდებლობის ანალიზის საფუძველზე შეიძლება ითქვას რომ, 10 წელი წარმოადგენს გარდამტეხ ასაკს ბავშვის მომწიფებულობის ხარისხის განსაზღვრის მიზნებისათვის. კერძოდ, საქართველოს სამოქალაქო კოდექსის მიხედვით, პირის დელიქტუნარიანობა იწყება 10 წლის ასაკიდან (იხ. 994-ე მუხლის პირველი ნაწილი); გვარის შეცვლის შემთხვევაში, 10 წლიდან სავალდებულოა ბავშვის თანხმობა (იხ. 1196-ე მუხლი), ხოლო ბავშვის უფლებათა კოდექსის მიხედვით, ხოლო 10 - დან 18 წლამდე ბავშვი ითვლება მოზარდად (იხ. კოდექსის მე-3 მუხლის ,,ბ" პუნქტი).

[83] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ" კანონის მე-2 მუხლის ,,ბ" პუნქტი.

[84] სახელმწიფო, კერძო სექტორი, მშობლები, არასამთავრობო სექტორი.

[85] ციფრულ გარემოში ბავშვთა უფლებების დაცვის პროცესში დაინტერესებული მხარეების ჩართულობის როლსა და მნიშვნელობაზე იხ.: *Council of Europe,* Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment.

[86] *United Nations Children's Fund (UNICEF)*, Children's Online Privacy and Freedom of Expression: Industry Toolkit, 7; *Council of Europe,* Recommendation CM/Rec (2018)7, 11.

[87] არასრულწლოვნების უფლებების დაცვის მიზნით, "Public Health Model"-ის გამოყენება პოპულარული მეთოდია. მეთოდი ეფუძნება საზოგადოებრივი ცნობიერების ამაღლებით კონკრეტული შედეგის მიღებას. "Public Health Model"-ის შესახებ დაწვრილებით იხ.: *Steinberg S.,* დასახელებული ნაშრომი, 866.

[88] *Council of Europe,* Recommendation CM/Rec (2018)7, 11, 14.

არასრულწლოვნის თანხმობის, როგორც ,,შარენტინგის“ პრევენციის ერთ-ერთი მექანიზმის ეფექტიანობის კიდევ ერთ ნაკლოვანებას წარმოადგენს ,,საჯარო ფიგურის“ არასრულწლოვანი შვილების შემთხვევაში ,,თანხმობის სავალდებულოების“ არაეფექტიანობა. საჯარო ფიგურის არასრულწლოვან შვილებს, მათი სტატუსიდან გამომდინარე, აქვთ თმენის ვალდებულება მშობლების მიერ მათი ფოტოების განთავსების შესახებ.[89] შესაბამისად, ამ ნაწილში თანხმობის გაცემის წესები შესაძლოა, განსხვავებულად მოწესრიგდეს.[90]

2.2.2 არასრულწლოვნის მიერ „დავიწყების უფლების“ გამოყენება

,,შარენტინგის“ უარყოფითი შედეგების თავიდან არიდების ერთ-ერთ ალტერნატიულ მექანიზმს წარმოადგენს არასრულწლოვანისათვის მონაცემთა დაცვის სამართლით განსაზღვრული ,,დავიწყების უფლების“ მინიჭება.[91] პირადი ცხოვრების ხელშეუხებლობის უფლების დაცულობის კონტექსტში, შედეგობრივად არასრულწლოვნის წინასწარი თანხმობა უფრო ეფექტიანი მექანიზმია,[92] თუმცა ,,დავიწყების უფლების“ გამოყენება შესაძლოა, ნაკლებად ეფექტიან, თუმცა ერთ-ერთ ალტერნატიულ გზად განვიხილოთ.

არასრულწლოვანისათვის ,,დავიწყების უფლების“ მინიჭების მაგალითს წარმოადგენს კალიფორნიის შტატის კანონმდებლობა. აღნიშნული შტატი, რომელიც წარმოადგენს ლიდერს ციფრული გარემოში პრივატულობის დაცვის კუთხით, მცირეწლოვნებს აძლევს უფლებას, მოითხოვონ მათი მონაცემების წაშლა ონლაინ ფორუმებიდან.[93] მართალია, ეს ეხება მათ მიერ განთავსებულ ინფორმაციას, მაგრამ ანალოგიის კუთხით შეიძლება, გამოყენებულ იქნეს მშობლების მიერ განთავსებულ ინფორმაციაზეც.

ამასთან, ციფრული გარემოს სპეციფიკის გათვალისწინებით, მშობლების მიერ გაზიარებული ინფორმაცია იკარგება ,,უკიდეგანო“ სივრცეში, ხშირია ინფორმაციის

[89] *Steinberg S.,* დასახელებული ნაშრომი, 859.

[90] აღნიშნული საკითხი არ არის განხილული წინამდებარე ნაშრომის ფარგლებში, რადგანაც წარმოადგენს დამოუკიდებელი კვლევის საგანს.

[91] ასევე, ცნობილია როგორც მონაცემების წაშლის უფლება. იხ: <https://gdpr.eu/right-to-be-forgotten/> [03.07.2022]. ,,დავიწყების უფლება“ არაპირდაპირი ფორმით არსებობდა ჯერ კიდევ 1995 წლის დირექტივაში. მოგვიანებით, მისი ფორმალიზაცია განხორციელდა რეგულაციის ძალაში შესვლის შემდეგ (იხ. რეგულაციის მე-17 მუხლი). ,,დავიწყების უფლება“ განსაკუთრებით პოპულარული გახდა ადამიანის უფლებათა ევროპული სასამართლოს მიერ 2014 წელს “Google Spain”-ის საქმეზე (Case of Google Spain, [2014], ECHR, C-131/12) მიღებული გადაწყვეტილების შემდეგ, რომელმაც რეგულაციით განსაზღვრული ,,დავიწყების უფლების“ ერთგვარი პრეცედენტი შექმნა.

[92] თანხმობის შემთხვევაში, არასრულწლოვნის უფლებები პრევენციულად დაცულია.

[93] *Steinberg S.,* დასახელებული ნაშრომი, 864.

მეორადი გამოყენებაც. შედეგად, ზოგჯერ, არასრულწლოვანს არ შეუძლია სთხოვოს მშობელს ინტერნეტში განთავსებული ინფორმაციის წაშლა.[94] ასევე რთულია ,,დავიწყების უფლების“ რეალიზაციის ტექნიკური მხარეც.[95] შესაბამისად, თანხმობასთან შედარებით, ,,დავიწყების უფლების“ გამოყენება შესაძლოა განვიხილოთ ,,შარენტინგის“ უარყოფითი შედეგების თავიდან აცილების ერთ-ერთ ნაკლებად ეფექტიან მექანიზმად.

2.2.3 არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება

არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება, ,,შარენტინგის“ უარყოფითი შედეგების მაკომპენსირებელ საშუალებას წარმოადგენს. ზოგადად, ყველა ბავშვს აქვს ზიანის ანაზღაურების მოთხოვნის უფლება, როცა მისი უფლებები ილახება.[96] თუმცა არასრულწლოვნის თანხმობის მექანიზმისგან განსხვავებით, ზიანის ანაზღაურების მოთხოვნის მექანიზმი არ ახდენს საკითხის პრევენციას და არც ,,დავიწყების უფლების“ მსგავსად ,,აჩერებს“ არასრულწლოვანისათვის მიყენებული ,,ზიანის გამომწვევ“ წყაროს. შესაბამისად, მისი დატვირთვის ,,სიმსუბუქიდან“ გამომდინარე, ის ნაკლებად პრიორიტეტული, თუმცა ერთ-ერთი ალტერნატიული მექანიზმია.

არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება საერთაშორისო დონეზე განმტკიცებულია ,,ბავშვის უფლებების შესახებ“ კონვენციის მე-12 მუხლის მე-2 ნაწილით, ეროვნულ დონეზე კი – საქართველოს სამოქალაქო კოდექსის მე-18 მუხლით, რომელიც პირადი არაქონებრივი უფლებების დაცვის საფუძველს ქმნის[97] და ბავშვის უფლებათა კოდექსის მე-13 მუხლის პირველი ნაწილით.

თუმცა შვილის მიმართ მშობლის განსაკუთრებული სტატუსიდან გამომდინარე, გასაჩივრების შესაძლებლობა, გარკვეულწილად, შეზღუდულია. მაგალითად, ამერიკული დელიქტური სამართლის მიხედვით, შვილის მიერ მშობლის წინააღმდეგ ზიანის ანაზღაურების მოთხოვნით სარჩელის შეტანის შესაძლებლობა, სამეცნიერო ლიტერატურაში განხილული არ არის,[98] ხოლო ზოგიერთი შტატი საერთოდ ზღუდავს

[94] *Steinberg S.,* დასახელებული ნაშრომი, 875.
[95] *Ambrose M. L., Ausloos J.*, დასახელებული ნაშრომი, 18.
[96] Committee on the Rights of the Child, General Comment no. 5; Human Rights Committee, General Comment No. 5; United Nations Human Rights Council, Resolution on the Rights of the Child: Access to justice, A/HRC/25/L.10, 25 March 2014, მითითებულია: *United Nations Children's Fund (UNICEF)*, Children's Online Privacy and Freedom of Expression: Industry Toolkit, 10.
[97] *Goshadze K.,* დასახელებული ნაშრომი, 4.
[98] *Porter E. G.*, Tort Liability in the Age of the Helicopter Parent, 64 ALA. L. REV. 533, 537 (2013). მითითებულია: *Steinberg S.,* დასახელებული ნაშრომი, 875.

არასრულწლოვანი შვილის მიერ მშობლის წინაშე სარჩელის შეტანის უფლებას.[99] ასევე, საქართველოს შემთხვევაში, ამკრძალავი ნორმის არარსებობის მიუხედავად, ნაკლებად წარმოსადგენია შვილის მიერ ამ უფლების გამოყენება.[100]

3. დასკვნა

„თანამედროვე ბავშვი იბადება და იზრდება სამყაროში, რომელიც ტექნოლოგიური პროცესებით ზედმიწევნით კონტროლდება, აანალიზდება და მანიპულირდება“.[101] ამ პირობებში კითხვის ნიშნის ქვეშ დგება ,,ციფრული ბავშვების“[102] პირადი ცხოვრების ხელშეუხებლობის უფლება და პერსონალური მონაცემების დაცვის საკითხები. მით უფრო, როცა ამ უფლების დარღვევის პროვოცირებას თავად მშობელი ახდენს.

წინამდებარე კვლევის ფარგლებში წარმოჩენილი პრობლემა გამოიხატება მშობლის მიერ შვილის პერსონალური მონაცემების სოციალური ქსელებში სისტემატური განთავსებით (,,შარენტინგით“). შედეგად, რისკის ქვეშ დგება ბავშვის როგორც არსებული, ასევე სამომავლო[103] უფლებრივი მდგომარეობა. ამავდროულად, ,,შარენტინგის“ პრაქტიკით, ერთმანეთს უპირისპირდება მშობლის გამოხატვის თავისუფლება და ბავშვის პირადი ცხოვრების ხელშეუხებლობის უფლებები.[104]

კვლევის შედეგად გამოიკვეთა, რომ პირადი მიზნებით მონაცემების დამუშავების ვიწრო ინტერპრეტაციის პირობებში, მშობლის მიერ არასრულწლოვანი შვილის შესახებ ინფორმაციის სოციალურ ქსელებში გავრცელების მონაცემთა დაცვის სამართლის ნორმების მოქმედების ქვეშ მოქცევით, შესაძლებელი ხდება ,,შარენტინგის“ უარყოფითი შედეგების თავიდან აცილება, ხოლო ზოგ შემთხვევაში – შემცირება. ამ მიმართულებით კვლევის ფარგლებში განხილულია შემდეგი სამართლებრივი მექანიზმები: არასრულწლოვნის სავალდებულო თანხმობა, არასრულწლოვნის მიერ ,,დავიწყების უფლების“ გამოყენება და ზიანის ანაზღაურების მოთხოვნის მექანიზმის გამოყენება. ზემოაღნიშნული მექანიზმები განსხვავებული სიძლიერით უზრუნველყოფენ ,,შატერინგის“ პირობებში არასრულწლოვნის უფლებრივი წონასწორობის შენარჩუნებას და ამ კონტექსტში მისი პერსონალური მონაცემების დაცულობას.

---

[99] *Wingerter I.,* Parent-Child Tort Immunity, 50 LA. L. REV. 1131 (1990). მითითებულია: *Steinberg S.,* დასახელებული ნაშრომი, 875.

[100] *Goshadze K.,* დასახელებული ნაშრომი, 5.

[101] ციტირებულია: *Wilson M.* (2019), 'Raising the ideal child? Algorithms, quantification and prediction', *Media, Culture & Society*, 41(5), 620-636. შემდგომი მითითებით: *Donovan S*., დასახელებული ნაშრომი, 40.

[102] "Datafied child". დეტალებისათვის იხ. სქოლიო 19.

[103] ,,შარენტინგის“ უარყოფითი შედეგები შეიძლება არ იყოს იმწუთიერი. ციტირებულია: *Donovan S*., დასახელებული ნაშრომი, 43

[104] *Steinberg S*., დასახელებული ნაშრომი, 869.

ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, საქართველოს პარლამენტის უწყებები, 31-33, 24/08/199.
2. „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის“ კონვენცია, 20/05/1999.
3. „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს №108 კონვენცია, 1981.
4. „ბავშვის უფლებების შესახებ“ კონვენცია, 02/07/1994.
5. „საქართველოს სამოქალაქო კოდექსი“, საქართველოს პარლამენტის უწყებანი, 31, 24/07/1997.
6. „ბავშვის უფლებათა კოდექსი“, 5004-Iს, 20/09/2019.
7. „პაციენტის უფლებების შესახებ“ საქართველოს კანონი, სსმ, 19, 25/05/2000.
8. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
9. ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის პერსონალურ მონაცემთა დაცვასა და ასეთი ტიპის მონაცემთა თავისუფალ გადაადგილებასთან მიმართებით ინდივიდების დაცვის თაობაზე დირექტივას (95/46/EC);
10. *საგინაშვილი ნ.,* პერსონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა, ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე, სტატიათა კრებული, კორკელია კ. (რედ.), 2015, 166-191;
11. *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2019, 15.
12. არასრულწლოვანთა მონაცემების დამუშავება, სახელმწიფო ინსპექტორის სამსახურის გადაწყვეტილებები, 2020, 4;
13. 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 L 119, 4/5/2016, 1–88.
14. *Battersby L.,* Millions of Social Media Photos Found on Child Exploitation Sharing Sites, Sydney Morning Herald, Vol. 30, 2015, <http://www.smh.com.au/national/millions-of-socialmedia-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html> [28.06.2022].

15. *Donovan S.,* "Sharenting": The Forgotten Children of the GDPR', Peace Human Rights Governance, 4(1), 2020, 36, 39–43.
16. *European Union Agency for Fundamental Rights and Council of Europe,* Handbook on European data protection law, 2018, 20.
17. *Gligorijevi´ C. J.,* Children's Privacy: The Role of Parental Control and Consent, Human Rights Law Review, 2019, 19, 201–229.
18. *Goshadze K.,* Legal Implications of "Shattering", International Journal of Law: "Law And World", № 15, Vol. 6, Issue 2, December 2020, 1-5.
19. *Hustinx P.,* EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013, 2.
20. *Joshua N.,* Why Do People Still Think Data Is the New Oil? Center for Data Innovation, January 16, 2018. Livingstone S., Children: A Special Case for Privacy?, InterMEDIA, International Institute of Communications, July 2018, Vol 4, 6, Issue 2.
21. *Levy E.,* Parenting in the Digital Age: How Are We Doing?*,* Parent Zone: Making the Internet Work for Families*,* 2017, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://parentzone.org.uk/sites/default/files/2021-12/PZ_Parenting_in_the_Digital_Age_2017.pdf> [26.06.2022].
22. *Macenaite M., Kosta E.,* Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?, Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, Netherlands, 146, 2017, <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096> [27.06.2022].
23. *Schwartz P. M.,* Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2004, 2056.
24. *Siibak A., Lipu M.,* 'Take it down!': Estonian Parents' and Pre-teens' Opinions and Experiences with Sharenting, Media International Australia Incorporating Culture and Policy, February 2019 1–11, 2019, 3-4, 7.
25. *Steinberg S. B.*, Sharenting: Children's Privacy in the Age of Social Media, 66 Emory L.J. 839, 2017, 844, 848-849, 850, 854-855, 861.
26. *Council of Europe,* "Guidelines to respect, protect and fulfil the rights of the child in the digital environment," Recommendation CM/Rec(2018)7 of the Committee of Ministers".
27. *WP* 29*,* Annex 2 Proposals for Amendments regarding exemption for personal or household Activities.
28. *Office for Children's Commissioner for England,* Children's Commissioner's Report Calls on Internet Giants and Toy Manufacturers to be Transparent About Collection of Children's Data, 2018.
29. *United Nations Children's Fund (UNICEF),* Children's Online Privacy and Freedom of Expression: Industry Toolkit, 2018, 4, 7, 10.

30. *Siibak A.,* Educating 21st Century Children, Chapter 6. Digital parenting and the datafied child, Institute of Social Studies, University of Tartu, Estonia, 2019.
31. *CJEU,* Case C-101/01, Bodil Lindqvist, [2003];
32. *Google Spain,* [2014], ECHR, C-131/12;
33. *CJEU,* Case C- 212/ 13, Ryneš [2014];
34. *CJEU*, C-345/17 – Buivids, [2019].
35. <www.ec.europa.eu> [28.06.2022].
36. <www.fff-legal.com> [01.07.2022].
37. <www.dataguidance.com> [05.05.2022];
38. <www.euconsent.eu> [03.07.2022].
39. <www.gdpr.eu> [03.07.2022].
40. <www.personaldata.ge> [03.07.2022].

ანა თოხაძე*

კორპორაციული მართვის სისტემაში მონაცემთა დაცვის ოფიცრის ინსტიტუციური როლის ინტერდისციპლინური ანალიზი

მსხვილი კორპორაციების მიერ პერსონალურ მონაცემთა სისტემური და ფართომასშტაბიანი დამუშავების მზარდმა ტენდენციამ განაპირობა პერსონალურ მონაცემთა დაცვის საკანონმდებლო მოწესრიგების გაძლიერება, განსაკუთრებით კი მონაცემთა სუბიექტების უფლებებისა და ინტერესების დაცვის თვალსაზრისით. მონაცემთა დაცვის ოფიცრის ინსტიტუტი, რომელიც მართალია, ეროვნულ კანონმდებლობაში ჯერ-ჯერობით არ არის ასახული, მონაცემთა დამუშავების კანონიერების, კორპორაციისა და მონაცემთა სუბიექტის ინტერესების თანაფარდობის უზრუნველყოფის ერთგვარი მექანიზმია. წინამდებარე ნაშრომი ამ ინსტიტუტის ინტერდისციპლინურ გააზრებას ეთმობა, ერთი მხრივ, საკორპორაციო სამართლის პერსპექტივით, ხოლო მეორე მხრივ — პერსონალურ მონაცემთა დაცვის სამართლის თვალსაზრისით, რათა განისაზღვროს მისი ინსტიტუციური ფუნცია კერძო სამართლის იურიდიული პირის ორგანიზაციულ სტრუქტურაში.

