პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

N2,2024

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

№2, 2024

P-ISSN 2720-8753

E-ISSN 2720-8761

სარჩევი

მთავარი რედაქტორისაგან

წარმოგიდგენთ „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ მორიგ გამოცემას, რომელიც პირადი ცხოვრების ხელშეუხებლობის დინამიკურად ცვალებად სირთულეებს ასახავს და მონაცემთა დაცვის სამართლის აქტუალურ საკითხებს განიხილავს.

გასული ათწლეულის ბოლო პერიოდში გაძლიერდა მონაცემთა დაცვის ფუნდამენტური უფლების ერთგვაროვანი რეგულირებისა და ერთიანი პრაქტიკის დამკვიდრების მცდელობები. პერსონალურ მონაცემთა დაცვის ფუნდამენტური უფლება გარანტირებული საქართველოს კონსტიტუციის მე-15 მუხლით, უზრუნველყოფს პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცულობას. დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების, ან სხვათა უფლებების დაცვის მიზნით ამ უფლებათა შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, სასამართლოს გადაწყვეტილებით ან მის გარეშეც, კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას. ამ უკანასკნელ შემთხვევაში უფლების შეზღუდვის შესახებ უნდა ეცნობოს სასამართლოს, რომელიც ადასტურებს შეზღუდვის კანონიერებას.

ციფრულ ეპოქაში, როდესაც ტექნოლოგიური განვითარება და მონაცემთა გამჭვირვალე მიმოცვლა ყოველდღიურად ახალ სამართლებრივ თუ ეთიკურ კითხვებს აჩენს, მნიშვნელოვანია, რომ საზოგადოების ცნობიერება მიესადაგებოდეს უალტერნატივო საჭიროებას — ადამიანის ფუნდამენტური უფლებების დაცვის აუცილებლობას ტექნოლოგიური პროგრესის გათვალისწინებით. პერსონალურ მონაცემთა უფლების დაცვისა და ამ თვალსაზრისით საზოგადოების ცნობიერების ამაღლების ერთ-ერთ საუკეთესო საშუალებას წარმოადგენს სამართლებრივი დისკუსია პერსონალურ მონაცემთა დამუშავების აქტუალურ საკითხებზე. სწორედ ამ მიზანს ემსახურება პერსონალურ მონაცემთა დაცვის სამსახურის სამეცნიერო ჟურნალი.

ჟურნალის წინამდებარე გამოცემა მკითხველს პერსონალურ მონაცემთა დაცვის სხვადასხვა აქტუალურ საკითხზე ღრმა სამართლებრივ ანალიზსა და ხედვას სთავაზობს. გამოქვეყნებული ნაშრომები შეეხება ისეთ საკითხებს, როგორებიცაა: პერსონალურ მონაცემთა დაცვის ევროპული სტანდარტების ინტერპრეტაცია და იმპლემენტაცია, მონაცემთა დაცვის საზედამხედველო ორგანოთა საქმიანობა და როლი, ტექნოლოგიური ტრანსფორმაციის ახალი საკანონმდებლო ჩარჩო და სხვა.

მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორის, გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლის, წინამდებარე ჟურნალის სარედაქციო კოლეგიის წევრის — ნორბერტ ბერნსდორფის სამეცნიერო პუბლიკაცია განიხილავს პერსონალურ მონაცემთა დაცვას ელექტრონული ვაჭრობის კონტექსტში, „ციფრული სერვისების აქტსა“ და მისი იმპლემენტაციის საკითხს ეროვნულ კანონმდებლობაში. ნაშრომს აქტუალობას სძენს ევროკავშირის „ციფრული სერვისების აქტით“ გათვალისწინებული ახალი ვალდებულებები ციფრული მომსახურების მიმწოდებლებისათვის, რაც მნიშვნელოვანია მონაცემთა სუბიექტების უფლებების დაცვის თვალსაზრისითაც. მსურს განსაკუთრებული მადლიერება გამოვთქვა პროფესორ ნორბერტ ბერნსდორფის მიმართ ჟურნალის ყველა გამოცემაში სამეცნიერო კონტრიბუციისა და სამსახურთან აქტიური თანამშრომლობისათვის.

მიუნსტერის უნივერსიტეტის ინფორმაციის, ტელეკომუნიკაციებისა და მედია სამართლის ინსტიტუტის დირექტორის — პროფესორ თომას ჰიორენის, ამავე უნივერსიტეტის ასისტენტ-მკვლევრის — ფილიპ მაიერისა და საერთაშორისო იურიდიული ფირმის ასისტენტ-მკვლევრის — გესა შენქეს თანაავტორობით შესრულებული ნაშრომი შეეხება *“Poena Sine Culpa”* პრინციპის არსსა და მოქმედების ფარგლებს პერსონალურ მონაცემთა დაცვის სამართალში. პუბლიკაციაში ასევე გაანალიზებულია ევროკავშირის მართლმსაჯულების სასამართლოს (“ECJ“) ერთ-ერთი უახლესი გადაწყვეტილება საქმეზე *“Deutsche Wohnen”*, რაც განსაკუთრებით ანგარიშგასაწევია პერსონალურ მონაცემთა დამუშავების კანონიერებისა და მონაცემთა სუბიექტის უფლებების დაცვის პერსპექტივიდან.

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასისტენტ-პროფესორის, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის პირველი მოადგილის, სამართლის დოქტორ ოთარ ჩახუნაშვილის სამეცნიერო სტატიაში გაანალიზებულია პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოების პრინციპები. ნაშრომში საკითხი განხილულია პერსონალურ მონაცემთა დამუშავების კანონიერების ძირითადი პრინციპები, რომელთა შესაბამისად ჩვენი სამსახური შეისწავლის მონაცემთა დამუშავების კანონიერებას.

პრაქტიკული თვალსაზრისით უაღრესად საინტერესო კვლევას წარმოადგენს ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასოცირებული პროფესორისა და ადვოკატის — სამართლის დოქტორ სერგი ჯორბენაძის ნაშრომი, რომელიც საადვოკატო საქმიანობის განხორციელებისას პერსონალურ მონაცემთა დამუშავების საკითხს შეეხება. ნაშრომში წარმოდგენილია პერსონალურ მონაცემთა დაცვის სამსახურის უახლესი პრაქტიკა და საკანონმდებლო სტანდარტი.

თანამედროვე ტექნოლოგიური პროგრესის ფონზე პერსონალურ მონაცემთა დაცვის ისეთ აქტუალურ საკითხებს, როგორებიცაა: ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება, დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეო-მონიტორინგი, ხელოვნური ინტელექტის სისტემების სამართლებრივი რეგულირება და პერსონალურ მონაცემთა დაცვასთან დაკავშირებული გამოწვევები, მონაცემთა დაცვა აკადემიური კვლევის პროცესში, პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლები საკუთარ ნაშრომებში განიხილავენ.

მსურს განსაკუთრებული მადლიერება გამოვხატო თითოეული ავტორის მიერ წინამდებარე გამოცემის მომზადების პროცესში შეტანილი ფასდაუდებელი წვლილისა და გაწეული შრომისთვის. ჟურნალის მიზანია, ხელი შეუწყოს მონაცემთა დაცვის სტანდარტის გაუმჯობესებასა და ცნობიერების ამაღლებას. თითოეული ნაშრომი პროფესიულ დისკურსში მნიშვნელოვანი ღირებულების მქონეა და აღრმავებს საზოგადოების სამართლებრივ განათლებას. ვიმედოვნებთ, რომ, გამოქვეყნებული პუბლიკაციების სამეცნიერო და პრაქტიკული მნიშვნელობიდან გამომდინარე, წინამდებარე გამოცემა დიდ დახმარებას გაუწევს პროფესიონალ იურისტებს, ამ საკითხებზე მომუშავე მკვლევრებს და მიიზიდავს მკითხველთა ფართო წრეს.