საკვანძო სიტყვები: *კორპორაციული მართვა, მონაცემთა დაცვა, მონაცემთა დაცვის ოფიცერი, მონაცემთა დაცვის ზოგადი რეგულაცია.*

1. შესავალი

პოზიტიურსამართლებრივი დებულებები დროში თვითმყოფად არსებობას სამართალშემოქმედებითი ტრანსფორმაციის ძალით განაგრძობს. ქართული

* ივ. ჯავახიშვილის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, კერძო სამართლის მიმართულების ასისტენტი; პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთოებების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის უფროსი.

სამართლის ევროპულ სამართალთან ჰარმონიზაციაზე მსჯელობის საზრისი, ალბათ, შემდეგ კითხვაზე პასუხის ძიებით იწყება: სამართალი გარდაქმნის საზოგადოებას თუ პირიქით — საზოგადოება გარდაქმნის მას? სოციუმის საყოველთაო კეთილდღეობას სამართალი, როგორც დროში განვითარებადი სისტემა, ქცევის სავალდებულო დებულებების განსაზღვრით ქმნის.[1] თუმცა თვალსაჩინოა, რომ თავისუფალი საბაზრო ეკონომიკის აღზევებას, ინდუსტრიათა და ეკონომიკური აქტორების თვითრეგულირება, ხოლო დეკოდიფიკაციის შემდგომ — სოციალურ-ეკონომიკურ ურთიერთობათა თვითნებური მოწესრიგება მოჰყვა[2]. ეს უფრო სპონტანურად, „მოთხოვნისა და მიწოდების პრინციპის“ გამო, ერთი მხრივ, კონკურენტუნარიანობის შესანარჩუნებლად, მეორე მხრივ კი სოციალური პასუხისმგებლობის ზეწოლით განხორციელდა.[3] სწორედ ამგვარად ჩამოყალიბდა კორპორაციების ნებაყოფლობითი ანგარიშვალდებულებაც სამოქალაქო საზოგადობის წინაშე.

თანამედროვე ტენდენციების გათვალისწინებით, მეგა-კორპორაციების ეკონომიკური საქმიანობის მასშტაბითა და ზეგავლენის თვალსაზრისით, კანონმდებლის ყურადღების ეპიცენტრში „დაკავშირებულ პირთა“[4], მათ შორის, მომხმარებელების და რაც მთავარია, წარმოდგენილი კვლევის ინტერესიდან გამომდინარე — მონაცემთა სუბიექტების უფლებრივი მდგომარეობა ექცევა. საკანონმდებლო მოწერსიგების სიხისტე სწორედ კორპორაციათა სამეწარმეო საქმიანობის „დაინტერესებულ პირთა“ ინტერესებზე ზეგავლენის ხარისხით ფასდება და ყალიბდება. მაშასადამე, ნათელია, იმპერტიული მოწესრიგების გზით, თუ რატომ ადგენს, ერთი მხრივ, საკორპორაციო სამართალი, ხოლო მეორე მხრივ — პერსონალურ მონაცემთა დაცვის სამართალი კორპორაციების მიმართ გარკვეულ ორგანიზაციულსამართლებრივ ვალდებულებებს. სწორედ ამგვარ მოთხოვნათა რიცხვს განეკუთვნება მონაცემთა დაცვის ოფიცრის ინსტიტუტის ინტეგრირება კორპორაციული მართვის სისტემაში.

მონაცემთა დაცვის ოფიცერი კორპორაციულსამართლებრივი მნიშვნელობით შიდაორგანიზაციული სტრუქტურის ინტეგრალური ელემენტია, ხოლო პერსონალურ

[1] *Bentham J.,* Of Laws in General, *Hart H. L. A. (ed.),* 1970, 31-33.

[2] *Magnier V.,* Comparative Corporate Governance, Legal Perspectives, 2017, 1-4. ამ მიზანს გამოხატავს კორპორაციული მართვის „რბილი მოწესრიგების“ რეჟიმი, რომელიც ევროპის კომისიის წინაშე *პროფ. ჰოლ დევისის* მიერ 1997 წელს იქნა წარდგენილი იმ იდეით, რომ კომისიას განესაზღვრა სუპრანაციონალური კორპორაციული მართვის სტანდარტი, ხოლო თითოეულ წევრ ქვეყანას „დაემორჩილე ან განმარტეს“ პრინციპით ეხელმძღვანელა ნაციონალური სამართლის ფარგლებში, *Johnson A.,* Soft Law, in: EC Regulation of Corporate Governance, UK, 2009, 343-347.

[3] *Picciotto S.,* Regulating Global Corporate Capitalism, 2011, 61-65, 193-200.

[4]სამეცნიერო ლიტერატურაში მოცემული „დაკავშირებულ პირთა“ (“Stakeholder”) ტერმინოლოგიური განმარტება იძლევა იმის შესაძლებლობას, რომ მასში მონაცემთა სუბიექტიც იყოს მოაზრებული, რამეთუ მასში იგულისხმება ნებისმიერი ისეთი პირი, რომლის ინტერესზე კორპორაციის საქმიანობა ზეგავლენის მომხდენია. იხ. *მახარობლიშვილი გ.,* კორპორაციული მართვის ზოგადი ანალიზი, 2015, 313-317.

მონაცემთა დაცვის სამართლის პერსპექტივიდან — მონაცემთა კანონიერი დამუშავებისა და მონაცემთა სუბიექტის უფლებების დაცვის ერთგვარი გარანტი. შესაბამისად, წინამდებარე კვლევის მიზანია შემდეგი თეზისის ჭეშმარიტების დადგენა: მონაცემთა დაცვის ოფიცერი უზრუნველყოფს კორპორაციისა და მონაცემთა სუბიექტის ინტერესებისა და უფლებების გონივრულ თანაფარდობას.

კვლევის ინტერდისციპლინური ხასიათი საკორპორაციო სამართლისა და პერსონალურ მონაცემთა დაცვის სამართლის ურთიერთდაკავშირების ერთგვარი მცდელობის შედეგია. და რაკი „[...] ყოველგვარი შეცნობა არის განმარტება“[5], საკვლევი საკითხისა და დარგის ცნებითი კატეგორიების გადმოსაცემად, ნაშრომი დესკრიფციული ხასიათისაა; გამოყენებულია ანალიტიკურ-სინთეზური მეთოდი შუალედური შედეგების ერთიან სისტემაში ფორმულირებისა და კვლევის მიზანთან მათი ლოგიკური კავშირის წარმოსაჩენად.

2. პერსონალურ მონაცემთა დაცვაზე ორიენტირი, როგორც კორპორაციული მართვის თანამედროვე მოდელი

ლიტერატურაში გამოთქმული პოზიციის თანახმად, არამატერიალური ეკონომიკის აღზევების ეპოქამ განაპირობა კაპიტალიზმის არსებობა კაპიტალის გარეშე.[6] პერსონალური მონაცემები სწორედ ასეთი არამატერიალური, თანამედროვე ტიპის კაპიტალია. მონაცემთა კანონიერი დამუშავების ვალდებულება კორპორაციის მიერ სათანადო ტექნიკური და ორგანიზაციული ღონისძიებების გატარებას, შესაბამისი შიდაორგანიზაციული სტრუქტურის ფორმირებასა და მართვის სისტემის დანერგვას საჭიროებს. კორპორაციული მართვა თავისი არსით არის საკუთრების (*სამეწარმეო საზოგადოებაში განხორციელებული აქციონერული კაპიტალის*) და კონტროლის (*გაერთიანებულ კაპიტალზე მართვის უფლებამოსილების მქონე ორგანოს*) გამიჯვნის, მართვისა და ხელმძღვანელობის იმგვარი სისტემა, რომელშიც გათვალისწინებულია აქციონერთა და დაინტერესებულ პირთა სამართლებრივი ინტერესები.[7] მართვის აღნიშნული სისტემა, ორგანიზაციული თვალსაზრისით შესაძლებელია, განხორციელდეს მონისტური ან დუალისტური სქემით.[8]

---

[5] *იასპერსი კ.,* ფილოსოფიის შესავალი, *გორგიშელი ვ. (თარგმ.)*, 2019, 73.

[6] იხ. *Haskel J., Westlake S.,* Capitalism without Capital: The Rise of the Intangible Economy, 2018, 3-10.

[7] *ბურდული ი., მახარობლიშვილი გ., თოხაძე ა., ზუბიტაშვილი ნ., ალადაშვილი გ., მაღრაძე გ., ეგნატაშვილი დ.,* საკორპორაციო სამართალი, 2022, 634-638.

[8] აღნიშნულს რიგ შემთხვევაში საწესდებო ავტონომია, ხოლო რიგ შემთხვევაში საკანონმდებლო მოთხოვნა უდევს საფუძვლად, იხ. მუხლები 124 და 182, „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-Xმპ, 02/08/2021.

კორპორაციულ მართვის სისტემას გააჩნია რამდენიმე სახის მოდელი, რომელიც გამოხატავს მის ძირითად ორიენტირს (*მაგალითად, არსებობს მენეჯერული მოდელი, აქციონერთა ქონებრივი მდგომარეობის მაქსიმიზაციაზე ორიენტირებული მოდელი, დასაქმებულ პირთა და დაინტერესებულ პირთა ინტერესების დაცვაზე ორიენტირებული მოდელი*).[9] ვიწრო გაგებით მოდელებს შორის სხვადასხვაობა განპირობებულია სწორედ კორპორაციის მმართველობითი პოლიტიკითა და სტრატეგიით, უფრო განზოგადებით კი — იმ გარემოს ეკონომიკური და სამართლებრივი ფაქტორებით, რომლის ფარგლებში ოპერირებს კორპორაცია.[10] შესაბამისად, თითოეული კორპორაციის მართვის მოდელი ინდივიდუალური სამეწარმეო საქმიანობის სფეროსა და მენეჯერული პოლიტიკის მიხედვით განსხვავდება. პერსონალურ მონაცემთა დაცვის ორიენტირით კორპორაციული მართვის განხორციელება ზემოხსენებულ მოდელთა ერთ-ერთ ნაირსახეობად შეიძლება შეფასდეს. ამგვარი მოდელი განსაკუთრებით საგულისხმოა ისეთი ეკონომიკური აქტორებისათვის, რომლებიც ახორციელებენ პერსონალური მონაცემების განსაკუთრებულად დიდი ოდენობით დამუშავებას, ასევე, რომელთა სამეწარმეო საქმიანობა არსებით ზეგავლენას ახდენს მონაცემთა სუბიექტების ინტერესებზე.

კორპორაციული მართვის ფუნდამენტური პრინციპებიდან[11] ერთ-ერთს წარმოადგენს გახსნილობა და გამჭვირვალობა, რომელიც ითვალისწინებს კორპორაციის ფინანსურ მდგომარეობასთან, მმართველობით სტრუქტურასთან, მართვასა და მენეჯმენტთან დაკავშირებული ინფორმაციის დროულ გამჟღავნებს. საგულისხმოა, რომ მონაცემთა დამუშავების პრინციპებიდან ერთ-ერთი სწორედ გამჭვირვალობის უზრუნველყოფას შეეხება, რომელიც ავალდებულებს დამმუშავებელს, უზრუნველყოს მონაცემთა სუბიექტისთვის მარტივი წვდომა ნებისმიერ ისეთ ინფორმაციაზე, რომელიც მონაცემთა დამუშავებას უკავშირდება.[12] აღსანიშნავია, რომ ევროპის საბჭოს კანონმდებლობაც[13] ადგენს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ანგარიშვალებულების მოვალეობას და დამატებით ვალდებულებებს პერსონალურ მონაცემთა ეფექტიანი

[9] *Tokhadze A.,* Enhancement of Corporate Social Responsibility – An Analysis from the Perspective of Economic and Sectoral Cooperation under the Three Association Ageements, in: Legal Aspects of the EU Association Agreements with Georgia, Moldova and Ukraine in the Context of the EU Eastern Partnership Initiative, *Trunk A., Panych N., Rieckhof S. (eds.),* 2017, 104-106.

[10] *მახარობლიშვილი გ.,* კორპორაციული მართვის ზოგადი ანალიზი, 2015, 161, 162-163.

[11] *G20/OECD*, Principles of Corporate Governance, 2015.

[12] პრეამბულა, §39, 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 L 119, 4/5/2016, 1–88. მე-4 მუხლის 1-ლი პუნქტის „ა“ ქვეპუნქტი, მე-15 მუხლი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.

[13] §84, Article 10, *Council of Europe,* Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.

დაცვის უზრუნველსაყოფად.[14] ამგვარ ღონისძიებათა ერთ-ერთ ფორმად მონაცემთა დაცვის ოფიცრის ინსტიტუტი მიიჩნევა.[15]

მაშასადამე, მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელს მეწარმე სუბიექტის სამეწარმეო საქმიანობის სფერო, მის ფარგლებში პერსონალური მონაცემის დამუშავების ინტენსივობა და მოცულობა აყალიბებს. მეორე მხრივ, სწორედ კორპორაციული მართვის ამგვარი მოდელის წიაღში ხორციელდება მონაცემთა სუბიექტის, როგორც „დაინტერესებული პირის“, სამართლებრივი ინტერესების გათვალისწინება. შესაბამისად, მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელის მიზანია: ა) კორპორაციის, როგორც მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის სრული შესაბამისობა მონაცემთა დაცვის საკანონმდებლო მოწესრიგებასთან; ბ) მონაცემთა სუბიექტის, როგორც „დაინტერესებული პირის“, უფლებების დაცვა.

3. მონაცემთა დაცვის ოფიცერი, როგორც პერსონალურ მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელის ელემენტი

ოფიცრის ინსტიტუტი მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელის ერთ-ერთი ელემენტია, თუმცა არა ერთადერთი. მონაცემთა დაცვის ზეგავლენის რისკების შეფასება (“Data Protection Impact Assessment”), მონაცემთა დაცვის შიდა პოლიტიკის არსებობა ანგარიშვალდებულების ერთგვარი გამოხატულებაა. ნაშრომის ფორმატიდან გამომდინარე, შეუძლებელია ოფიცრის ინსტიტუტის ყველა სამართლებრივი ასპექტის განხილვა, ამდენად, წინამდებარე თავიც ინსტიტუტის ძირითად მახასიათებლებზე აქცენტირდება.

3.1. მონაცემთა დაცვის ოფიცრისა და კორპორაციული შესაბამისობის ოფიცრის ფუნქციური ურთიერთგამიჯვნა

მონაცემთა დაცვის ოფიცერი არის მონაცემთა დაცვის კვალიფიციური ექსპერტი, რომლის ფუქნციაა კორპორაციის ხელმძღვანელობას კონსულტაცია გაუწიოს მონაცემთა დაცვის წესებთან შესაბამისობის უზრუნველსაყოფად.[16] განსხვავებით კორპორაციის ხელმძღვანელი პირებისაგან, მონაცემთა დაცვის ოფიცერი არ არის სამეწარმეო

[14] *Council of Europe,* Explanatory Report, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018, მუხლი 10.
[15] იქვე, § 87.
[16] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 198.

საზოგადოების ფიდუციარი[17] (*სხვა სიტყვებით კი სამეწარმეო საზოგადოების საუკეთესო ინტერესის განმახორციელებელი წარმომადგენელი*). იგი არც კორპორაციული შესაბამისობის ოფიცერია. თუმცა პარალელის გავლების მიზნით, შესაძლებელია ამ ორი ინსტიტუტის ფუნქციების ზოგადი შედარება.

კორპორაციული შესაბამისობა ანგლო-ამერიკული სამართლის ოჯახის პირმშოა. იგი აერთიანებს რიგ ღონისძიებებს, რომლის მეშვეობით ხორციელდება კორპორაციულ ინსაიდერთა (*ხელმძღვანელების, თანამშრომლების*) საქმიანობა საკანონმდებლო ნორმების შესაბამისად.[18] სწორედ კორპორაციული შესაბამისობის ოფიცერზე ხდება სამართლებრივი თუ ეკონომიკური გამოწვევებისა და ამონაცების განსაზღვრის დელეგირება. ერთი შეხედვით, მათი ფუნქციები თითქოს თანმხვედრია, თუმცა დაუშვებელია კორპორაციული შესაბამისობის ოფიცრისა და მონაცემთა დაცვის ოფიცრის ინსტიტუციური როლის ურთიერთაღრევა. ამ თვალსაზრისით საინტერესოა, რომ ინტერესთა კონფლიქტის მოტივით, ბელგიის მონაცემთა დაცვის საზედამხდველო ორგანომ დამმუშავებელი 50 000 ევროს ოდენობით დააჯარიმა, რადგან მონაცემთა ოფიცრის პოზიციაზე დაინიშნა პირი, რომელიც ამავდროულად იყო კორპორაციული შესაბამისობის სამსახურის უფროსი, ფულის გათეთრების ანგარიშგების ოფიცერი.[19]

გარდა ამისა, აუცილებელია, რომ მონაცემთა დაცვის ოფიცერს ჰქონდეს სათანადო კვალიფიკაცია, მონაცემთა დაცვის დარგის საექსპერტო ცოდნა და შესაძლებლობა, რომ დამოუკიდებლად განახორციელოს მასზე დაკისრებული მოვალეობა.[20] ამდენად, მის მიმართ მოქმედებს კომპეტენტურობის პრინციპი. მონაცემთა დაცვის ოფიცერი ანგარიშვალდებულია უშუალოდ მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის პირველი რანგის ხელმძღვანელთა წინაშე,[21] რაც პერიოდული ანგარიშის წარდგენასაც მოიაზრებს როგორც ანგარიშვალდებულების პრინციპის პრაქტიკული გამოხატულება. ოფიცრის დამოუკიდებლობის უზრუნველყოფის მიზნით, დაუშვებელია მისთვის დამმუშავებლის ან უფლებამოსილის მიერ რაიმე სახის ინსტრუქციის ან დავალებების მიცემა.[22] საპირწონედ, კორპორაციული შესაბამისობის ოფიცრის ფუნქცია შესაძლებელია, რომ კორპორციის რომელიმე სტრუქტურულ ერთეულში დაინერგოს. ამას გარდა, განსხვავებით კორპორაციული შესაბამისობის ოფიცრისგან, მონაცემთა

[17] ფიდუციალური მოვალეობის მატარებელნი არიან კორპორაციის ხელმძღვანელი პირები, რომლებიც სამეწამეო გადაწყვეტილებას საზოგადოების საუკეთესო ინტერესებიდან გამომდინარე იღებენ. *Schneeman A.,* Law of Corporations and Other Business Organizations, 2010, 39.

[18] იქვე, 363.

[19] Autorité de protection des données, Dossiernummer: DOS-2019-04309, 2020, <https://cedpo.eu/dpo-case-law/> [20.01.2023].

[20] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 56-57.

[21] მუხლი 38(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 L 119, 4/5/2016, 1–88.

[22] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 59.