დოქტ., დოქტ. ლელა ჯანაშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

ბარსელონის ავტონომიური უნივერსიტეტის ასოცირებული პროფესორი

ნორბერტ ბერნსდორფი[*]

ელექტრონული ვაჭრობა და მონაცემთა დაცვა - ციფრული სერვისების აქტი და მისი იმპლემენტაცია ეროვნულ კანონმდებლობაში

როგორც „ევროპის მონაცემთა სტრატეგიის“ ნაწილი, ევროკომისია დიდი ხანია ცდილობს მონაცემთა ერთიანი ევროპული შიდა ბაზრის შექმნას და ახალი რეგულაციების დადგენას ხელოვნური ინტელექტის გამოყენებისათვის. არსებობს კონფლიქტი, ერთი მხრივ, ევროკავშირის ძირითად უფლებათა ქარტიის მე-8 მუხლით დადგენილ მონაცემთა დაცვის ვალდებულებსა და, მეორე მხრივ, პერსონალური მონაცემების დამუშავების გამარტივების აუცილებლობას შორის, რაც მნიშვნელოვანია ციფრული ეკონომიკისთვის. ევროკომისიის მიერ შემოთავაზებული სხვადასხვა კანონით (მონაცემთა მართვის აქტი, მონაცემთა აქტი, ციფრული სერვისების აქტი და ციფრული ბაზრის აქტი) შეიქმნა აუცილებელი საკანონმდებლო ჩარჩო. ციფრული სერვისების აქტი ახალ ვალდებულებებს აკისრებს ციფრული მომსახურების მიმწოდებლების.

საკვანძო სიტყვები: *მონაცემთა დაცვა ინტერნეტსივრცეში, ციფრული სერვისების აქტი, მონაცემთა შიდა ბაზარი, ელექტრონული ვაჭრობა, ციფრული სერვისები, ტრანსმისია, ონლაინ პლატფორმა, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”).*

1. შესავალი

ციფრული სერვისები საზოგადოებრივ ცხოვრებაზე დიდწილად ახდენს გავლენას და სხვადასხვა გზით ხელს უწყობს მის განვითარებას. კერძოდ, ციფრული სერვისები გამოიყენება კომუნიკაციის, ონლაინ ვაჭრობის, ინტერნეტში ინფორმაციის მოძიებისა ან/და ციფრულ სივრცეში გართობის მიზნით (ონლაინ თამაშები, მუსიკა ან ფილმები). აქედან გამომდინარე, ონლაინ სერვისების მრავალ კატეგორიას განასხვავებენ.

[*] მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის სარედაქციო კოლეგიის წევრი.

თითოეული პირის მიერ პერსონალური მონაცემების დამუშავება, გარდა პირადი მიზნით დამუშავებისა, უნდა შეესაბამებოდეს ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციის“ (“GDPR”) მოთხოვნებს.[1] არაუფლებამოსილი პირისთვის ინფორმაციის მიწოდება, შესაძლოა, შეფასდეს, როგორც მონაცემთა უსაფრთხოების დარღვევა, ისევე, როგორც მომხმარებლის მონაცემების გაუმართლებლად დიდი ხნის განმავლობაში შენახვა ან კომპანიის მიერ პირის შესახებ შენახული მონაცემების შესახებ ინფორმაციის დაგვიანებით მიწოდება. აღნიშნული პროცესები რეგულირდება ძირითადი რეგულაციით (“GDPR”), რადგან მოიცავს ფიზიკური პირებისგან ანალოგურ ან ციფრულ ფორმატში შეგროვებულ პერსონალურ მონაცემების დამუშავებას. თუმცა ყველა მონაცემი ფიზიკური პირებისგან არ გროვდება. მონაცემები მუშავდება, ასევე, მაშინაც, როდესაც კომპანიები ინახავენ სხვადასხვა მონაცემებს კომპიუტერებში, მობილურ ტელეფონებსა და პროგრამული უზრუნველყოფის მოწყობილობებზე, ოპერაციულ სისტემებსა და „ბრაუზერებში“. თუ ვებგვერდის ან აპლიკაციის პროვაიდერს მოწყობილობაზე წვდომა არ აქვს, მოწყობილობებს პროვაიდერის სერვერებთან დაკავშირება არ შეუძლია. თუმცა, აღნიშნული უნდა განხორციელდეს, რათა მოხდეს მონაცემთა გადაცემა, რაც იწვევს კონტენტის გადატანას პროვაიდერის სერვერიდან ბოლო მოწყობილობაზე სურათების, ტექსტის ან ხმის სახით. ევროკავშირის ფარგლებში (“EU”) ამ ტიპის მონაცემთა დამუშავება არ წესრიგდება ძირითადი რეგულაციით (“GDPR”), არამედ უფრო ახალი ციფრული სერვისების აქტით (“DSA”).[2]

2. ციფრული სერვისების აქტის მიზანი

მომავალში ციფრული სერვისების აქტი დაარეგულირებს ციფრული სერვისის მიმწოდებლების საქმიანობას ევროკავშირის მასშტაბით, რაც შექმნის ციფრული პოლიტიკის რეგულაციების ერთ-ერთ ყველაზე მნიშვნელოვან კომპლექტს. „ციფრული ბაზრის აქტთან“ (“DMA”)[3] ერთად, მოსალოდნელია, რომ იგი გახდეს ინტერნეტსივრცის რეგულირების ერთგვარი ძირითადი კანონი, რომლის მთავარი მიზანია მონაცემთა უკონტროლო დამუშავების კონტროლი ელექტრონული ვაჭრობის სფეროში.

2022 წლის 16 ნოემბერს ციფრული სერვისების აქტი შევიდა ძალაში ევროკავშირის მასშტაბით. საწყის ეტაპზე, ციფრული სერვისების აქტის

[1] Regulation (EU) 2016/679 of the European Parliament and of 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, OJ 2016 L 119, pp. 1.

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, OJ 2022 L 277, pp. 1.

[3] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ 2022 L 265, pp. 1.

მოქმედება ვრცელდებოდა მხოლოდ დიდ ონლაინ პლატფორმებსა და საძიებო სისტემებზე. რეგულაცია სრულად ამოქმედდა 2024 წლის 17 თებერვალს. მისი მიზანია დაიცვას ევროპელი მომხმარებლები, მათი ფუნდამენტური უფლებები ციფრულ სივრცეში და უზრუნველყოს თანაბარი პირობები. ციფრული ბაზრისა და ციფრული სერვისების აქტის მიზანია შექმნას ყოვლისმომცველი სახელმძღვანელო ინტერნეტრეგულირებისთვის. აქედან გამომდინარე, უახლოეს პერიოდში ციფრული სერვისების მიმწოდებლები არსებითი ცვლილებების წინაშე აღმოჩნდებიან. ევროპულმა საბჭომ, ევროპარლამენტთან ერთად, ციფრული სერვისების აქტი ციფრული ბაზრის გაძლიერების მიზნით მიიღო.

ციფრული სერვისების აქტი მკაფიო წესებისა და გამჭვირვალობის ვალდებულებების გზით აძლიერებს მომხმარებელთა დაცვის სტანდარტს ციფრულ სივრცეში. აღნიშნული მოიცავს მკაფიო ვალდებულებების დაწესებას ონლაინ პლატფორმებსა და სოციალურ მედიისთვის. კერძოდ, აქტი არეგულირებს უკანონო კონტენტსა და პროდუქტებს. ასევე, ხელს უწყობს უსაფრთხო და გამჭვირვალე ციფრული გარემოს შექმნას. დებულებები, ასევე, იცავს გამოხატვის თავისუფლებას შინაარსის მოდერაციის მკაფიო წესების დადგენის გზით. საშუამავლო სერვისის პროვაიდერები, მაგალითად, ჰოსტინგის სერვისები, ონლაინ ბაზრები და სოციალური ქსელები, უნდა შეესაბამებოდეს აქტის გამჭვირვალობისა და ანგარიშვალდებულების მოთხოვნებს. აღნიშნული ქმნის ერთიან საკანონმდებლო ბაზას ციფრული სერვისებისთვის ევროკავშირის მასშტაბით.