დაცვის ოფიცერს აქტიური კავშირი აქვს გარე აქტორებთანაც (*მაგალითად, მონაცემთა სუბიექტთან, მონაცემთა დაცვის საზედამხედველო ორგანოსთან*). შესაბამისად, სავალდებულოა მისი საკონტაქტო ინფორმაციის გამჟღავნება, ხოლო ოფიცრის დანიშვნის თაობაზე მონაცემთა დაცვის საზედამხედველო ორგანოს ინფორმირება.[23]

მონაცემთა დაცვის ოფიცრის ფუნქცია სამ სეგმენტს მოიცავს: ინფორმირების, თანამშრომლობისა და ზედამხედველობის ვალდებულებებს.[24] პირველში მოიაზრება დამმუშავებლისათვის/უფლებამოსილი პირისთვის მონაცემთა დამუშავების თაობაზე სათანადო კონსულტაციის გაწევა; მეორე გულისხმობს მონაცემთა დაცვის საზედამხედველო ორგანოსთან აქტიურ კავშირსა და თანამშრომლობას; მესამე კი — მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან შესაბამისობის ზედამხედველობას.[25] ამ ფუნქციების ჯეროვნად განხორციელების მიზნით, იგი უფლებამოსილია, ჩაატაროს ინსპექტირება, ჰქონდეს წვდომა პერსონალურ მონაცემებზე, გაეცნოს მონაცემთა სუბიექტების განცხადებებს და ამ მიზნით დამოუკიდებლად განახორციელოს ნებისმიერი ქმედება ეთიკის სტანდარტის ფარგლებში.[26]

3.1. მონაცემთა დაცვის ოფიცრის დანიშვნის წინაპირობა

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულებას სამ ცალკეულ შემთხვევაში ითვალისწინებს.[27] კერძო სექტორში ოპერირებადი მეწარმე სუბიექტში ოფიცრის ინსტიტუტის არსებობა უკავშირდება დამმუშავებლის ან უფლებამოსილი პირის იმგვარ ძირითად საქმიანობას, რომლის ფარგლებში განხორციელებული ოპერაციები ფართო მასშტაბით ითვალისწინებს მონაცემთა სუბიექტის რეგულარულ, სისტემურ მონიტორინგს ან თუკი მათი ძირითადი საქმიანობა უკავშირდება განსაკუთრებული კატეგორიის მონაცემთა ფართომასშტაბიან დამუშავებას.[28] აღნიშნულ განმარტებაში საგულისხმოა დამმუშავებლის ან უფლებამოსილი პირის „ძირითადი საქმიანობა“ და მის ფარგლებში განხორციელებული ოპერაციების „კვალიტატური“ (*ე. ი. „ხარისხობრივი“*) და

[23] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 10.
[24] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.
[25] იქვე.
[26] *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13.
[27] მუხლი 37, 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 L 119, 4/5/2016, 1–88.
[28] იქვე, მუხლი 37(1).

„კვანტიტატური“ (*ე. ი. „რაოდენობრივი“*) მაჩვენებლები. რაკი კორპორაციულსამართლებრივი გაგებით ძირითადი, იგივე ჩვეულებრივი სამეწარმეო საქმიანობა და კერძო სამართლის იურიდიული პირის ზოგადი უფლებაუნარიანობის ფარგლებში განხორციელებული დამხმარე ეკონომიკური საქმიანობა სხვადასხვა ცნებებია[29], ოფიცრის დასანიშნად მნიშვნელოვანია, რომ მეწარმე სუბიექტის მიერ პერსონალური მონაცემები მუშავდებოდეს მოგების მიღების მიზნით, ორგანიზებულად, მართლზომიერად, არაერთჯერადად და დამოუკიდებლად განხორციელებული[30] ძირითადი სამეწარმეო საქმიანობის ფარგლებში. ასევე უნდა შეფასდეს, პერსონალურ მონაცემთა დამუშავების მასშტაბი, რომელიც განისაზღვრება შემდეგი კრიტერიუმებით: ა) მონაცემთა სუბიექტების რაოდენობა; ბ) დამუშავებულ მონაცემთა მოცულობა; გ) დამუშავების ხანგრძლივობა; დ) დამუშავების გეოგრაფიული დაფარვა.[31] ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს მონაცემთა დაცვის ოფიცრის დანიშვნის სხვა საფუძვლებსაც. მაგალითად, გერმანიის მონაცემთა დაცვის ფედერალური აქტის თანახმად, იმ კერძო კომპანიაში, რომელშიც დასაქმებულია სულ მცირე 20 თანამშრომელი, რომელსაც შემხებლობა აქვს პერსონალურ მონაცემთა ავტომატურ დამუშავებასთან, სავალდებულოა მონაცემთა დაცვის ოფიცრის დანიშვნა.[32] ოფიცრის არსებობა ასევე აუცილებელია, თუკი ხორციელდება მონაცემთა იმგვარი დამუშავება, რომელიც ექვემდებარება დამუშავების ზეგავლენის შეფასების კვლევას ან თუკი პერსონალური მონაცემები მუშავდება კომერციული გადაცემის, ანონიმური გადაცემის ან ბაზრის ან აზრის კვლევის მიზნებისთვის.[33]

რაც შეეხება მონაცემთა დაცვის ოფიცრის კლასიფიკაციას — განასხვავებენ შიდა და გარე ოფიცრის ინსტიტუტებს.[34] შიდა ოფიცერი კორპორაციაში დასაქმებული პირია, ხოლო მეორე — კორპორაციასთან გარიგებითსამართლებრივი გზით (*ხელშეკრულებით*) დაკავშირებული პირი. ასევე შესაძლებელია სავალდებულო და ნებაყოფლობითი ოფიცრის ინსტიტუტების გამიჯვნა. როგორც წინა პარაგრაფში იქნა წარმოჩენილი, განხილულ შემთხვევებში ოფიცრის განსაზღვრა სავალდებულოა[35], თუმცა აღნიშნული არ გამორიცხავს კომპანიის მიერ ოფიცრის ნებაყოფლობით, თვითრეგულირებისა და

[29] *ბურდული ი., მახარობლიშვილი გ., თოხაძე ა., ზუბიტაშვილი ნ., ალადაშვილი გ., მაღრაძე გ., ეგნატაშვილი დ.,* საკორპორაციო სამართალი, 2022, 60-63.

[30] მე-2 მუხლის მე-2 პუნქტი, „მეწარმეთა შესახებ“ საქართველოს კანონი, №875-Vრს-Xმპ, 02/08/2021.

[31] *Kuner Ch., Bygrave L., Docksey Ch.,* The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 693.

[32] § 38, Bundesdatenschutzgesetz, (BDSG), 30/06/2017.

[33] იქვე.

[34] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 57.

[35] სტატიის მიზნებიდან გამომდინარე, ნაშრომში არ განიხილება მონაცემთა დაცვის ოფიცრის სავალდებულო დანიშვნის შემთხვევა საჯარო უწყებაში. იხ. მუხლი 37(1), 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 L 119, 4/5/2016, 1–88.

საწესდებო ავტონომიის ფარგლებში დანიშვნას. ცხადია, ეს კორპორაციული მართვის კარგ კულტურასა და ანგარიშვალდებულების მაღალ სტანდარტზე მიუთითებს. მონაცემთა დაცვის ზოგადი რეგულაცია (მუხლი 37(2)) განსაზღვრავს საერთო ოფიცრის ინსტიტუტსაც, როდესაც რამდენიმე დამმუშავებელს/უფლებამოსილ პირს ჰყავს ერთი ოფიცერი. აღნიშნული საკმაოდ პრაქტიკულია კორპორაციული კონსორციუმებისთვის, ორგანიზაციათა ჯგუფისთვის, ჰოლდინგური კომპანიებისათვის.

როგორც ზემოთ აღინიშნა, დანიშვნის ერთ-ერთ წინაპირობას სათანადო პროფესიული კვალიფიკაცია წარმოადგენს. კომენტატორული ლიტერატურის თანახმად, ეს ოფიცრის სერტიფიცირებას, ბიზნეს სექტორის ადმინისტრირების ზოგადი წესების ცოდნას უკავშირდება.[36]

3.2. ოფიცრის დამოუკიდებლობა და ინტერესთა კონფლიქტის აკრძალვა

მონაცემთა დაცვის ოფიცერი უნდა იყოს აღჭურვილი შესაბამისი რესურსით, რაც უზრუნველყოფს მის მიერ საკუთარი მოვალეობის დამოუკიდებლად, დროულად და კვალიფიციურად შესრულებას.[37] აკრძალულია მასზე რაიმე სახის ზეგავლენა ან ზეწოლა. ასევე დაუშვებელია, რომ კორპორაციაში იგი იკავებდეს იმგვარ პოზიციას, რომელიც მას შესაძლებლობას მისცემს, განსაზღვროს მონაცემთა დამუშავების მიზანი და საშუალება.[38] შესაბამისად, იგი არ უნდა იყოს მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი. ამასთანავე აღსანიშნავია, რომ მონაცემთა დაცვის ოფიცერმა შესაძლებელია, შეითავსოს სხვა ფუნქციები იმ პირობით, თუკი აღნიშნული არ იწვევს ინტერესთა კონფლიქტს.[39] ინტერესთა კონფლიქტი სწორედ მაშინ არის სახეზე, როდესაც ოფიცერი პარალელურად იმგვარ ფუნქციას ასრულებს, რომელიც პირდაპირ წინააღმდეგობაში მოდის იმ ორგანიზაციის მონაცემთა დაცვის ინტერესთან, რომელშიც იგი ფუნქციონირებს.[40] მოცემულ შემთხვევაში, აუცილებელია მონაცემთა დაცვის ოფიცრის მხრიდან მსგავსი ინტერესთა კონფლიქტის გაცხადება, გამჟღავნება. კორპორაციულსამართლებრივი თვალსაზრისით ინტერესთა კონფლიქტის საკითხი დღის წესრიგში არ დგას, როდესაც ორგანიზაციათა გარკვეულ ჯგუფს საერთო ოფიცერი

[36] *Kuner Ch., Bygrave L., Docksey Ch.,* The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 695.
[37] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 58-59.
[38] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 24.
[39] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.
[40] *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 15.

ჰყავს. თუმცა, როგორც ეს ზემოთ იქნა აღნიშნული, მონაცემთა დაცვის ოფიცერს უნდა შეეძლოს საკუთარი ფუნქციის სრულყოფილი განხორციელება.

საინტერესოა მონაცემთა დაცვის საზედამხედველო ორგანოების პრაქტიკა: სლოვენიის მონაცემთა დაცვის საზედამხედველო ორგანომ კომპანიის მთავარი აღმასრულებელი დირექტორის ან დირექტორთა ბორდის წევრის მონაცემთა დაცვის ოფიცრად დანიშვნის ფაქტი ინტერესთა კონფლიქტად ცნო და დაუშვებლად მიიჩნია.[41] 2019 წელს ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი კორპორაცია 25 000 ევროს ოდენობით დააჯარიმა, რადგან მონაცემთა დაცვის ოფიცრის ფუნქცია შიდაკორპორაციულ სტრუქტურაში შექმნილ ორგანოს ე. წ. „მონაცემთა დაცვის შიდა ბორდს“ მიანიჭა, რომელიც დამმუშავებლის განმარტებით, სწორედ იმავე ფუნქციას ასრულებდა, რასაც მონაცემთა დაცვის ოფიცერი.[42]

ევროპის მონაცემთა დაცვის ზედამხედველის (*European Data Protection Supervisor*) რეკომენდაციის თანახმად, მონაცემთა დაცვის ოფიცერი არ უნდა იყოს კორპორაციაში ვადიანი ან მოკლევადიანი ხელშეკრულებით დასაქმებული პირი; მას უნდა ჰქონდეს ეკონომიკური სახსრების დამოუკიდებლად განკარგვის შესაძლებლობა და უნდა იყოს ანგარიშვალდებული მხოლოდ კორპორაციის ტოპ-მენეჯმენტის წინაშე.[43]

შესაბამისად, მონაცემთა დაცვის ოფიცრის მიმართ, სხვა ზემოხსენებულ პრინციპებთან ერთად, ასევე მოქმედებს დამოუკიდებლობის პრინციპი და ინტერესთა კონფლიქტის აკრძალვის მოთხოვნა. დამოუკიდებლობისა და მიუკერძოებლობის პრინციპის ლოგიკური გაგრძელებაა სათანადო ანაზღაურების წესი, რასაც საკორპორაციო სამართლაშიც ხელმძღვანელ პირთა დამოუკიდებლობის უზრუნველყოფის თვალსაზრისით[44] გარკვეული მნიშვნელობა აქვს მინიჭებული.

3.3. ოფიცრის პასუხისმგებლობის საკითხი

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია არ შეიცავს მონაცემთა დაცვის ოფიცრის პასუხისმგებლობის მომწესრიგებელ ცალკეულ დებულებას. მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან შეუსაბამობისათვის მონაცემთა დაცვის ოფიცრის პერსონალური პასუხისმგებლობა არ დგება. თუმცა აღსანიშნავია, რომ მასზე

[41] *Informacijski pooblaščenec,* Advisory Opinion, N07121-1/2021/577, 2021, <https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts> [22.01.2023].

[42] *Agencia Española Proteccion Datós,* Resolución de procedimiento sancionador, Procedimiento №: PS/00417/2019, იხ.: <https://cedpo.eu/dpo-case-law/> [22.01.2023].

[43] *European Data Protection Supervisor,* Data Protection Officer (DPO), <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> [20.01.2023].

[44] ხელმძღვანელ პირთა ანაზღაურების წესზე იხ. *Schneeman A.,* Law of Corporations and Other Business Organizations, 2010, 348-349.

ვრცელდება ერთგულების მოვალეობა სწორედ იმ ორგანიზაციის მიმართ, რომელშიც იგი იქნა დანიშნული.[45] ოფიცერი მოქმედებს შინაგანი პროფესიული რწმენის საფუძველზე, რაც გულისხმიერების პრინციპს უკავშირდება. შესაბამისად, მას აქვს თითოეული შემთხვევის გულისხმიერად და დაყოვნების გარეშე შესწავლის ვალდებულება.[46]

მონაცემთა დაცვის ოფიცერზე ასევე ვრცელდება კონფიდენციალურობის ვალდებულება.[47] კორპორაციული მართვის სისტემაში დუმილის მოვალეობის კონცეფციაც, რომელიც ხელმძღვანელ პირებსა და სამეთვალყურეო საბჭოს წევრებს აკისრიათ, სწორედ ინსაიდერული ინფორმაციის დაცვის მიზანს ემსახურება.[48] მისი შემსუბუქება ან გამორიცხვა დაუშვებელია.[49]

ნაკისრ ვალდებულებათა არაკეთილსინდისიერი და არაჯეროვანი შესრულება მონაცემთა დაცვის ოფიცრის პირდაპირ პასუხისმგებლობას უკავშირდება. ამ თვალსაზრისით სამეცნიერო ლიტერატურაში საუბარია გარე ოფიცრის სახელშეკრულებოსამართლებრივ პასუხისმგებლობაზე, ხოლო მონაცემთა სუბიექტის ჭრილში — მის დელიქტურ პასუხისმგებლობაზე.[50] რაც შეეხება შიდა ოფიცერს, მისი პასუხისმგებლობა შრომითსამართლებრივი საფუძვლით დგება.[51]

3.4. ოფიცრის გაწვევა

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია არ აწესრიგებს ოფიცრის გაწვევის, მასთან სამართლებრივი ურთიერთობის შეწყვეტის საკითხს. შესაბამისად, აღნიშნული ევროკავშირის წევრი სახელმწიფოს ეროვნული კანონმდებლობით რეგულირების საგანს წარმოადგენს. რეგულაციის 38(3)-ე მუხლის თანახმად, დაუშვებელია ოფიცრის სამსახურიდან დათხოვნა ან ჯარიმის დაკისრება, მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ მასზე დაკისრებული ფუნქციების შესრულების გამო. ოფიცერი ვერ იქნება გაწვეული მარტოოდენ იმ მიზეზით, რომ მონაცემთა დამუშავების შესახებ მის მიერ გაცემულ კონსულტაციას არ ეთანხმება

[45] *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 14-15.
[46] იქვე, 15.
[47] მუხლი 38(5), 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 L 119, 4/5/2016, 1–88.
[48] *ჭანტურია ლ.,* კორპორციული მართვა და ხელმძღვანელთა პასუხისმგებლობა საკორპორაციო სამართალში, 2006, 360-361.
[49] იქვე, 362.
[50] *Paal P. B., Pauly D. A.,* Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.
[51] იქვე.

მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი.[52] საკითხის ამგვარად რეგულირება ქმნის დამმუშავებლის/უფლებამოსილი პირის ზეწოლისაგან ოფიცრის დაცვის მაღალ სტანდარტს, რაც, ბუნებრივია, დადებითად აისახება მის დამოუკიდებლობაზე. მეორე მხრივ, აღნიშნული არ მიემართება ოფიცერთა მხრიდან უხეშ გაუფრთხილებლობას ან კანონდარღვევის შემთხვევებს.

ევროპული მართლმსაჯულების სასამართლომ 2022 წლის 22 ივნისის გადაწყვეტილებაში საქმეზე: "Leistritz AG v. LH" აღნიშნა, რომ რეგულაციის ზემოხსენებული მოთხოვნა (რეგულაციის 38(3)-ე მუხლის ფარგლებში) ვრცელდება როგორც შიდა, ისე გარე ოფიცერზე; წევრი სახელმწიფოს ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს ოფიცერთან ხელშეკრულების შეწყვეტის შესაძლებლობას მხოლოდ სამართლიანი საფუძვლით, მაშინაც კი, თუკი ხელშეკრულების შეწყვეტა არ უკავშირდება ოფიცრის ამოცანების შესრულებას, რამდენადაც ეს ხელს არ უშლის ზოგადი რეგულაციით დასახული მიზნის მიღწევას.[53] აღნიშნული წარმოადგენს ოფიცრის დამოუკიდებლობის დამატებით გარანტს, რაც თავის მხრივ უზრუნველყოფს ევროკავშირის მასშტაბით მონაცემთა დამუშავებასთან დაკავშირებული უფლებების მომწესრიგებელი რეგულაციების ჰომოგენურ და თანმიმდევრულ განხორციელებას.[54] უფრო მეტიც, ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს ოფიცრის განთავისუფლებისაგან გაცილებით ძლიერი დაცვის მექანიზმს, ვიდრე ეს ევროკავშირის ზოგადი რეგულაციითაა დადგენილი.[55]

4. დასკვნა

პერსონალურ მონაცემთა დაცვის საერთაშორისო დონეზე აღიარებულმა სტანდარტები კორპორაციების მმართველობის სტრატეგიაზეც აისახა. აღნიშნული განაპირობებს კორპორაციული მართვის ახალი მოდელის ჩამოყალიბებას, რომელიც მონაცემთა სუბიექტის უფლებებისა და ინტერესის დაცვაზეა ორიენტირებული. ამგვარი მმართველობითი პოლიტიკა წინამდებარე სტატიაში დასახელებულია, როგორც პერსონალურ მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელი. მისი მმართველობით სისტემაში დანერგვა უზრუნველყოფს კორპორაციის შესაბამისობას მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან, აგრეთვე,

[52] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 15.
[53] CJEU, C-534/20, *Leistritz AG v. LH* [2022], პარა. 23-24, 36.
[54] იქვე, პარა. 26.
[55] იქვე, პარა. 33-36.

მონაცემთა სუბიექტის – როგორც „დაინტერესებული პირის“ ინტერესების გათვალისწინებას კორპორაციული მართვის სისტემაში. ამგვარი მოდელის ერთ-ერთ ელემენტს მონაცემთა დაცვის ოფიცერი წარმოადგენს. იგი უზრუნველყოფს, ერთი მხრივ, მეწარმე სუბიექტის, ხოლო მეორე მხრივ – მონაცემთა სუბიექტის სამართლებრივი და ეკონომიკური ინტერესების თანაფარდობას. აღნიშნული მიზნის განსახორციელებლად, ოფიცერი აღჭურვილია შესაბამისი სამართლებრივი ბერკეტებით. კერძოდ, მის მიმართ მოქმედებს დამოუკიდებლობის, კონფიდენციალურობის, კომპეტენტურობის, ანგარიშვალდებულების პრინციპები. გარდა ამისა, იგი დაცულია კორპორაციულ ინსაიდერთა (*იგულისხმებიან ხელმძღვანელები, სამეთვალყურეო საბჭოს წევრები*) პირდაპირი ან არაპირდაპირი ზეგავლენისგან. თავის მხრივ ოფიცრის მიმართ მოქმედი კომპეტენტურობის, გულისხმიერების პრინციპები, ასევე, ინტერესთა კონფლიქტის აკრძალვა ემსახურება მონაცემთა სუბიექტის უფლების დაცვის ეფექტიან განხორციელებას და კორპორაციის მონაცემთა დაცვის მარეგულირებელ აქტებთან შესაბამისობას.

მონაცემთა დაცვის ოფიცრის ინსტიტუტის ეკონომიკურ-სამართლებრივ ანალიზზე[56] დაყრდნობით შეიძლება ითქვას, რომ იგი უზრუნველყოფს კორპორაციულ შესაბამისობასთან დაკავშირებულ იმ დამატებითი ხარჯის შემცირებას, რაც მეწარმე სუბიექტმა მონაცემთა დაცვის მომწესრიგებელ აქტებთან შეუსაბამობით (*მაგალითად, დაკისრებული ჯარიმის სახით*) შეიძლება, რომ განიცადოს. ოფიცრის ნებაყოფლობითი დანიშვნა სწორედ ამ ეკონომიკური ხარჯის შემცირებას ემსახურება და როგორც ეს ნაშრომში არის შეფასებული, კორპორაციული მართვის, პერსონალურ მონაცემთა დაცვის მაღალ კულტურაზე მიანიშნებს.

დღესდღეობით მონაცემთა დაცვის ოფიცრის ინსტიტუტი ჯერ-ჯერობით უცხოა ეროვნული საკანონმდებლო მოწესრიგებისათვის. მიუხედავად ამისა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი[57] მის ინსტიტუტიურ მოწესრიგებას ითვალისწინებს, რაც დადებით ზეგავლენას იქონიებს, მათ შორის, სამეწარმეო საზოგადოებების პერსონალურ მონაცემთა დამუშავებისადმი ცნობიერების ამაღლებასა და კორპორაციული მართვის თანამედროვე მოდელის პრაქტიკაში დამკვიდრებაზე.

[56] იგულისხმება სამართლის ეკონომიკური ანალიზი, როგორც სამართლის მეცნიერებაში დამკვიდრებული მეთოდი, *Posner R.,* Economic Analysis of Law, 2011, 1-3.

[57] მუხლი 33, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი№ 07-3/353/9, 22/05/2019, <www.parliament.ge> [23.01.2023].

ბიბლიოგრაფია:

1. „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-Xმპ, 02/08/2021.
2. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
3. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი, № 07-3/353/9, 22/05/2019, <www.parliament.ge> [23.01.2023].
4. *ბურდული ი., მახარობლიშვილი გ., თოხაძე ა., ზუბიტაშვილი ნ., ალადაშვილი გ., მაღრაძე გ., ეგნატაშვილი დ.,* საკორპორაციო სამართალი, 2022, 60-63, 634-638.
5. *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 198.
6. *იასპერსი კ.,* ფილოსოფიის შესავალი, *გორგიშელი ვ. (თარგმ.)*, 2019, 73.
7. *მახარობლიშვილი გ.,* კორპორაციული მართვის ზოგადი ანალიზი, 2015, 161, 162-163, 313-317.
8. *ჭანტურია ლ.,* კორპორციული მართვა და ხელმძღვანელთა პასუხისმგებლობა საკორპორაციო სამართალში, 2006, 360-36, 362.
9. 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 L 119, 4/5/2016, 1–88.
10. *Council of Europe,* Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
11. *Council of Europe,* Explanatory Report, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
12. Bundesdatenschutzgesetz, (BDSG), 30/06/2017.
13. *OECD*, Principles of Corporate Governance, 2015.
14. *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 10, 15, 24.
15. *Bentham J.,* Of Laws in General, *Hart H. L. A. (ed.),* 1970, 31-33.
16. *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13, 14-15.
17. *European Data Protection Supervisor,* Data Protection Officer (DPO), <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> [20.01.2023].
18. *Haskel J., Westlake S.,* Capitalism without Capital: The Rise of the Intangible Economy, Princeton, 2018, 3-10.

19. *Johnson A.,* Soft Law, in: EC Regulation of Corporate Governance, UK, 2009, 343-347.
20. *Kuner Ch., Bygrave L., Docksey Ch.,* The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 693, 695.
21. *Magnier V.,* Comparative Corporate Governance, Legal Perspectives, 2017, 1-4.
22. *Paal P. B., Pauly D. A.,* Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.
23. *Posner R.,* Economic Analysis of Law, 2011, 1-3.
24. *Picciotto S.,* Regulating Global Corporate Capitalism, 2011, 61-65, 193-200.
25. *Schneeman A.,* Law of Corporations and Other Business Organizations, 2010, 39, 348-349, 363.
26. *Tokhadze A.,* Enhancement of Corporate Social Responsibility – An Analysis from the Perspective of Economic and Sectoral Cooperation under the Three Association Ageements, in: Legal Aspects of the EU Association Agreements with Georgia, Moldova and Ukraine in the Context of the EU Eastern Partnership Initiative, *Trunk A., Panych N., Rieckhof S. (eds.),* 2017, 104-106.
27. *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 56-60.
28. CJEU, C-534/20, *Leistritz AG v. LH* [2022].
29. *Autorité de protection des données*, Dossiernummer: DOS-2019-04309, 2020, <https://cedpo.eu/dpo-case-law/> [20.01.2023].
30. *Agencia Española Proteccion Datós,* Resolución de procedimiento sancionador, Procedimiento Nº: PS/00417/2019, იხ.: <https://cedpo.eu/dpo-case-law/> [22.01.2023].
31. *Informacijski pooblaščenec,* Advisory Opinion, N07121-1/2021/577, 2021, <https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts> [22.01.2023].

ქეთევან კრაწაშვილი*

სად მთავრდება ჩემი პერსონალური მონაცემები?

ინფორმაციული თვითგამორკვევა ადამიანის არაერთი ძირითადი უფლების რეალიზებას განაპირობებს. მაგალითად, პიროვნების თავისუფალი განვითარება დაფუძნებულია საკუთარი ნების, გადაწყვეტილების, არჩევანის შესაბამისად განვითარების შესაძლებლობაზე, რისთვისაც საჭიროა იმის გამორკვევაც რა იციან დაინტერესებულმა პირებმა ჩვენს შესახებ. საკუთარ თავზე მონაცემების მაქსიმალური სიზუსტით იდენტიფიცირება ადამიანს საშუალებას აძლევს შექმნას, დაიცვას და აკონტროლოს თავისი პრივატული სფერო. გამიჯნოს სივრცე, რომელშიც საზოგადოებრივი აზრისთვის ანგარიშის გაწევის გარეშე შეუძლია, განავითაროს პიროვნება, სივრცისგან, რომელშიც მისი მანერები, ქცევები, მოსაზრებები, ინდივიდუალური მახასიათებლები დაკვირვების თუ სხვადასხვა ფორმით დამუშავების ობიექტი ხდება. ყველას აქვს უფლება დაიცვას საკუთარი თავი სხვების გადაჭარბებული ცნობისმოყვარეობისგან. რაც უფრო სრულყოფილი წარმოდგენა აქვს ადამიანს თავისი მონაცემების გავრცელების მასშტაბზე, მით უკეთ ახერხებს პირადი ცხოვრების დაცვას. საკუთარი უფლების რეალიზებისთვის კი, ამ უფლების სიღრმისეული ცოდნა საუკეთესო იარაღია. ინდივიდის შესახებ თითოეული მონაცემი მისი იდენტობის ნაწილია, თუმცა ხშირად დისკუსიის საგანია კონკრეტულ ადამიანთან გარკვეული ინფორმაციის დაკავშირება, მის შესახებ მონაცემად განხილვა.

საკვანძო სიტყვები: *პერსონალური მონაცემები, ინფორმაციული თვითგამორკვევა, ფიზიკური პირი, მონაცემთა სუბიექტი, დამუშავება, მონაცემთა დამმუშავებელი, მონაცემთა დაცვის ზოგადი რეგულაცია, კონვენცია.*

* ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი; პერსონალურ მონაცემთა დაცვის სამსახურის საჯარო სექტორზე ზედამხედველობის დეპარტამენტის უფროსი.

1. შესავალი

კომერციული, პროფესიული თუ სახელმწიფო ინტერესების უკან, როგორც წესი, დიდი რაოდენობის პერსონალური მონაცემები დგას. მაგალითად, მართლწესრიგის დასამკვიდრებლად, საარსებო პირობების უზრუნველსაყოფად, პიროვნული განვითარებისთვის, სოციალური კეთილდღეობის მისაღწევად, საზოგადოებრივი უსაფრთხოების დასაცავად თუ მატერიალური დოვლათის შესაქმნელად სახელმწიფო და კერძო დაწესებულებები ადამიანებისგან მუდმივად მოითხოვენ ინფორმაციას. ეს ინფორმაცია კი დიდწილად მათი პერსონალური მონაცემებია. ერთად თავმოყრილი მონაცემები როგორც წესი ჯაჭვურად ვრცელდება ერთი დაინტერესებული მონაცემთა დამმუშავებლიდან მეორეზე. ამ პროცესში კი ხშირად ადამიანი ინფორმაციულ კავშირს წყვეტს იმ პირებთან, რომლებისთვის პირადად და გაცნობიერებულად არ მიუწოდებია საკუთარ თავზე ინფორმაცია.

კონკრეტულ ინფორმაციაზე წვდომის შესაძლებლობა და ამ შესაძლებლობის დამკვიდრებაში პოზიტიური სამართლის როლი არსებითად აქტიურია მაშინ, როდესაც საქმე ინდივიდის მონაცემებს ეხება, დაინტერესებული პირი კი თავად მონაცემთა სუბიექტია[1]. პერსონალური მონაცემები თითოეული ჩვენგანის შესახებ ზღვა ინფორმაციას ნიშნავს, რომლის დაცვაც პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვას უტოლდება. პერსონალური მონაცემების დაცვის სამართალი, რომელიც ტექნოლოგიური პროგრესის კვალდაკვალ სწრაფად ვითარდება განსაკუთრებულ ყურადღებას ადამიანის ინფორმაციული თვითგამორკვევის პროცესს უთმობს და მას მკაფიო, რეალური შესაძლებლობებით აღჭურავს. ამ შესაძლებლობების სათავე კონსტიტუციითაა[2] განმტკიცებული. პოზიტიური სამართლით მიკუთვნებული ინფორმაციული თვითგამორკვევის უფლებით ინდივიდის მიერ სარგებლობა, საკუთარ თავზე ინფორმაციის მოპოვება, მისი კანონიერების გაკონტროლებაში მონაწილეობა და ამდენად საკუთარი პირადი ცხოვრების ხელშეუხებლობის დაცვა დიდწილად პერსონალური მონაცემების სწორად იდენტიფიცირებაზეა დამოკიდებული.

თითოეული ჩვენგანის პირადი ინფორმაცია ხშირად გარკვეული მოვლენების შესახებ გარემოებებს, მაგალითად თარიღებს, ადგილმდებარეობებს, ემოციებს, გრძნობებს, მოსაზრებებს, შეხედულებებს, სხვა ადამიანების მონაცემებს და კიდევ არაერთ ინფორმაციას მოიცავს. გარკვეულ კრიტერიუმებზე დამყარებული მიდგომის

[1] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011. მე-2 მუხლის „ვ“ ქვეპუნქტი.
[2] საქართველოს კონსტიტუცია, 786- რს, 24/08/1995, მე-18 მუხლი.

ჩამოყალიბების გარეშე, შეუძლებელია ზუსტად დადგინდეს, სად მთავრდება ერთი კონკრეტული ადამიანის შესახებ მონაცემები.

წინამდებარე ნაშრომი მკითხველს ზემოაღნიშნული გამოწვევის დაძლევაში დაეხმარება. ნაშრომი შედგება შესავლისგან, პერსონალური მონაცემების განმარტების სამართლებრივი ასპექტებისა და ცნების ელემენტების განმსაზღვრელი ქვეთავებისგან, ასევე, დასკვნისგან. მასში გაანალიზებულია პრაქტიკულ შემთხვევებზე დამყარებული კრიტერიუმები და პერსონალური მონაცემების იდენტიფიცირების შესახებ რამდენიმე კონცეპტუალური მიდგომა, რომლებსაც საკითხის გადაწყვეტისას უნდა მიექცეს ყურადღება. ნაშრომი გამოსადეგი იქნება ინდივიდუალური შემთხვევების გასაანალიზებლად, როგორც მონაცემთა სუბიექტებისთვის, ასევე დაინტერესებული მონაცემთა დამმუშავებლებისთვის.

2. პერსონალური მონაცემების განმარტების პრაქტიკულ-სამართლებრივი ასპექტები

ევროკავშირისა და ევროპის საბჭოს კანონმდებლობა „პერსონალურ მონაცემებს“ განმარტავს, როგორც ინფორმაციას იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირის შესახებ, რომლის ვინაობა ცნობილია, ან შეიძლება დადგინდეს დამატებითი ინფორმაციის საფუძველზე.[3] არის თუ არა პირი იდენტიფიცირებადი, ამის გასარკვევად მონაცემთა დამმუშავებელმა, მონაცემების მიმღებმა ან სხვა სუბიექტმა უნდა გაითვალისწინოს ყველა გონივრული საშუალება, რომელთა გამოყენებაც პირის პირდაპირი ან ირიბი იდენტიფიცირებისათვის (მაგ.: პირის ამოცნობა, რომელიც იძლევა ერთი ადამიანის განსხვავებულად მოპყრობის შესაძლებლობას მეორე ადამიანის მხრიდან) არის შესაძლებელი.[4] „თუ რამდენად არსებობს გონივრული შესაძლებლობა, რომ გამოყენებული იქნება ფიზიკური პირის იდენტიფიცირების საშუალებები, გასათვალისწინებელია ყველა ობიექტური ფაქტორი, როგორიცაა იდენტიფიკაციისთვის საჭირო დრო, მისი ღირებულება, ასევე, დამუშავების მომენტისათვის არსებული ტექნოლოგიები და ტექნოლოგიური განვითარების დონე.“[5]

[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 L 119, 4/5/2016, 1–88 (შემდგომში - მონაცემთა დაცვის ზოგადი რეგულაცია) მუხლი 4 (1); *Council of Europe,* Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018, მუხლი 2 (ა).

[4] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 26.

[5] იქვე.

მსგავსად ზემოაღნიშნულისა, ეროვნული კანონმდებლობაც პერსონალურ მონაცემად მიიჩნევს ნებისმიერ ინფორმაციას, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი პირთა ჯგუფიდან გამოცალკევება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.[6]

პერსონალური მონაცემების, როგორც ზედმეტად ფართო, ასევე გადაჭარბებულად ვიწრო შინაარსის განმარტება შესაძლოა, პრობლემური იყოს სხვადასხვა მიზეზით. პირველმა შემთხვევამ ცნებასთან დაკავშირებული მექანიზმების უმოქმედობა, არაპრაქტიკულობა შეიძლება გამოიწვიოს, მეორე კი ადამიანის უფლების დაცვის დაბალ სტანდარტად შეფასდეს. მაგალითად, თუკი ყველა იმ ინფორმაციას, რასაც ადამიანი დღის განმავლობაში გამოიყენებს, მის შესახებ პერსონალურ მონაცემად განვიხილავთ, მონაცემებთან დაკავშირებული შეზღუდვების გათვალისწინებით პირადი მონაცემების დაცვის კონცეფცია პარადოქსად იქცევა.[7] შესაბამისად, საჭიროა განმარტების ოპტიმალური ფარგლების განსაზღვრა, რაც მუდმივ გადახედვას უნდა დაექვემდებაროს, რადგან ტექნოლოგიური პროგრესის პირობებში არსებითად იცვლება მონაცემთა ანალიტიკის თუ დაკავშირების მეთოდები და ტაქტიკა.[8]

საქმეზე: "Breyer v. Bundesrepublik Deutschland"[9] ევროკავშირის მართლმსაჯულების სასამართლომ (CJEU) იმსჯელა მონაცემთა სუბიექტის ირიბი იდენტიფიცირების შესაძლებლობაზე. საქმე შეეხებოდა დინამიკურ IP მისამართებს, რომლებიც ინტერნეტთან დაკავშირებისას ყოველ ჯერზე იცვლება. ბ-ნი *ბრეიერის* იდენტიფიცირებისთვის საჭირო დამატებითი ინფორმაცია ჰქონდა მხოლოდ იმ ინტერნეტმომსახურების მიმწოდებელს, რომელსაც იგი იყენებდა. CJEU-მ დაადგინა, რომ დინამიკური IP მისამართი, რომელსაც არეგისტრირებს ონლაინ მედია მომსახურების მიმწოდებელი პირის ვებგვერდზე შესვლისას იმგვარი პერსონალური მონაცემია, სადაც მხოლოდ ინტერნეტ მომსახურების მიმწოდებელს აქვს პიროვნების იდენტიფიცირებისათვის საჭირო დამატებითი მონაცემები. სასამართლომ აღნიშნა: „არ არის აუცილებელი, ყველა ინფორმაცია, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას, ერთი პირის ხელში ინახებოდეს", რომ პერსონალურ

[6] „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, 5669-რს, 28/12/2011, მე-2 მუხლის „ა" ქვეპუნქტი.
[7] *Betkier M., Mazey N., Baptista R.,* Privacy Foundation New Zealand - Privacy in the Internet Economy Working Group, Is the Current Definition of Personal Information Enough to Protect Individuals from Privacy Harms?, 2021, <https://www.privacyfoundation.nz/wp-content/uploads/2021/03/Is-the-current-definition-of-personal-information-enough-to-protect.pdf> [24.01.2023].
[8] იქვე.
[9] CJEU, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* [2016], პუნქტი 43.