3. არაევროპული დირექტივა, არამედ ევროპული რეგულაცია

ევროკავშირის წევრ ქვეყნებში ციფრული სერვისების აქტი 2024 წლის 17 თებერვლიდან ამოქმედდა, რომელსაც ეროვნულ კანონმდებლობაში შემდგომი იმპლემენტაცია აღარ ესაჭიროება. სამართლებრივი თვალსაზრისით, აღნიშნული წარმოადგენს ევროპულ რეგულაციას და არა მხოლოდ დირექტივას.

ევროპული დირექტივები ევროკავშირის წევრი ქვეყნებისთვის კონკრეტულ მიზნებს განსაზღვრავს, თუმცა სახელმწიფოებს საშუალებას აძლევს თავად გადაწყვიტონ მიზნების მიღწევის გზები. მათ უნდა განახორციელონ იმპლემენტაცია გარკვეულ ვადებში საკუთარი ეროვნული კანონმდებლობის მეშვეობით. ამის საპირისპიროდ, ევროკავშირის რეგულაციები სავალდებულოა ყველა წევრი ქვეყნისათვის და, დირექტივის მსგავსად, არ იზღუდება მხოლოდ მისაღწევი შედეგით.

რამ აიძულა ევროკავშირი მიეღო ციფრული სერვისების აქტი, როგორც რეგულაცია?

მონაცემთა დაცვის წინამორბედი კანონით, ევროკავშირის ყველა წევრი ქვეყანა იზიარებდა ერთსა და იმავე სამართლებრივ საფუძველს, თუმცა შესაძლებელი იყო მისი განსხვავებული იმპლემენტაცია. აღნიშნულიდან

გამომდინარე, მნიშვნელოვნად განსხვავდებოდა მონაცემთა დაცვის დონეები სხვადასხვა ქვეყნებში. ციფრული სერვისების აქტის მიზანი კი არის აღნიშნული დისბალანსის აღმოფხვრა.

4. დაწვრილებით ციფრული სერვისების აქტის შესახებ

მომდევნო გვერდებზე წარმოდგენილია "DSA"-ის ძირითადი მარეგულირებელი შინაარსი:

4.1. გამოყენების მატერიალური ფარგლები: „ციფრული სერვისები"

ციფრული სერვისების აქტის მოქმედების ფარგლებში არსებული სერვისების სპექტრი ფართოა, რომელთა შორისაა, ონლაინ ბაზრები, სოციალურ ქსელები და საძიებო სისტემები.

"DSA"-ს დებულებები ვრცელდება ყველა „ციფრულ სერვისზე". „ციფრული სერვისები" ძირითადად მოიაზრებს საზოგადოების საინფორმაციო სერვისებს. თითოეული მომსახურება, რომლიც უზრუნველყოფილია ელექტრონულად, როგორც წესი, საფასურის სანაცვლოდ, დისტანციურად და ინდივიდუალური მოთხოვნით[4]. "DSA"-ს მე-2 (1) მუხლით განსაზღვრულია „საშუამავლო სერვისების" მაგალითები:

- ე.წ. „ჰოსტინგის" მომსახურება, რომელიც ინახავს მომხმარებლის მიერ მოწოდებულ ინფორმაციას მათი სახელით.[5]
- ე.წ. "Caching" მომსახურება, რომელიც დროებით ინახავს და გადასცემს მომხმარებლის მიერ მოწოდებულ ინფორმაციას საკომუნიკაციო ქსელში.[6]
- „გადაცემის" მომსახურება, რომელიც გადასცემს მომხმარებლის მიერ მოწოდებულ ინფორმაციას საკომუნიკაციო ქსელში ან იძლევა მასზე წვდომის საშუალებას.[7]