მონაცემად ჩაითვალოს. ინტერნეტ მომსახურების მიმწოდებლის მიერ დარეგისტრირებული დინამიკური IP მისამართის მომხმარებელთა იდენტიფიცირება შეიძლება გარკვეულ სიტუაციებში, მაგალითად კიბერთავდასხმაზე წარმოებული სისხლის სამართლის საქმის ფარგლებში, სხვა პირთა დახმარებით.[10] CJEU-ს განმარტებით, როდესაც პროვაიდერს სამართლებრივი საშუალება მონაცემთა სუბიექტის იდენტიფიცირების შესაძლებლობას აძლევს - იმ დამატებითი ინფორმაციის გამოყენებით, რომელიც მას დაფიქსირებული აქვს პირის შესახებ - ეს „საშუალება, გონივრული ვარაუდით, გამოყენებული იქნება მონაცემთა სუბიექტის იდენტიფიცირებისთვის.“[11]

მთლიანობაში, პერსონალური მონაცემების ცნება საკმარისად ფართოდ უნდა განიმარტოს იმისათვის, რომ დაიტიოს ყველა ის ინფორმაცია, რომელსაც საზოგადოება ლეგიტიმურად მიიჩნევს, როგორც პირადულს და რომლის უკანონო გამოყენებასაც ინდივიდის პირადი ცხოვრებისთვის ზიანის გამოწვევა შეუძლია.[12]

3. პერსონალური მონაცემების ცნების ელემენტები

პერსონალურ მონაცემთა ცნების შინაარსს აყალიბებს შემდეგი ელემენტები: „ფიზიკური პირი“, „ნებისმიერი ინფორმაცია“, „რომელიც უკავშირდება“, „იდენტიფიცირებული ან იდენტიფიცირებადი“ და მათი კუმულაციური არსებობა.[13]

ა) „ფიზიკური პირი“ – არის იგივე მონაცემთა სუბიექტი ანუ პირი, რომლის შესახებ მუშავდება მონაცემი.[14] მოქმედი კანონმდებლობის მიხედვით ინფორმაცია საჯარო დაწესებულებებისა და იურიდიული პირების შესახებ არ განეკუთვნება პერსონალურ მონაცემებს. თუმცა, მაგალითად ინფორმაცია პოლიტიკური თანამდებობის პირების, ინდივიდუალური მეწარმეების, კომპანიის და საჯარო დაწესებულებების თანამშრომლებისა, მათ შორის დირექტორების შესახებ, როდესაც ხდება მათი ინდივიდუალურად იდენტიფიცირება, წარმოადგენდეს პერსონალურ მონაცემებს.[15]

---

[10] CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011], პუნქტები 47-51.

[11] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 106.

[12] *Gilbert+Tobin*, Privacy Law Reform Series: Definition of "Personal Information", 2022, <https://www.gtlaw.com.au/knowledge/privacy-law-reform-series-definition-personal-information> [24.01.2023].

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

[14] იქვე, „ვ“ ქვეპუნქტი.

[15] *Information Commissioner's Office (ICO),* What is Personal Data?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#2> [24.01.2023]

ბ) „ნებისმიერი ინფორმაცია“ – შინაარსობრივი დატვირთვის გათვალისწინებით მიუთითებს კანონმდებლის ნებაზე, დაამკვიდროს პერსონალური მონაცემების ფართო განმარტების კონცეფცია. ცნების ამ ელემენტის ქვეშ მოიაზრება ფიზიკურ პირთან დაკავშირებული როგორც „ობიექტური“, ისე „სუბიექტური“ ინფორმაცია. „ობიექტურ“ ინფორმაციაში მოიაზრება, მაგალითად, სისხლის ანალიზის შედეგები, მონაცემთა სუბიექტის ასაკი და სხვა. „სუბიექტური“ ინფორმაცია გულისხმობს მოსაზრებებსა და შეფასებებს.[16]

გ) „რომელიც უკავშირდება“ – იმისათვის, რომ ინფორმაცია მიჩნეულ იქნეს პერსონალურ მონაცემად, იგი დაკავშირებული უნდა იყოს იდენტიფიცირებად ფიზიკურ პირთან.[17] ხშირ შემთხვევაში, ინფორმაცია ამგვარად მიიჩნევა, როდესაც იგი ეხება ფიზიკურ პირს. თუმცა არსებობს შემთხვევები, როდესაც მონაცემები უკავშირდება არა ფიზიკურ პირს, არამედ, მაგალითად, მის საკუთრებას, სხვადასხვა ღონისძიებას, მაგრამ მაინც წარმოადგენს პერსონალურ მონაცემს.[18] გასათვალისწინებელია ისიც, რომ ამგვარი კავშირი უნდა უზრუნველყოფდეს მონაცემთა სუბიექტის მარტივ და სწრაფ იდენტიფიცირებას, არაპროპორციული ხარჯის, დროისა და ძალისხმევის გარეშე.[19]

ერთ-ერთი მოსაზრების მიხედვით, ინდივიდი უნდა იყოს ინფორმაციის „საგანი“, რათა კონკრეტული ინფორმაცია პიროვნებასთან დაკავშირებულად შეფასდეს და მოექცეს პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოქმედების ფარგლებში.[20]

მონაცემები დაკავშირებულია პირთან, თუ იგი ეხება მის იდენტობას, მახასიათებლებს ან ქცევას, ან თუ ამგვარი ინფორმაცია გამოიყენება იმისათვის, რომ განისაზღვროს ან გავლენა მოახდინოს იმაზე, თუ როგორ ეპყრობიან ან აფასებენ პირს. იმისათვის, რომ მონაცემები ჩაითვალოს პირთან დაკავშირებულად, უნდა იყოს წარმოდგენილი ალტერნატიული სახით „შინაარსის“, „მიზნის“ ან „შედეგის“ ელემენტი.[21]

---

[16] *Article 29 Working Party*, Opinion 4/2007 on the Concept of Personal Data, 2007, 6, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> [24.01.2023].

[17] *Information Commissioner's Office (ICO),* What is personal data?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#2> [24.01.2023].

[18] *Article 29 Working Party*, Opinion 4/2007 on the Concept of Personal Data, 2007, 9, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>, [24.01.2023].

[19] ევროპის მართლმსაჯულების სასამართლომ 2016 წელს დაადგინა, რომ რეალობაში იდენტიფიცირების რისკი უმნიშვნელოა, თუკი იგი საჭიროებს არაპროპორციულ დროით, ეკონომიკურ რესურსსა და ძალისხმევას. *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR) A Practical Guide, 2017, 12.

[20] *Gilbert+Tobin,* Privacy Law Reform Series: Definition of "Personal Information", 2022, <https://www.gtlaw.com.au/knowledge/privacy-law-reform-series-definition-personal-information> [24.01.2023].

[21] *Article 29 Working Party,* Opinion 4/2007 on the Concept of Personal Data, 2007, 10, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> [24.01.2023].

გ.1) „შინაარსის“ ელემენტი სახეზეა იმ შემთხვევებში, როდესაც ინფორმაციის ძირითადი საგანია კონკრეტული ინდივიდი, მიუხედავად მონაცემთა დამმუშავებლის ან მესამე მხარის მიზნებისა, ან მონაცემთა სუბიექტზე ამ ინფორმაციის ზემოქმედებისა. ინფორმაცია დაკავშირებულია პირთან, როდესაც ის მის შესახებაა, მაგალითად, სამედიცინო ანალიზის შედეგები ცალსახად დაკავშირებულია პაციენტთან, ან კომპანიის პირადი საქმეების საქაღალდეში მოცემული ინფორმაცია გარკვეული თანამშრომლის სახელის მითითებით, აშკარაა, რომ ეხება მას.[22]

გ.2) „მიზნის“ ელემენტი შეიძლება არსებობდეს, როდესაც მონაცემები გამოიყენება ან სავარაუდოდ გამოყენებული იქნება, კონკრეტული შემთხვევის გარემოებების გათვალისწინებით, შეფასების, გარკვეული გზით მოპყრობის ან ინდივიდის სტატუსზე ან ქცევაზე ზემოქმედების მიზნით.[23]

გ.3) მესამე სახის მაკავშირებელი პირებთან ჩნდება მაშინ, როდესაც არსებობს *„შედეგის“* ელემენტი. „შინაარსის“ ან „მიზნის“ ელემენტის არარსებობის შემთხვევაში, მონაცემები შეიძლება ჩაითვალოს პირთან დაკავშირებულად, თუ მათი გამოყენება, შესაძლოა გავლენას ახდენდეს გარკვეული პირის უფლებებსა და ინტერესებზე, კონკრეტული შემთხვევის, გარემოების გათვალისწინებით. აღსანიშნავია, რომ აუცილებელი არ არის პოტენციურ შედეგს ჰქონდეს არსებითი გავლენა კონკრეტული ადამიანის ინტერესებზე. საკმარისია, თუ ასეთი მონაცემების დამუშავების შედეგად შესაძლებელია, rom პირს სხვა პირებისგან განსხვავებულად მოექცნენ.[24]

კავშირის ელემენტის მოკლე შეჯამება – ერთ-ერთ საქმეში[25] ევროკავშირის მართლმსაჯულების სასამართლომ (CJEU) დაადგინა, რომ კანდიდატის მიერ პროფესიულ გამოცდაზე წარდგენილი წერილობითი პასუხები და გამომცდელის ნებისმიერი კომენტარი ამ პასუხებთან დაკავშირებით კანდიდატის პერსონალური მონაცემებია. ასეთი სუბიექტური ინფორმაცია არის პერსონალური მონაცემები „მოსაზრებებისა და შეფასებების სახით, იმ პირობით, რომ ისინი „ეხება“ მონაცემთა სუბიექტს“ საგამოცდო კითხვებისგან განსხვავებით, რომლებიც არ განიხილება პერსონალურ მონაცემებად. ამგვარად, კონტექსტურმა შეფასებამ უნდა მოჰფინოს ნათელი, როდის შეიძლება ჰქონდეს ინფორმაციას გავლენა ინდივიდზე და შესაბამისად, განისაზღვროს მონაცემებზე ხელმისაწვდომობის უფლების ფარგლები.[26] ამდენად, ერთი და იგივე ინფორმაცია შეიძლება ეხებოდეს სხვადასხვა პირს ერთსა და

[22] იქვე.
[23] იქვე.
[24] იქვე, 11.
[25] CJEU, Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, [2017].
[26] *EDPB*, Guidelines 01/2022 on data subject rights, Version 1.0, 2022, 30, <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf> [24.01.2023].

იმავე დროს, იმის მიხედვით, თუ რა ელემენტს შეიცავს თითოეული მათგანი. ეს ასევე ნიშნავს იმას, რომ არ არის აუცილებელი მონაცემები ფოკუსირებული იყოს ვინმეზე, რათა ჩაითვალოს, რომ ეს მონაცემები ამ პირს ეხება. მაგალითად, ა-მ გადაწყვიტა ბ-ს დაწინაურება და ხელი მოაწერა მისი სამსახურებრივი წახალისების შესახებ ბრძანებას. ბ-ს მონაცემებმა გავლენა იქონია ა-ზე კონკრეტული შედეგის თვალსაზრისით, შესაბამისად ბ-ს შესახებ მონაცემი, რომელიც მას შინაარსის ელემენტით უკავშირდება, ა-ს დაუკავშირდა შედეგის ელემენტით.

დ) „იდენტიფიცირებული ან იდენტიფიცირებადი [ფიზიკური პირი]“ – ფიზიკური პირი ინდივიდთა ჯგუფში „იდენტიფიცირებულად“ მიიჩნევა, როდესაც იგი გამორჩეულია ჯგუფის სხვა წევრებისგან. ხოლო „იდენტიფიცირებადია“ ფიზიკური პირი, რომელიც ჯერ არ არის იდენტიფიცირებული, თუმცა შესაძლებელია მისი გამორჩევა ჯგუფის სხვა წევრებისგან.[27]

იმის დასადგენად, არის თუ არა პირი იდენტიფიცირებადი, მონაცემთა დამმუშავებელმა ან სხვა პირმა უნდა გაითვალისწინონ ყველა გონივრული საშუალება, რომელთა გამოყენებაც შესაძლებელია პიროვნების პირდაპირი ან ირიბი იდენტიფიცირებისათვის.[28] პიროვნების პირდაპირი ან ირიბი იდენტიფიცირების შესაძლებლობა საჭიროებს მუდმივ შეფასებას, მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიებისა და ზოგადად, ტექნოლოგიური განვითარების გათვალისწინებით.[29] იდენტიფიცირების შესაძლებლობის გასარკვევად, უნდა შემოწმდეს მონაცემთა სუბიექტის იდენტიფიკაციისთვის საჭირო ინფორმაციის ერთობლიობა ხელმისაწვდომია თუ არა დაინტერესებული პირისთვის.[30] საკითხის შეფასებისას გათვალისწინებულ უნდა იქნას არა მხოლოდ ის საშუალებები, რომლებსაც გონივრულად იყენებს ჩვეულებრივი ადამიანი, არამედ უნდა მოიაზრებოდეს განსაზღვრული ადამიანი, რომელსაც გააჩნია პირის იდენტიფიცირების კონკრეტული მიზეზი.[31] მაგალითად, გამომძიებელი ჟურნალისტები, ყოფილი პარტნიორები და სხვ. შესაბამისად, აუცილებელია განისაზღვროს, რა საშუალებები არსებობს პირის იდენტიფიცირებისთვის და რამდენად ხელმისაწვდომია ისინი. ამასთანავე, დროთა

---

[27] *Article 29 Working Party*, Opinion 4/2007 on the Concept of Personal Data, 2007, 12, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> [24.01.2023].

[28] მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR), პრეამბულა, პუნქტი 26.

[29] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 95, 102.

[30] *European University Institute,* Guide on Good Data Protection Practice in Research, 2022, 6, <https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf> [24.01.2023].

[31] *Information Commissioner's Office (ICO),* Guide to the General Data Protection Regulation (GDPR), 2022, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> [24.01.2023]

განმავლობაში იცვლება პიროვნებების იდენტიფიცირების საშუალებები. თუ დამმუშავებელს მიაჩნია, რომ მის მიერ შენახული მონაცემები არ იძლევა პიროვნების იდენტიფიკაციის შესაძლებლობას, ეს საკითხი რეგულარულად უნდა გადახედოს ახალი ტექნოლოგიების ან უსაფრთხოების განვითარების ან გარკვეული ჩანაწერების საჯაროდ ხელმისაწვდომობის თვალსაზრისით.[32]

ინდივიდი პირდაპირ იდენტიფიცირებადია, თუ შესაძლებელია მისი იდენტიფიცირება დამატებითი ინფორმაციის გამოყენების გარეშე. მაგალითად, მისი სახელისა და ადგილმდებარეობის ცოდნით, შესაძლებელია პირდაპირ ამოიცნოთ კონკრეტული პირი. თუმცა სახელის ცოდნის გარეშე კონკრეტულ ადგილზე მყოფი პირის ამოცნობა შესაძლებელი იქნებოდა მისი სიახლოვისა და ფიზიკური ფაქტორების კომბინაციით, როგორიცაა სიმაღლე და თმის ფერი.

არაპირდაპირი იდენტიფიკაციისას გასათვალისწინებელია მეტი ფაქტორი. არაპირდაპირი იდენტიფიკაცია ნიშნავს, რომ შეუძლებელია პიროვნების იდენტიფიცირება მხოლოდ იმ ინფორმაციის საშუალებით, რომელსაც ამუშავებს მონაცემთა დამმუშავებელი, მაგრამ შეიძლება პირის იდენტიფიცირება სხვა დამატებითი ინფორმაციის გამოყენებით, რომელსაც ფლობს დამმუშავებელი ან იმ ინფორმაციის გამოყენებით, რომელზეც ექნება წვდომის გონივრული შესაძლებლობა სხვა წყაროდან. ინფორმაციის მარტივი მაგალითი, რომელიც შეიძლება გამოყენებულ იქნეს პირის ირიბად იდენტიფიცირებისთვის, არის ავტოსატრანსპორტო საშუალების სანომრე ნიშანზე ასახული ციფრები. სამართალდამცავ ორგანოს შეუძლია სწრაფად დაუკავშიროს სახელი და გვარი სანომრე ნიშნის ნომერს.[33]

4. დასკვნა

თეორიულ-პრაქტიკული მოსაზრებების გაანალიზება ცხადყოფს, რომ ადამიანის შესახებ პერსონალური მონაცემები ყველაფერია, რაც მის სამოქალაქო, იურიდიული იდენტობის განსაზღვრის და სხვებისგან გამორჩევის, ინდივიდუალიზაციის საშუალებას იძლევა. ტექნოლოგიური განვითარების კვალდაკვალ კი, შეუძლებელია ზუსტად დადგინდეს სად მთავრდება მონაცემები თითოეული ჩვენგანის შესახებ. აღნიშნული საკითხი ნაშრომში მოხმობილი კრიტერიუმების მიხედვით უნდა გადაწყდეს, დროის კონკრეტულ მონაკვეთში არსებული შემთხვევის დეტალური გარემოებების გაანალიზებით.

როგორც ნათლად გამოიკვეთა, კლასიკური და ყველასთვის სამაგალითო პერსონალური მონაცემების გარდა (მაგალითად სახელის, გვარის და სხვა), აღნიშნული ტერმინი კიდევ მრავალ ინფორმაციას იტევს. კონკრეტული სიტყვათშეთანხმება,

[32] იქვე.
[33] What is considered personal data under the EU GDPR?, <https://gdpr.eu/eu-gdpr-personal-data/> [24.01.2023].

გარემოება, ფაქტი, მოსაზრება თუ შემთხვევა იმისათვის, რომ პერსონალურ მონაცემად შეფასდეს, აუცილებელია, იგი ფიზიკურ პირთან დაკავშირებადი იყოს პირთა ფართო თუ ვიწრო, პროფესიული თუ დაინტერესებული წრის მიერ.

მონაცემთა სუბიექტისთვის პოზიტიური სამართლით მინიჭებული უფლებებიდან ერთ-ერთი ინფორმირების უფლებაა, რომლის მეშვეობით მას შეუძლია დეტალურად გაარკვიოს, თუ რომელ მონაცემებს ამუშავებს მის შესახებ კონკრეტული დაწესებულება თუ სხვა პირი, რა მიზნით და საფუძვლით, ასევე თუ რომელი გარეშე პირებისთვის იქნა გადაცემული მოთხოვნილი მონაცემები და სხვა. მონაცემთა სუბიექტის წინაშე არსებული მოვალეობების ზედმიწევნით შესრულება შესაძლოა, მნიშვნელოვანი რისკის წინაშე აღმოჩნდეს იმ შემთხვევაში, თუ დაწესებულებაში პერსონალურ მონაცემთა დაცვის შიდაორგანიზაციული წესები სათანადოდ განვითარებული არ არის. ინდივიდი საზოგადი ხასიათის მოთხოვნის საპასუხოდ მონაცემთა დამმუშავებელმა რთულია, შეძლოს და მცირე დროში (რომელიც მოქმედი კანონმდებლობის თანახმად 10 კალენდარულ დღეს შეადგენს[34]) დააკავშიროს მაგალითად წლების წინ საკონკურსო კომისიის ერთ-ერთი წევრის მიერ კანდიდატის მიმართ გამოხატული მოსაზრებები იმ კანდიდატთან, რომელიც ამჯერად მონაცემთა სუბიექტის სტატუსით მოევლინა.

ორგანიზაციებში პერსონალურ მონაცემებთან შემხებლობაში არსებული ყველა პროცესი და რეგულაცია ჯაჭვურადაა დაკავშირებული ერთმანეთთან. თუკი დამმუშავებლები მკაცრად დაიცავენ მონაცემთა დამუშავების საფუძვლებსა და სხვა პრინციპებთან ერთად იხელმძღვანელებენ მონაცემთა მინიმიზაციის, მიზნის და ვადის შეზღუდვის პრინციპით, თუკი ყველაფერს იმგვარს, რაც ზედმეტია, არასაჭიროა და თუნდაც შემთხვევით მოხვდა მათ ხელში დროულად გაანადგურებენ, წაშლიან, მიმწოდებელ პირს დაუბრუნებენ, შეძლებენ რომ მარტივად მოიძიონ მონაცემთა სუბიექტზე სრული ინფორმაცია და დროულად მიაწოდონ მას. „ნებისმიერი სისტემის შექმნისას მხედველობაში უნდა იქნეს მიღებული საქართველოს კონსტიტუციის მე-18 მუხლის მე-2 პუნქტის სულისკვეთება, სახელდობრ პრინციპი, რომ საჯარო დაწესებულებაში პიროვნების შესახებ არსებული ინფორმაციის ამავე პიროვნებისათვის გაცემის უფლება იყოს წესი, ხოლო მისი შეზღუდვა – გამონაკლისი და შესაბამისი აუცილებლობით განპირობებული.“[35]

როგორც ნაშრომიდან გამომდინარეობს, ერთი ადამიანის შესახებ მონაცემებად, ხშირად, სხვა ფიზიკური პირის მონაცემებიც განიხილება. მაგალითად, საკუთარ ბინაში რეგისტრირებულ ადამიანებზე ინფორმაცია მესაკუთრისთვის განსაკუთრებულად ღირებულია, თუმცა მან შეიძლება ინფორმაცია მანამდე ვერ გამოარკვიოს, ვიდრე სასამართლოს ჩარევით არ მოიპოვებს მას. ეს კი ხშირად მონაცემთა სუბიექტის

[34] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მუხლი 21.
[35] საქართველოს საკონსტიტუციო სასამართლოს 2020 წლის 18 დეკემბრის გადაწყვეტილება საქმეზე № 1/3/1312, II 49.

უფლებების დაუსაბუთებელ შეზღუდვას შეიძლება ნიშნავდეს, ვინაიდან დაწესებულება ცდილობს ინფორმაცია არ გასცეს იმიტომ, რომ ბინაში რეგისტრირებული პირების მონაცემებიც პერსონალურია. რეალურად, მას არჩევანის საშუალება მხოლოდ მონაცემთა სუბიექტის უფლების რეალიზებას ან ამ უფლების ლეგიტიმურად შეზღუდვას შორის უნდა ჰქონდეს იმ პირობებში, როდესაც სხვა ინდივიდის მონაცემები იმ მონაცემთა სუბიექტს უკავშირდება, რომელიც საკუთარი თავის შესახებ ინფორმაციის გარკვევას ცდილობს. ინფორმაციის პერსონალურ მონაცემებად კლასიფიკაცია არ არის დამოკიდებული იმაზე, რომ ეს პერსონალური მონაცემები ასევე სხვა ფიზიკურ პირს ეხება. ცხადია, მსგავს შემთხვევაში, დაწესებულება შესაბამისი პირის მონაცემებს ამჟღავნებს, მაგრამ აღნიშნულს მას კანონმდებლობა პირდაპირ ავალდებულებს მონაცემთა სუბიექტისთვის ინფორმირების უფლების გარანტირებით. ამასთან, წარმოდგენილი დასკვნა, არ ნიშნავს დაკავშირებული ინდივიდების მონაცემების გამჟღავნების თავისთავად კანონიერებას. პოზიტიური სამართალი[36] ითვალისწინებს ფიზიკური პირებისთვის საკუთარ მონაცემებზე ხელმისაწვდომობის უფლების შეზღუდვას მონაცემთა დამმუშავებლის მხრიდან, მათ შორის მაშინ, როდესაც დასაცავია სხვათა უფლებები და თავისუფლებები[37].

საკუთარი თავის შესახებ პერსონალური მონაცემების გარკვევა დაუსრულებელი პროცესია, რომელიც მონაცემთა დამმუშავებლების და ინდივიდების სათანადო და რაციონალური მიდგომის შემთხვევაში საუკეთესო საშუალებაა პირადი ცხოვრების ხელშეუხებლობის ეფექტიანი კონტროლისათვის.

ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, 786- რს, 24/08/1995.
2. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
3. *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 95, 102, 106.
4. საქართველოს საკონსტიტუციო სასამართლოს 2020 წლის 18 დეკემბრის გადაწყვეტილება № 1/3/1312, II 49.
5. 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 L 119, 4/5/2016, 1–88.

[36] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, 24-ე მუხლი.
[37] მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR), მუხლი 15.4.

6. *Council of Europe,* Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
7. *Article 29 Working Party,* Opinion 4/2007 on the Concept of Personal Data, 2007, 6, 9, 10, 12 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> [24.01.2023].
8. *Betkier M., Mazey N., Baptista R.,* Privacy Foundation New Zealand - Privacy in the Internet Economy Working Group, Is the Current Definition of Personal Information Enough to Protect Individuals from Privacy Harms?, 2021, <https://www.privacyfoundation.nz/wp-content/uploads/2021/03/Is-the-current-definition-of-personal-information-enough-to-protect.pdf> [24.01.2023].
9. *EDPB*, Guidelines 01/2022 on data subject rights, Version 1.0, 2022, 30, <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf> [24.01.2023]
10. *European University Institute,* Guide on Good Data Protection Practice in Research, 2022, 6, <https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf> [24.01.2023].
11. *Information Commissioner's Office (ICO)*, Guide to the General Data Protection Regulation (GDPR), 2022.
12. *Information Commissioner's Office (ICO),* What is Personal Data?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#2> [24.01.2023].
13. *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 12.
14. CJEU, C-70/10*, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011].
15. CJEU, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* [2016].
16. CJEU, Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, [2017].
17. <https://www.gtlaw.com.au/knowledge/privacy-law-reform-series-definition-personal-information> [24.01.2023].
18. <https://gdpr.eu/eu-gdpr-personal-data/> [24.01.2023].

დავით ყარაშვილი*

სატრანსპორტო საშუალებაზე განსათავსებელი შეზღუდული შესაძლებლობის მქონე პირის საცნობი ნიშნის გამოყენების სამართლებრივი შეფასება პერსონალური მონაცემების დაცვის ჭრილში

სტატია მიმოიხილავს განსაკუთრებული კატეგორიის მონაცემის დამუშავების კანონიერებას შეზღუდული შესაძლებლობის მქონე პირის სატრანსპორტო საშუალების საცნობი ნიშნის სავალდებულო გამოყენების მაგალითზე. ერთი შეხედვით მარტივი შემთხვევა, შესაძლოა, პრობლემური აღმოჩნდეს პერსონალურ მონაცემთა დაცვის ჭრილში და შეზღუდული შესაძლებლობის მქონე პირისთვის არასასურველი ინფორმაციის ზედმეტი დოზით გამჟღავნებას გულისხმობდეს. სტატიაში შემოთავაზებულია ალტერნატიული გზა, რომლის განხორციელებაც, მონაცემთა დამმუშავებლისათვის არ უნდა წარმოადგენდეს სირთულეს.

საკვანძო სიტყვები: *პერსონალური მონაცემი, განსაკუთრებული კატეგორიის მონაცემი, შშმ პირი.*

1. შესავალი

მსოფლიოში დიდი ყურადღება ექცევა შეზღუდული შესაძლებლობის მქონე (შშმ) პირთათვის (შეზღუდული შესაძლებლობის მქონე პირი – პირი მყარი ფიზიკური, ფსიქიკური, ინტელექტუალური ან სენსორული დარღვევით, რომლის სხვადასხვა დაბრკოლებასთან ურთიერთქმედებამ შესაძლოა, ხელი შეუშალოს საზოგადოებრივ ცხოვრებაში ამ პირის სრულ და ეფექტიან მონაწილეობას სხვებთან თანაბარ პირობებში.)[1] შესაბამისი პირობებისა თუ გარანტიების შექმნას, რათა მათ სრულად

* ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი; შავი ზღვის უნივერსიტეტის მოწვეული ლექტორი; პერსონალურ მონაცემთა დაცვის სამსახურის იურიდიული დეპარტამენტის უფროსი.

[1] „შეზღუდული შესაძლებლობის მქონე პირთა უფლებების შესახებ“ საქართველოს კანონი, 6823-რს, 14/07/2020, მე-2 მუხლის „ა“ ქვეპუნქტი.

მიუწვდებოდეთ ხელი ყველა მომსახურებაზე თუ პროდუქტზე, რასაც საჯარო თუ კერძო სექტორი სთავაზობს ფიზიკურ პირებს. საქართველოს კონსტიტუციის თანახმად, შშმ პირთა უფლებებისა და თავისუფლებების დასაცავად სახელმწიფოს აქვს ვალდებულება, აქტიური ქმედებით უზრუნველყოს სათანადო პირობების შექმნა ასეთი პირებისათვის – სახელმწიფო ქმნის განსაკუთრებულ პირობებს შეზღუდული შესაძლებლობის მქონე პირთა უფლებებისა და ინტერესების რეალიზებისთვის.[2] ერთ-ერთი ასეთი ღონისძიებაა სპეციალურად შშმ პირთათვის განკუთვნილი სატრანსპორტო საშუალების პარკირების ადგილების განსაზღვრა, რაც მიზნად ისახავს, შშმ პირთა გადაადგილებისა და სხვადასხვა მომსახურების მიღების შესაძლებლობის გამარტივებას, მათ ადაპტაციას არსებული ინფრასტრუქტურისადმი. მიუხედავად მნიშვნელოვანი ლეგიტიმური მიზნისა, საჭიროა მსგავსი გარანტიების შექმნა იმგვარად, რომ რაც შეიძლება ნაკლები დოზით მოხდეს შშმ პირის სტატუსის აფიშირება, რამაც თავის მხრივ, შესაძლოა, გამოიწვიოს შშმ პირთა სტიგმატიზება.

წინამდებარე სტატია წარმოადგენს ერთგვარ მსჯელობას შშმ პირთა სატრანსპორტო საშუალებების საცნობი ნიშნის გამოყენების კანონიერების შესახებ პერსონალურ მონაცემთა დაცვის ჭრილში.

2. სატრანსპორტო საშუალებებზე დასამაგრებელი საცნობი ნიშნების გამოყენების წესი მოქმედი კანონმდებლობის შესაბამისად

„საგზაო მოძრაობის შესახებ“ საქართველოს კანონის მე-19 მუხლი განსაზღვრავს სატრანსპორტო საშუალებაზე დასამაგრებელ საცნობ ნიშნებს. აღნიშნული მუხლის პირველი პუნქტი ადგენს იმ საცნობ ნიშნებს, რომელთა დამაგრებაც სატრანსპორტო საშუალებაზე არის სავალდებულო და როგორიცაა, მაგალითად, „სმენადაქვეითებული მძღოლი“.[3]

„საგზაო მოძრაობის შესახებ“ საქართველოს კანონის მე-19 მუხლის მე-2 პუნქტი, პირველი პუნქტისგან განსხვავებით, ადგენს იმ საცნობ ნიშნებს, რომელთა სატრანსპორტო საშუალებაზე განთავსებაც მძღოლის სურვილზეა დამოკიდებული. აღნიშნული პუნქტის „ა“ ქვეპუნქტი ასეთ საცნობ ნიშნად განსაზღვრავს ნიშანს – „შეზღუდული შესაძლებლობის მქონე პირი“.

„საგზაო მოძრაობის შესახებ“ საქართველოს კანონი მეტს არაფერს ამბობს ზემოაღნიშნული საცნობი ნიშნების შესახებ. კანონი პირდაპირ არ საუბრობს აღნიშნული ნიშნების გამოყენების კონკრეტულ მიზნებზე. თუმცა კანონის მე-19 მუხლის გაანალიზების შედეგად, შესაძლებელია იმის ვარაუდი, რომ საცნობი ნიშნების

[2] საქართველოს კონსტიტუცია, 786, 24/08/1995, მე-11 მუხლის მე-4 პუნქტი.

[3] „საგზაო მოძრაობის შესახებ“ საქართველოს კანონი, 1830-რს, 24/12/2013, მე-19 მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტი.

გამოყენება განსხვავებულ მიზნებს ემსახურება. როგორც ზემოთ აღინიშნა, ნიშნის – „სმენადაქვეითებული მძღოლი“ – გამოყენება და განთავსება სატრანსპორტო საშუალებაზე, ხილვად ადგილას, სავალდებულოა. მე-19 მუხლის პირველი პუნქტით ჩამოთვლილი ნიშნების სპეციფიკიდან გამომდინარე, შეიძლება ითქვას, რომ აღნიშნული ნიშნების გამოყენება ემსახურება ისეთ ლეგიტიმურ მიზანს, როგორიცაა საგზაო მოძრაობის უსაფრთხოება. აღნიშნული ნიშნების გამოყენების მთელი არსი სწორედ იმაშია, რომ შესამჩნევი იყოს, რომ მაგალითად, სატრანსპორტო საშუალებას მართავს სმენადაქვეითებული მძღოლი, რათა საჭიროების შემთხვევაში, სხვა მძღოლმა იმოქმედოს შესაბამისად (მაგალითად, არ იყოს ხმოვანი სიგნალის იმედად და ა. შ.).

ადგილობრივი თვითმმართველობის კოდექსის მე-16 მუხლის მე-2 ნაწილის „კ“ ქვეპუნქტის თანახმად, „მუნიციპალიტეტის საკუთარ უფლებამოსილებას განეკუთვნება ადგილობრივი მნიშვნელობის საავტომობილო გზების მართვა და ადგილობრივი მნიშვნელობის გზებზე საგზაო მოძრაობის ორგანიზება; ავტოსატრანსპორტო საშუალებების პარკირების ადგილებით უზრუნველყოფა და დგომის/გაჩერების წესების რეგულირება“.

ადგილობრივი თვითმმართველობის კოდექსის ზემოაღნიშნული მე-16 მუხლის მე-2 ნაწილის „კ“ ქვეპუნქტის საფუძველზე მუნიციპალიტეტების საკრებულოების მიერ გამოცემულია არაერთი დადგენილება შესაბამისი მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესის დამტკიცების შესახებ. დადგენილებებში წარმოდგენილი დებულებები თითქმის იდენტურია და მსგავს ჩანაწერებს შეიცავს.

ქვემოთ მიმოხილულია რამდენიმე მუნიციპალიტეტის საკრებულოს დადგენილება, რათა მკითხველს შეექმნას გარკვეული წარმოდგენა, თუ როგორ წესრიგდება აღნიშნული საკითხი მუნიციპალიტეტების მიერ.

მაგალითისათვის, სიღნაღის მუნიციპალიტეტის საკრებულოს 2010 წლის 29 ოქტომბრის N30 დადგენილებით დამტკიცებული სიღნაღის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესის მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის თანახმად, „სიღნაღის მუნიციპალიტეტის საკრებულო უფლებამოსილია, განსაზღვროს სპეციალური პარკირების ადგილები და პირობები შეზღუდული შესაძლებლობის მქონე პირთა გადაადგილების უზრუნველსაყოფად, შესაბამისი საცნობი ნიშნის მქონე ავტოსატრანსპორტო საშუალებათა პარკირებისათვის.“ ამავე მუხლის მე-3 პუნქტის თანახმად, „შეზღუდული შესაძლებლობის მქონე პირის საცნობი ნიშნის მატარებელი ავტოსატრანსპორტო საშუალებებისათვის განსაზღვრული პარკირების ადგილები უნდა იყოს შესაბამისად გამოყოფილი და აღნიშნული. ასეთ პარკირების ადგილზე შეიძლება მხოლოდ შეზღუდული შესაძლებლობის მქონე პირის საცნობი ნიშნის მატარებელი

ავტოსატრანსპორტო საშუალებების პარკირება.“ ამავე წესის მე-7 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის შესაბამისად კი, „ავტოსატრანსპორტო საშუალების მძღოლი ან მესაკუთრე ვალდებულია არ მოახდინოს პარკირება სპეციალურ, მათ შორის, შეზღუდული შესაძლებლობის მქონე პირთა პარკირების ადგილას შესაბამისი საცნობი ნიშნის ან სტატუსის მქონე ავტოსატრანსპორტო საშუალების გარეშე.“

მსგავს დებულებებს შეიცავს ბორჯომის მუნიციპალიტეტის საკრებულოს 2011 წლის 18 მარტის N7 დადგენილებით დამტკიცებული ბორჯომის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესი. გარდა იდენტური დებულებებისა, ბორჯომის მუნიციპალიტეტის საკრებულოს მიერ დამტკიცებული წესი შეიცავს ისეთ დებულებებს, რომლებსაც არ განსაზღვრავს სიღნაღის მუნიციპალიტეტის საკრებულოს მიერ მიღებული დადგენილება. კერძოდ, ბორჯომის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესის მე-9 მუხლის მე-3 პუნქტის თანახმად, „საცნობი ნიშნის მისაღებად შეზღუდული შესაძლებლობის მქონე პირმა განცხადებით უნდა მიმართოს მუნიციპალიტეტს და განცხადებასთან ერთად წარუდგინოს პირადობის, შეზღუდული შესაძლებლობის დამადასტურებელი და ავტოსატრანსპორტო საშუალების იდენტიფიკაციის საბუთი.“ ამავე მუხლის მე-5 პუნქტის შესაბამისად, „შეზღუდული შესაძლებლობის მქონე პირის შემთხვევაში, საცნობი ნიშანი გაიცემა შეზღუდული შესაძლებლობის მქონე პირზე და მის ან მისი ოჯახის წევრის ავტოსატრანსპორტო საშუალებაზე.“