ინდივიდუალური სერვისების მარეგულირებელი სისტემა კლასიფიცირებულია სერვისის როლის, ზომისა და ონლაინ გარემოში გავლენის მიხედვით. ყველაზე დაბალ დონეზე, თითოეული საშუამავლო სერვისის პროვაიდერი ექვემდებარება ძირითად რეგულაციებს[8]. უმაღლეს საფეხურებზე დამატებით არსებობს კუმულაციური ვალდებულებები „ჰოსტინგის" მომსახურების მიმწოდებლებისთვის[9], ონლაინ

[4] იხ. Art. 1 (1) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a Procedure for the Provision of Information in the field of Technical Regulations and of the Rules of Information Society Services, OJ 2015 L 241, pp. 1.
[5] Art. 6 of the DSA.
[6] Art. 5 of the DSA.
[7] Art. 4 of the DSA.
[8] იხ.: Art. 11 et seq. of the DSA.
[9] Art. 16 et seq. of the DSA.

პლატფორმებისთვის[10] და დიდი პლატფორმებისთვის[11]. „ჰოსტინგის“ მომსახურების მიმწოდებლები გათავისუფლებულნი არიან სპეციფიკური ვალდებულებებისაგან და მხოლოდ ზოგადი ვალდებულებების შესრულება ეკისრებათ. თუმცა, ეს ზოგადი ვალდებულებები უკვე მოიცავს ზოგიერთს, რომელიც სპეციალურად ხელოვნურ ინტელექტზეა[12] მორგებული.

ყოვლისმომცველი პირობები, ასევე, ვრცელდება ციფრული სერვისების აქტის 33-ე მუხლის პირველი ნაწილით განსაზღვრულ მსხვილ პლატფორმებზე (45 მილიონზე მეტი მომხმარებელი). ამასთან, ევროკომისიას შეუძლია მაჩვენებელი დაარეგულიროს მოსახლეობის ტენდენციების მიხედვით “DSA”-ის 33(2) მუხლის შესაბამისად, რათა იგი მოიცავდეს ევროკავშირის მოსახლეობის დაახლოებით 10 პროცენტს. „ძალიან დიდ ონლაინ პლატფორმებს“ ყოველწლიური რისკების ანალიზის ჩატარების[13], შემოწმებისა[14] და შესაბამისობის ოფიცრის დანიშვნის ვალდებულება აქვთ.[15]

ციფრული სერვისების აქტი ელექტრონული ვაჭრობის შესახებ დირექტივას 2000[16] წლიდან ნაწილობრივ ანაცვლებს, თუმცა ონლაინ პლატფორმების რეგულირების ფარგლებს სცდება და მათ „სოციალური პასუხისმგებლობის“ ხარისხს აკისრებს ბიზნეს მოდელის შესაბამისად.[17]

4.2. რომელი ციფრული საშუამავლო სერვისების მიმწოდებლები არიან ყურადღების ცენტრში?

ციფრული სერვისების აქტი, როგორც წესი, ვრცელდება ციფრული სერვისების, როგორც მსხვილ, ისე მცირე მიმწოდებლებზე. თუმცა რეგულირების ფარგლები და სათანადო გულმოდგინების ვალდებულებები განსხვავდება სერვისის ტიპისა და ზომის მიხედვით. აღნიშნული ვრცელდება იმ შემთხვევაშიც კი, როდესაც მიმწოდებლები ევროკავშირის გარეთ არიან დაფუძნებული. თუმცა, შესაბამის საშუამავლო სერვისებს უნდა ჰქონდეთ „მნიშვნელოვანი კავშირი“ ევროკავშირთან (მაგალითად, სერვისის მიმწოდებლის ევროკავშირში დაფუძნება). ციფრული სერვისების აქტის რეგულირების სფეროში ხვდებიან ღრუბლოვანი სერვისები, ინტერნეტპროვაიდერები, „ჰოსტინგის“ სერვისის პროვაიდერები, ონლაინ

[10] იხ.: Art. 19 et seq. of the DSA.
[11] Art. 33 et seq. of the DSA.
[12] იხ.: *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, 2022, 256.
[13] Art. 34 et seq. of the DSA.
[14] იხ.: Art. 37 of the DSA.
[15] Art. 41 of the DSA.
[16] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, OJ 2000 L 178, 1.
[17] იხ.: *Beck W.*, Der Entwurf des Digital Services Act - Hintergrund, Ziele und Grundsätze künftiger Regulierung des virtuellen Raums in der EU, Deutsches Verwaltungsblatt (DVBl) 2021, 1000; *von Lewinski K., Rüpke G.; Eckhardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, 2022, 256.