განსხვავებულ დებულებებს ვხვდებით თვითმმართველი ქალაქი ფოთის საკრებულოს 2014 წლის 7 ივლისის N14/18 დადგენილებით დამტკიცებულ ქალაქ ფოთის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესში, რომლის მე-6 მუხლის მე-3, მე-4 და მე-5 პუნქტების თანახმად, „შეზღუდული შესაძლებლობის მქონე პირთა გადაადგილების უზრუნველსაყოფად, შესაბამისი საცნობი ნიშნის მქონე ავტოსატრანსპორტო საშუალებათა პარკირების ადგილებს განსაზღვრავს ქალაქ ფოთის მუნიციპალიტეტის მერი ან მერის მიერ უფლებამოსილი პირი. შეზღუდული შესაძლებლობის მქონე პირთა გადაადგილების უზრუნველსაყოფად, საცნობი ნიშნის გაცემაზე პასუხისმგებელია ქალაქ ფოთის მუნიციპალიტეტის მერი ან მერის მიერ უფლებამოსილი პირი. საცნობი ნიშანი გაიცემა როგორც მკვეთრად გამოხატული შეზღუდული შესაძლებლობის, ისე მნიშვნელოვნად გამოხატული შეზღუდული შესაძლებლობის სტატუსის მქონე პირებზე. საცნობი ნიშნის განთავსება შესაძლებელია ნებისმიერ ავტოსატრანსპორტო საშუალებაზე, მიუხედავად შეზღუდული შესაძლებლობის მქონე პირის სარგებლობაში არსებული ავტოსატრანსპორტო საშუალების კუთვნილებისა. სხვა მუნიციპალიტეტის ტერიტორიაზე გაცემულ საცნობ ნიშანს იგივე იურიდიული ძალა აქვს როგორც ქალაქ ფოთის მუნიციპალიტეტის მერის ან მერის მიერ უფლებამოსილი პირის მიერ გაცემულ საცნობ ნიშანს. შეზღუდული შესაძლებლობის მქონე პირის საცნობი ნიშნის მატარებელი ავტოსატრანსპორტო საშუალებებისათვის განსაზღვრული პარკირების

ადგილები უნდა იყოს შესაბამისად გამოყოფილი და აღნიშნული. ასეთ პარკირების ადგილზე შეიძლება მხოლოდ შეზღუდული შესაძლებლობის მქონე პირის საცნობი ნიშნის მატარებელი ავტოსატრანსპორტო საშუალებების პარკირება.“

საინტერესოა დედაქალაქის საკრებულოს მიდგომა შეზღუდული შესაძლებლობის მქონე პირის საცნობი ნიშნისადმი. ქალაქ თბილისის მუნიციპალიტეტის საკრებულოს 2016 წლის 27 დეკემბრის N33-99 დადგენილებით დამტკიცებულია ქალაქ თბილისის ადმინისტრაციულ საზღვრებში სატრანსპორტო საშუალებების პარკირების რეგულირების წესი. აღნიშნული წესის მე-2 მუხლის „ყ“ ქვეპუნქტის თანახმად, „საცნობი ნიშანი არის ქალაქ თბილისის მუნიციპალიტეტის საჯარო სამართლის იურიდიული პირი – ქალაქ თბილისის მუნიციპალიტეტის ტრანსპორტისა და ურბანული განვითარების სააგენტოს მიერ შეზღუდული შესაძლებლობის მქონე პირისთვის ან იურიდიული პირის საკუთრებაში მქონე შეზღუდული შესაძლებლობის მქონე პირისთვის ადაპტირებულ სატრანსპორტო საშუალებაზე ამ წესის შესაბამისად გაცემული ნიშანი.“ ამავე წესის „ხ“ ქვეპუნქტის შესაბამისად, „შეზღუდული შესაძლებლობის მქონე პირი არის საქართველოს ნორმატიული აქტების შესაბამისად მკვეთრად გამოხატული შეზღუდული შესაძლებლობის სტატუსის მქონე პირი.“ ამავე წესის მე-9 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის შესაბამისად, „სატრანსპორტო საშუალების მძღოლი ან/და მესაკუთრე ვალდებულია, არ მოახდინოს პარკირება სპეციალურ, მათ შორის, შეზღუდული შესაძლებლობის მქონე პირთა პარკირების ადგილზე ამ წესით განსაზღვრული საცნობი ნიშნის გარეშე.“ ამავე წესის მე-11 მუხლი კი, არეგულირებს საცნობი ნიშნის გაცემისა და საცნობი ნიშნის მქონე სატრანსპორტო საშუალების პარკირების წესს, რომლის მე-8 პუნქტის თანახმადაც, „საცნობი ნიშანი განთავსებული უნდა იყოს სატრანსპორტო საშუალების წინა საქარე მინაზე ისე, რომ უფლებამოსილი პირის მიერ შესაძლებელი იყოს მისი ამოკითხვა.“ ამავე მუხლის მე-13 პუნქტის მიხედვით, „თუ საცნობი ნიშანი ამ წესის შესაბამისად არ იქნება განთავსებული სატრანსპორტო საშუალებაზე და მოხდება ამ სატრანსპორტო საშუალების პარკირება შეზღუდული შესაძლებლობის მქონე პირისთვის განსაზღვრულ პარკირების ადგილზე, აღნიშნული შემთხვევა განიხილება შეზღუდული შესაძლებლობის მქონე პირის სატრანსპორტო საშუალებისთვის განსაზღვრულ პარკირების ადგილზე არაუფლებამოსილი პირის მიერ სატრანსპორტო საშუალების პარკირებად.“

როგორც ზემოთ მოყვანილი მაგალითებიდან ირკვევა, პრაქტიკაში პარკირების უფლების მოსაპოვებლად გადამწყვეტი მნიშვნელობა მაინც შეზღუდული შესაძლებლობის მქონე პირის საცნობ ნიშანს ენიჭება, მიუხედავად იმისა, რომ „საგზაო მოძრაობის შესახებ“ საქართველოს კანონის მე-19 მუხლი მკაფიოდ ადგენს ასეთი ნიშნის გამოყენების ნებაყოფლობითობას („მძღოლის სურვილისამებრ,

სატრანსპორტო საშუალებაზე შეიძლება დამაგრდეს შემდეგი საცნობი ნიშნები: ...“)[4]. გამოდის, რომ შშმ პირის საცნობი ნიშნის გამოყენება არ არის დამოკიდებული სრულად პირის ნებაზე და მისი ნებაყოფლობითობა მხოლოდ უშუალოდ სატრანსპორტო საშუალებით გადაადგილების (მართვის) პერიოდით შემოიფარგლება.

ყურადსაღებია ის მოცემულობაც, რომ თითოეული საცნობი ნიშანი მოქმედებს მხოლოდ იმ მუნიციპალიტეტის ადმინისტრაციულ ფარგლებში, რომლის საკრებულოს მიერაც გაიცა საცნობი ნიშანი. აღნიშნული სერიოზულ პრობლემას წარმოშობს შშმ პირებისათვის, რამეთუ პირი, რომელსაც ბორჯომში აქვს აღებული საცნობი ნიშანი, თბილისში პარკირების შემთხვევაში მაინც დაჯარიმდება, რადგან აღნიშნულ ნიშანს ქალაქ თბილისის ადმინისტრაციულ საზღვრებში იურიდიული ძალა არ ექნება. ამ თვალსაზრისით, კარგ მაგალითს იძლევა ქალაქ ფოთის საკრებულო, რომელმაც პირდაპირ დაადგინა, რომ სხვა მუნიციპალიტეტის ტერიტორიაზე გაცემულ საცნობ ნიშანს იგივე იურიდიული ძალა აქვს როგორც ქალაქ ფოთის მუნიციპალიტეტის მერის ან მერის მიერ უფლებამოსილი პირის მიერ გაცემულ საცნობ ნიშანს.[5]

3. შეზღუდული შესაძლებლობის მქონე პირის სატრანსპორტო საშუალებაზე დასამაგრებელი საცნობი ნიშანი, როგორც პერსონალური მონაცემი და მისი გამოყენების კანონიერება პერსონალურ მონაცემთა დაცვის ჭრილში

3.1. პერსონალური მონაცემის დამუშავების კანონიერება

პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც პირის პირდაპირ ან არაპირდაპირ იდენტიფიცირების საშუალებას იძლევა (პერსონალური მონაცემი – ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.)[6]. სატრანსპორტო საშუალებაზე არსებული საცნობი ნიშანი მარტივად ასოცირდება მძღოლთან, რომლის იდენტიფიცირებაც, რა თქმა უნდა, არ არის რთული, რამეთუ მძღოლი წარმოადგენს ხილვად ობიექტს საზოგადოებისთვის. ასევე აღსანიშნავია, რომ

[4] „საგზაო მოძრაობის შესახებ“ საქართველოს კანონი, 1830-რს, 24/12/2012, მე-19 მუხლის მე-2 პუნქტის პრეამბულა.

[5] თვითმმართველი ქალაქი ფოთის საკრებულოს 2014 წლის 7 ივლისის N14/18 დადგენილებით დამტკიცებულ ქალაქ ფოთის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესის მე-6 მუხლის მე-5 პუნქტი.

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

ზოგადად, პირის გამოსახულება იმდენად მაღალი ხარისხით არის დაახლოებული პირის ვინაობასთან, რომ მისი ვინაობის ცალკე იდენტიფიცირების საჭიროება აღარ არის იმდენად მნიშვნელოვანი პირის გამოსახულების პერსონალურ მონაცემად მიჩნევის მიზნებისათვის. როდესაც პირი მართავს სატრანსპორტო საშუალებას, ის ხილვადია მის ირგვლივ მყოფი ადამიანებისთვის. შესაძლოა, კონკრეტულ მომენტში ადამიანებმა არ იცოდნენ მძღოლის ვინაობა, მაგრამ ხილვადი პირისთვის უკვე მინიჭებული გარკვეული სტატუსის დემონსტრირება, მით უმეტეს, თუ ეს სტატუსი ჯანმრთელობის მდგომარეობას უკავშირდება, წარმოადგენს მის პირად სივრცეში ჩარევას და სახეზეა მისი პერსონალური მონაცემების დამუშავება. გარდა აღნიშნულისა, შესაძლებელია პირის სრული იდენტიფიცირება იმ პირების მიერ, რომლებმაც იციან აღნიშნული პირის ვინაობა.

ზემოაღნიშნული მსჯელობის საპირისპიროდ, შესაძლებელია გაჩნდეს კითხვა, როდესაც საცნობი ნიშნის მქონე სატრანსპორტო საშუალების პარკირება მოხდება შშმ პირისთვის განკუთვნილ სპეციალურ პარკირების ადგილზე, აღნიშნული ხომ ისედაც ნათელყოფს, რომ კონკრეტული პირი შშმ სტატუსის მქონეა? უმეტეს შემთხვევაში ეს ასეც იქნება, თუმცა, როდესაც მონაცემები მუშავდება ერთი საშუალებით (შშმ პირის აღმნიშვნელი საგზაო ნიშანი), ეს სულაც არ ხდის კანონიერს დამატებით სხვა საშუალებით მონაცემთა დამუშავებას (სატრანსპორტო საშუალების საქარე მინაზე საცნობი ნიშნის განთავსება), მით უმეტეს, როცა ამ უკანასკნელის არანაირი საჭიროება არსებობს. მონაცემთა სუბიექტს შესაძლოა, არ სურდეს, მოახდინოს საკუთარი სტატუსის დემონსტრირება საქარე მინაზე საცნობი ნიშნის განთავსების გზით. ამასთან, აღსანიშნავია ისიც, რომ შშმ პირის საგზაო ნიშანს ალტერნატივა არ აქვს, რადგან ყველას უნდა შეეძლოს შშმ პირისათვის განკუთვნილი პარკირების ადგილის დანახვა, რათა იქ არ გააჩეროს საკუთარი ავტომობილი. რაც შეეხება საცნობი ნიშნის გამოყენებას, მას გააჩნია საკმაოდ მარტივი ალტერნატივა (ამ საკითხზე მსჯელობა იხ. 2.3 ქვეთავში).

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ბ“ ქვეპუნქტის[7] („განსაკუთრებული კატეგორიის მონაცემი – მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში გაწევრებასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან, აგრეთვე ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც

[7] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მე-2 მუხლის „ბ“ ქვეპუნქტი.

ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა“) თანახმად, სატრანსპორტო საშუალებისთვის განკუთვნილი შშმ პირის საცნობი ნიშანი წარმოადგენს განსაკუთრებული კატეგორიის მონაცემს, რადგან აღნიშნული მონაცემები ეხება პირის ჯანმრთელობას.

„შეზღუდული შესაძლებლობის მქონე პირთა შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის თანახმად, „სახელმწიფო ხელს უწყობს შეზღუდული შესაძლებლობის მქონე პირის დამოუკიდებელ ცხოვრებასა და საზოგადოებრივი ცხოვრების ყველა სფეროში მის სრულყოფილ მონაწილეობას სხვებთან თანასწორად, აგრეთვე სხვადასხვა სახის მხარდამჭერი მომსახურების და საზოგადოებრივი სარგებლობის ობიექტების, ასევე კომუნიკაციის საშუალებების ხელმისაწვდომობას, რაც საზოგადოებრივ ცხოვრებაში მისი სრულყოფილი მონაწილეობისათვის აუცილებელია.“ ამავე მუხლის მეორე პუნქტის თანახმად კი, „ზემოაღნიშნული მიზნების მისაღწევად პერსონალური მონაცემების დამუშავება ხორციელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნათა შესაბამისად.“

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი განსაზღვრავს მონაცემთა დამუშავების პრინციპებს. აღნიშნული მუხლის „ა“ ქვეპუნქტის თანახმად, „მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად.“ მონაცემთა დამუშავების კანონიერების დასადგენად აუცილებელია, შეფასდეს მონაცემთა დამუშავების საფუძველი.

რადგანაც შეზღუდული შესაძლებლობის მქონე პირის სატრანსპორტო საშუალების საცნობი ნიშანი წარმოადგენს განსაკუთრებული კატეგორიის მონაცემს, მნიშვნელოვანია, აღნიშნული მონაცემის დამუშავების საფუძველი შეფასდეს ამავე კანონის მე-6 მუხლის ჭრილში, რომლის თანახმადაც, განსაკუთრებული კატეგორიის მონაცემთა დამუშავების მთავარ საფუძველს მონაცემთა სუბიექტის წერილობითი თანხმობა წარმოადგენს. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ზ“ და „თ“ ქვეპუნქტების შესაბამისად, მონაცემთა სუბიექტის თანხმობა უნდა იყოს ნებაყოფლობითი, რომლითაც ნათლად დადგინდება მონაცემთა სუბიექტის ნება.[8]

ნებაყოფლობითი თანხმობა უნდა იყოს გამოხატული თავისუფლად და თანხმობაზე უარი არ უნდა იწვევდეს უარყოფით ან შემზღუდავ ეფექტს მონაცემთა სუბიექტისთვის.[9] მოცემულ შემთხვევაში, თუ პირი უარს განაცხადებს შშმ პირის საცნობი ნიშნის განთავსებაზე, ის ვერ ისარგებლებს შშმ პირებისათვის განკუთვნილი პარკირების ადგილზე ავტომობილის გაჩერების უფლებით, დაჯარიმდება და მისი ავტომობილი

[8] დამატებით იხ. *EDPB*, Guidelines 05/2020 on Consent Under Regulation 2016/679, Version 1.1., 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [24.01.2023].

[9] სრულყოფილი ინფორმაცია თანხმობის სტანდარტთან დაკავშირებით იხ. *EDPB*, Guidelines 05/2020 on Consent Under Regulation 2016/679, Version 1.1., 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [24.01.2023].

გადაყვანილ იქნება საჯარიმო სადგომზე. შესაბამისად, თავისუფლად შეიძლება ითქვას, რომ შშმ პირის საცნობი ნიშნის განთავსების საფუძვლად თანხმობა არ გამოდგება, როგორც მონაცემთა დამუშავების კანონიერი საფუძველი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-2 პუნქტით ჩამოთვლილია განსაკუთრებული კატეგორიის მონაცემების დამუშავების სხვა საფუძვლები, რომელთაგან არცერთი მიესადაგება შშმ პირებისთვის სპეციალური საცნობი ნიშნების გამოყენების დავალდებულებას. ამასთან, არც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლი, რომელიც კანონის მოქმედების სფეროს არეგულირებს, შეიცავს რაიმე საგამონაკლისო ჩანაწერს, რომელიც გავრცელდებოდა მოცემულ შემთხვევაზე.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, არ არსებობს შშმ პირის სატრანსპორტო საშუალების საცნობი ნიშნის სატრანსპორტო საშუალებაზე განთავსების გზით განსაკუთრებული კატეგორიის მონაცემის დამუშავების სათანადო საფუძველი, რაც თავის მხრივ, წარმოადგენს კანონიერების პრინციპის დარღვევას, რომლის თანახმადაც მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად. [10]

3.2. პერსონალური მონაცემის დამუშავება მონაცემთა დამუშავების სხვა პრინციპების ჭრილში

შშმ პირის სატრანსპორტო საშუალების საცნობი ნიშნის სატრანსპორტო საშუალებაზე განთავსების გზით განსაკუთრებული კატეგორიის მონაცემის დამუშავების სათანადო საფუძვლის არარსებობის მიუხედავად, საინტერესოა, რამდენად დაცულია მონაცემთა დამუშავების სხვა პრინციპი, რომელსაც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი არეგულირებს. კერძოდ, ყურადსაღებია აღნიშნული მუხლის „გ“ ქვეპუნქტი, რომლის თანახმად, მონაცემები შეიძლება, დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი.

აღნიშნული პრინციპი საკმაოდ ფართო შინაარსის მატარებელია, თუმცა სტატიის მიზნებისთვის, მხოლოდ განსახილველი შემთხვევის ფარგლებში იქნება მსჯელობა წარმოდგენილი. „პროპორციულობის პრინციპის“ თანახმად, მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი

[10] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მე-4 მუხლის „ა“ ქვეპუნქტი.

მიზნის მისაღწევად. მოცემულ შემთხვევაში ისმის კითხვა, თუ რა არის კანონიერი მიზანი იმისა, რომ შშმ პირს კანონმდებლობა სთხოვს, განათავსოს სპეციალური საცნობი ნიშანი სატრანსპორტო საშუალებაზე, იმ შემთხვევაში, თუ მას სურს ისარგებლოს შშმ პირებისათვის განკუთვნილ ადგილზე პარკირების უფლებით. მიზანი მოცემულ შემთხვევაში არის ის, რომ უფლებამოსილ პირებს, რომლებიც მონიტორინგს ახორციელებენ, მიეცეთ შესაძლებლობა, დააიდენტიფიცირონ ნამდვილად შშმ პირის სატრანსპორტო საშუალებაა თუ არა გაჩერებული პარკირების შესაბამის ადგილას. სხვა შემთხვევაში, უშუალოდ სატრანსპორტო საშუალებით გადაადგილებისას[11], „საგზაო მოძრაობის შესახებ“ საქართველოს კანონის მე-19 მუხლის მე-2 პუნქტი ნებაყოფლობითს ხდის შშმ პირის საცნობი ნიშნის გამოყენებას, რადგან მისი გამოყენება არ არის დაკავშირებული საგზაო მოძრაობის უსაფრთხოებასთან.

რადგანაც მონაცემთა დამუშავების ერთადერთი მიზანი არის შესაბამისი სატრანსპორტო საშუალების სტატუსის დადგენა, კითხვები, რაც უნდა დაისვას არის ის, რომ ერთი მხრივ, შესაძლებელია, თუ არა იგივე კანონიერი მიზნის მიღწევა უფრო ნაკლები მოცულობის მონაცემების დამუშავების გზით, ხოლო მეორე მხრივ, რამდენად ადეკვატური და რელევანტურია ის შშმ პირის საცნობი ნიშანი, როგორც განსაკუთრებული კატეგორიის მონაცემი შესაბამისი სატრანსპორტო საშუალების სტატუსის დადგენის მიზნით?

პროპორციულობის პრინციპის დაცვა უნდა შეფასდეს არა მხოლოდ რაოდენობრივი, არამედ ხარისხობრივი საზომით. კერძოდ, მხოლოდ საცნობი ნიშნის გამოყენება შესაძლოა, რაოდენობრივი თვალსაზრისით, აკმაყოფილებდეს მონაცემთა მინიმიზაციას და საცნობი ნიშანი მინიმალური მოცულობის მონაცემს წარმოადგენდეს ზემოაღნიშნული კანონიერი მიზნის მისაღწევად, თუმცა, უნდა დაისვას კითხვა, გამოყენებული მექანიზმი რამდენად ითვალისწინებს მინიმალურ ჩარევას ადამიანის უფლებებში და ხარისხობრივად რამდენად მინიმალური მონაცემის დამუშავება ხორციელდება. ხომ არ არის შესაძლებელი, უფრო ნაკლები ჩარევის ხარისხის მქონე მონაცემის დამუშავების მეთოდის გამოყენების გზით მიღწეულ იქნეს იდენტური მიზანი? აქვე გასათვალისწინებელია ის, თუ რამდენად შესაძლებელია სხვა, უფრო მსუბუქი მეთოდის გამოყენება ტექნოლოგიური თვალსაზრისით, რადგან ტექნოლოგიური პროგრესის კვალდაკვალ, ის რაც წარსულში შეუძლებელი იყო, დღეს მარტივად შესრულებადია.

აღსანიშნავია ე. წ. „უნივერსალური დიზაინის“ ვალდებულება, რომელიც შეზღუდული შესაძლებლობის მქონე პირთა უფლებების კონვენციის ხელმოწერით

[11] თუმცა „საგზაო მოძრაობის შესახებ“ საქართველოს კანონის მე-19 მუხლი მე-2 პუნქტი არ აკეთებს კონკრეტულ მითითებას, თუ როდისაა საცნობი ნიშნის გამოყენება ნებაყოფლობითი და როდის სავალდებულო, რაც თავის მხრივ, ბუნდოვანს ხდის აღნიშნულ ჩანაწერს.

აიღეს წევრმა სახელმწიფოებმა.[12] კონვენციის მე-2 მუხლის მიხედვით, „უნივერსალური დიზაინი გულისხმობს პროდუქტის, გარემოს, პროგრამებისა და მომსახურების ისეთ დიზაინს, რომელიც ყველა ადამიანს აძლევს მისი მაქსიმალური გამოყენების საშუალებას, ადაპტაციისა და სპეციალური დიზაინის გამოყენების აუცილებლობის გარეშე. „უნივერსალური დიზაინი" არ გამორიცხავს საჭიროების შემთხვევაში, შეზღუდული შესაძლებლობის მქონე კონკრეტული ჯგუფის მიერ დამხმარე საშუალებების გამოყენებას." ამავე კონვენციის მე-4 მუხლის თანახმად, „მონაწილე სახელმწიფოები იღებენ ვალდებულებას, უზრუნველყონ და ხელი შეუწყონ შეზღუდული შესაძლებლობის მქონე პირთა მიერ ადამიანის უფლებებისა და ძირითად თავისუფლებათა სრულ რეალიზებას, შეზღუდული შესაძლებლობის საფუძველზე აღმოცენებული ყოველგვარი დისკრიმინაციის გარეშე. ამ მიზნით, მონაწილე ქვეყნები ვალდებულებას იღებენ, განახორციელონ ან ხელი შეუწყონ წინამდებარე კონვენციის მე-2 მუხლით განსაზღვრული, ისეთი სახის უნივერსალური დიზაინის მქონე პროდუქტის, მომსახურების, დანადგარებისა და მოწყობილობების კვლევა-გამოგონებით საქმიანობას, რომელთა შეზღუდული შესაძლებლობის მქონე პირთა სპეციფიკურ საჭიროებებზე მორგება მინიმალურ ადაპტაციასა და თანხებს მოითხოვს; ხელი შეუწყონ მათ გამოყენებასა და მისაწვდომობას, სტანდარტებისა და სახელმძღვანელოების შექმნაში უნივერსალური დიზაინის იდეის გატარებას."

უნივერსალური დიზაინი ემსახურება სწორედ იმ მიზანს, რომ შშმ პირთა საჭიროებების ადაპტაცია ყოველდღიურ ცხოვრებაში, განხორციელდეს იმგვარად, რომ არ ხდებოდეს აღნიშნულის გამოკვეთა და აფიშირება და საჭიროებების უზრუნველყოფა მაქსიმალურად შეუმჩნეველი იყოს გარეშე თვალისთვის.

3.3. შშმ პირის სატრანსპორტო საშუალებაზე დასამაგრებელი საცნობი ნიშნის ალტერნატივა, როგორც პერსონალურ მონაცემთა დაცვის უფლებაში ჩარევის მინიმალური საშუალება

ალტერნატიულ საშუალებაზე მსჯელობის ფარგლებში, მნიშვნელოვანია, შევეხოთ არსებულ პრაქტიკას, რომელიც გამოიყენება პარკირების წესის დაცვის მონიტორინგის მიზნით. დღესდღეობით, შპს „თბილისის სატრანსპორტო კომპანიას"[13] აქვს მინიჭებული

[12] „შეზღუდული შესაძლებლობის მქონე პირთა უფლებების კონვენციას" თანდართული დეკლარაციის გათვალისწინებით, საქართველომ ხელი 2013 წელს მოაწერა (საქართველოს პარლამენტის 2013 წლის 26 დეკემბრის N1888-რს დადგენილება გაერთიანებული ერების ორგანიზაციის „შეზღუდული შესაძლებლობის მქონე პირთა უფლებების კონვენციის" თანდართული დეკლარაციის გათვალისწინებით რატიფიცირების შესახებ).

[13] თბილისის სატრანსპორტო კომპანიის ოფიციალური ვებგვერდი: <https://ttc.com.ge/> [24.01.2023]

თბილისში პარკირებასთან დაკავშირებულ სამართალდარღვევებზე, საქართველოს კანონმდებლობით დადგენილი წესით საჯარიმო ქვითრის – ადმინისტრაციული სამართალდარღვევის ოქმის შევსების უფლებამოსილება.

შპს „თბილისის სატრანსპორტო კომპანიის“ თანამშრომლებს სპეციალური ელექტრო ხელსაწყოს საშუალებით წვდომა აქვთ ელექტრონულ მონაცემთა ბაზასთან, სადაც ისინი მომენტალურად ხედავენ, გადახდილი აქვს თუ არა პირს პარკირების საფასური ან გააქტიურებული აქვს თუ არა ზონალური პარკირების დაწყების ფუნქციონალი. ამისათვის, „თბილისის სატრანსპორტო კომპანიას“ არ სჭირდება რაიმე საცნობი ნიშანი და მისი თანამშრომლების გარდა, არავინ იცის არიდებს თუ არა კონკრეტული მძღოლი თავს პარკირების საფასურის გადახდას. მძღოლებისათვის უაღრესად გამარტივებულია პარკირების ფუნქციის გააქტიურება და თბილისის სატრანსპორტო კომპანია რამდენიმე ალტერნატივასაც კი სთავაზობს მათ ამისთვის (მობილური აპლიკაცია, ვებგვერდი ან გადახდის აპარატი).

მატერიალური ფორმით არსებული ლამინირებული საშვების დრო ნელ-ნელა მიდის და მას თანამედროვე მარტივი ტექნოლოგიური საშუალებები ანაცვლებენ. ზემოაღნიშნული, იდენტური მექანიზმის გამოყენებით, შესაძლებელია შშმ პირთა სატრანსპორტო საშუალებების იდენტიფიცირება არა მატერიალური ფორმის საცნობი ნიშნის გამოყენებით, არამედ ელექტრონულად, კონფიდენციალურობის მაქსიმალური დაცვით. კერძოდ, ყოველგვარი საშვის გარეშე, მონიტორინგის თანამშრომლის მიერ სპეციალური ხელსაწყოს გამოყენებით მოხდეს სატრანსპორტო საშუალების გადამოწმება ელექტრონულ მონაცემთა ბაზაში, სადაც კონკრეტული სატრანსპორტო საშუალებებისთვის მინიჭებული იქნება პარკირების უფლება შშმ პირებისათვის განკუთვნილ პარკირების ადგილზე. თუმცა, ამ კუთხით, პრობლემას წარმოშობს არსებული პრაქტიკა, რომლის თანახმადაც, საცნობი ნიშნები გაიცემა პიროვნებაზე და არა სატრანსპორტო საშუალებაზე. ერთადერთი გამონაკლისია, როდესაც სატრანსპორტო საშუალების მესაკუთრე იურიდიული პირია, რომელიც შშმ პირის/პირების ტრანსპორტირებას უზრუნველყოფს. გარკვეული ლოგიკა ამაში დევს, რამეთუ შშმ პირი არ არის შეზღუდული, ვისი სატრანსპორტო საშუალებით იმგზავრებს და მას ნებისმიერ სატრანსპორტო საშუალებაზე გააჩნია საკუთარი საცნობი ნიშნის განთავსების უფლება.

მიუხედავად გაპიროვნებული საცნობი ნიშნის დადებითი მხარეებისა, მას უარყოფითი მხარეც ბევრი აქვს. კერძოდ, აღნიშნული შეიცავს საცნობი ნიშნის უკანონოდ, არამიზნობრივად გამოყენების საშუალებას. მოქმედი კანონმდებლობის თანახმად, შშმ პირს არ აქვს უფლება, საკუთარი საცნობი ნიშანი სხვას გადასცეს, თუმცა მსგავსი შემთხვევის პრევენციის საშუალება ფაქტობრივად არ არსებობს.[14] როგორ უნდა

[14] საცნობი ნიშანი გამოყენებულ უნდა იქნეს მხოლოდ იმ პირის მიერ ან/და სატრანსპორტო საშუალებისთვის, რომლისთვისაც ის გაიცა. ქალაქ თბილისის მუნიციპალიტეტის საკრებულოს 2016 წლის

დაადგინოს მონიტორინგის განმახორციელებელმა პირმა, ნამდვილად შშმ პირი გადაადგილდება კონკრეტული ავტომობილით, თუ სხვა პიროვნება, როდესაც ავტომობილზე განთავსებული საცნობი ნიშანი არანაირ მონაცემს შეიცავს სატრანსპორტო საშუალების შესახებ.

არსებობს ასევე საცნობი ნიშნის დაკარგვის ან დაზიანების რისკი, რის შესახებ მფლობელი ვალდებულია შესაბამისი ინფორმაცია დაუყოვნებლივ მიაწოდოს სააგენტოს.[15] საცნობი ნიშნის დაკარგვისას, მისი აღდგენის თხოვნით სააგენტოს წერილობით მიმართავს საცნობი ნიშნის კანონიერი მფლობელი და აღდგენისთვის მასვე ეკისრება ქალაქ თბილისის მუნიციპალიტეტის მერიის ანგარიშზე თანხის გადახდის ვალდებულება ათი ლარის ოდენობით.[16] სახელმწიფოს მხრიდან შშმ პირებისადმი მსგავსი მიდგომა არ არის მიზანშეწონილი. არ შეიძლება შშმ პირს საცნობი ნიშნის დაკარგვის თუ შემთხვევით განადგურების გამო, მიზანმიმართულად შეექმნას დაბრკოლება და ვერ ისარგებლოს საქართველოს კანონმდებლობით განსაზღვრული უფლებებით.

მიზანშეწონილია, პარკირების დროის გააქტიურების მსგავსად, საცნობი ნიშნის ნაცვლად, შესაბამისი მონიტორინგის სამსახურის თანამშრომელი ელექტრონულად ხედავდეს კონკრეტულ ავტომობილზე ვრცელდება თუ არა შშმ პირის სტატუსიდან გამომდინარე პარკირების უფლება. აღნიშნულისთვის კი საჭიროა, რომ გაპიროვნებული საცნობი ნიშნები არ იყოს ერთადერთი არჩევანი და მას ჰქონდეს ალტერნატივა. კონკრეტული მდგომარეობიდან გამომდინარე, შშმ პირებისათვის შესაძლოა არსებობდეს რამდენიმე ალტერნატივა:

პირველი, შესაძლებელი უნდა იყოს შშმ პირის სატრანსპორტო საშუალების რეგისტრაცია, რა დროსაც, არანაირი საცნობი ნიშნის დამზადება აღარ იქნება საჭირო, რადგან სატრანსპორტო საშუალების გადამოწმება ელექტრონულად იქნება შესაძლებელი. ასეთი მიდგომა ასევე მოხსნის ერთი საცნობი ნიშნის სხვადასხვა მუნიციპალიტეტის ადმინისტრაციულ საზღვრებში გამოყენების არსებულ ბარიერს.

მეორე, შშმ პირს უნდა ჰქონდეს არა ერთი, არამედ რამდენიმე სატრანსპორტო საშუალების რეგისტრაციის უფლება, თუ მას სხვადასხვა სატრანსპორტო საშუალებით უწევს გადაადგილება (მაგალითად, შშმ პირის საკუთრებაში ორი ავტომობილია).

მესამე, თუ შშმ პირი წინასწარ ვერ ასახელებს ავტოსატრანსპორტო საშუალებას, რითაც იგი აპირებს მგზავრობას, საგამონაკლისო სახით, საცნობი ნიშნის მიღება მხოლოდ და მხოლოდ მის სურვილზე უნდა იყოს დამოკიდებული.

27 დეკემბრის N33-99 დადგენილებით დამტკიცებულია ქალაქ თბილისის ადმინისტრაციულ საზღვრებში სატრანსპორტო საშუალებების პარკირების რეგულირების წესის მე-11 მუხლის მე-9 პუნქტი.

[15] იქვე.

[16] იქვე.

4. დასკვნა

მნიშვნელოვანია, არ არსებობდეს ყველასთვის ერთნაირი მიდგომა, მით უმეტეს, თუ ასეთი მიდგომა იწვევს განსაკუთრებული კატეგორიის მონაცემის ნებისმიერ შემთხვევაში არაპროპორციულად, იმაზე მეტი მოცულობით დამუშავებას, რაც არ არის აუცილებელი კანონიერი მიზნის მისაღწევად.

სტატიაში მოყვანილი ალტერნატივები საშუალებას მისცემს შშმ პირს, კანონმდებლობით განსაზღვრული პირობების დაკმაყოფილების შემთხვევაში, დაარეგისტრიროს სატრანსპორტო საშუალება და მოახდინოს მისი პარკირება შშმ პირებისათვის განკუთვნილ ზონებში. მას არ დასჭირდება საცნობი ნიშანი, რადგან მონიტორინგის განმახორციელებელი უფლებამოსილი პირი ავტომობილის ნომრის მიხედვით გადაამოწმებს შესაბამის ინფორმაციას. თუ შშმ პირს ჰყავს რამდენიმე ავტომობილი ან რამდენიმე ავტომობილით უწევს გადაადგილება, მას უფლება უნდა ჰქონდეს მოახდინოს ამ ავტომობილების რეგისტრაცია შესაბამის ბაზაში, რათა შეძლოს რეგისტრირებული ავტომობილების პარკირება შშმ პირებისათვის განკუთვნილი პარკირების ადგილზე. აღნიშნული გზები უზრუნველყოფს განსაკუთრებული კატეგორიის მონაცემის მინიმალურად დამუშავებას და თავიდან აგვარიდებს შშმ პირის მიერ საცნობი ნიშნის განთავსების ვალდებულებას.

იმ შემთხვევაში, თუ შშმ პირს სურს, ჰქონდეს განპიროვნებული საცნობი ნიშანი (როდესაც საცნობი ნიშანი არ შეიცავს სატრანსპორტო საშუალების სახელმწიფო ნომერს), მხოლოდ მისი მოთხოვნით, მას ექნება შესაძლებლობა, მიიღოს საცნობი ნიშანი, რომლის გამოყენებაც მხოლოდ და მხოლოდ მისი ნების გამოვლენის შედეგი იქნება. ასეთი შემთხვევებისთვის მნიშვნელოვანია, ყველა მუნიციპალიტეტმა საკუთარ ადმინისტრაციულ საზღვრებში მიანიჭოს იურიდიული ძალა სხვა მუნიციპალიტეტის მიერ გაცემულ საცნობ ნიშანს (როგორც ეს გააკეთა ფოთის მუნიციპალიტეტმა).

ყოველივე ზემოაღნიშნული უზრუნველყოფს, შშმ პირმა თავად მიიღოს გადაწყვეტილება და თუ მას გარკვეული მიზეზების გამო არ სურს, სატრანსპორტო საშუალებაზე დაამაგროს შშმ პირისათვის განკუთვნილი საცნობი ნიშანი, მას მაინც ჰქონდეს შესაძლებლობა, ისარგებლოს შშმ პირებისათვის განკუთვნილ პარკირების ადგილებზე სატრანსპორტო საშუალების პარკირების უფლებით.

ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, 786, 24/08/1995.
2. შეზღუდული შესაძლებლობის მქონე პირთა უფლებების კონვენცია, მიღებულია გაერთიანებული ერების ორგანიზაციის 2006 წლის 13 დეკემბრის A/RES/61/106 რეზოლუციით.
3. ადგილობრივი თვითმმართველობის კოდექსი, 1958-IIს, 05/02/2014.
4. „შეზღუდული შესაძლებლობების მქონე პირთა უფლებების შესახებ“ საქართველოს კანონი, 6823-რს, 28/07/2022.
5. „საგზაო მოძრაობის შესახებ“ საქართველოს კანონი, 1830-რს, 24/12/2013.
6. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
7. საქართველოს პარლამენტის 2013 წლის 26 დეკემბრის N1888-რს დადგენილება გაერთიანებული ერების ორგანიზაციის „შეზღუდული შესაძლებლობის მქონე პირთა უფლებების კონვენციის“ თანდართული დეკლარაციის გათვალისწინებით რატიფიცირების შესახებ.
8. ქალაქ თბილისის მუნიციპალიტეტის საკრებულოს 2016 წლის 27 დეკემბრის N33-99 დადგენილებით დამტკიცებულია ქალაქ თბილისის ადმინისტრაციულ საზღვრებში სატრანსპორტო საშუალებების პარკირების რეგულირების წესი.
9. „ბორჯომის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების რეგულირების შესახებ“ ბორჯომის მუნიციპალიტეტის საკრებულოს 2011 წლის 18 მარტის N7 დადგენილება.
10. „ქალაქ ფოთის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესის დამტკიცების შესახებ“ თვითმმართველი ქალაქი ფოთის 2014 წლის 7 ივლისის N14/18 დადგენილება.
11. „სიღნაღის მუნიციპალიტეტის ტერიტორიაზე ავტოსატრანსპორტო საშუალებების პარკირების წესის დამტკიცების შესახებ“ სიღნაღის მუნიციპალიტეტის საკრებულოს 2019 წლის 29 ოქტომბრის N30 დადგენილება.
12. *EDPB*, Guidelines 05/2020 on Consent Under Regulation 2016/679, Version 1.1., 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [24.01.2023].
13. თბილისის სატრანსპორტო კომპანია, <https://ttc.com.ge/> [24.01.2023].

პერსონალურ მონაცემთა
დაცვის სამსახური

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