ბაზრები, ვებმაღაზიები, და სოციალურ ქსელები. დღესდღეობით ციფრული სერვისების აქტის მოქმედების სფეროში 19 დიდი ონლაინ სერვისი მოექცა, რომელთა შორისაა:

- Alibaba Aliexpress;
- Amazon Store;
- Apple AppStore;
- Booking.com;
- Bing;
- Google Maps;
- Google Play;
- Google Shopping;
- Instagram;
- LinkedIn;
- Meta (Facebook);
- Temu;
- TikTok;
- Wikipedia;
- X (Twitter);
- YouTube and;
- Zalando.

ზემოხსენებული პლატფორმების უმრავლესობა არა მხოლოდ მნიშვნელოვან გავლენას ახდენს მომხმარებელთა მოსაზრებების ფორმირებაზე ახალი ამბების ფიდების, ონლაინ მაღაზიების საშუალებით, არამედ მათი მხრიდან არსებობს პერსონალური მონაცემების უკონტროლო გამოყენების რისკი.

4.3. ციფრული სერვისების აქტის აღსრულების მექანიზმები

ციფრული სერვისების აქტით ჩამოყალიბდა ორდონიანი აღსრულების სისტემა:[18]

4.3.1. საჩივრების მართვა და მომხმარებლის დაცვა

ციფრული სერვისების აქტი მომხმარებლებს კონკრეტულ უფლებებით აღჭურავს.

იმ შემთხვევაში თუ ონლაინ პლატფორმებზე აღმოჩნდა უკანონო კონტენტი ან დაირღვა მონაცემთა დაცვის კანონმდებლობა, აღნიშნულის შესახებ შეტყობინებები ყურადღებით უნდა იქნეს შესწავლილი; ასევე,

[18] იხ. *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].

უზრუნველყოფილი იყოს საჩივრების განხილვის პროცედურა.[19] მაგალითად, შესაძლებელია, გასაჩივრდეს ონლაინ პლატფორმების გადაწყვეტილებები კონტენტის წაშლასთან ან წაშლაზე უარის თქმასთან დაკავშირებით, ასევე, შემთხვევები, როდესაც მომხმარებლებს პლატფორმაზე წვდომა ეზღუდებათ. მომავალში, მიმწოდებლებს მარტივად და გასაგებად ახსნის ვალდებულება ექნებათ - თუ როგორ მივიდნენ შესაბამის გადაწყვეტილებამდე, ხოლო მომხმარებლებს შესაძლებლობა, რომ სამართლებრივი გზებით მოითხოვონ გადაწყვეტილების გადახედვა.[20]

ციფრული სერვისები აქტი შეეხება ელექტრონულ ვაჭრობასა და ონლაინ რეკლამას. არასრულწლოვანებზე მორგებული მარკეტინგი აკრძალულია. ანალოგიურად, რეკლამები არ უნდა შეეხებოდეს რელიგიურ მრწამსს ან სექსუალურ ორიენტაციას. იგი აუცილებლად უნდა იყოს აღქმული, როგორც რეკლამა. ასევე, მნიშვნელოვანია, რომ შესაძლებელი იყოს რეკლამის დამკვეთის იდენტიფიცირება; გამჭვირვალობის შესახებ ვალდებულებები ამარტივებს პლატფორმებსა და სამართალდამცავ ორგანოებს შორის თანამშრომლობას. ონლაინ პლატფორმებმა უნდა უზრუნველყონ: ა) ვებსაიტზე განთავსებული რეკლამა აღქმული იყოს როგორც რეკლამა; ბ) დამკვეთის ვინაობის დადგენის შესაძლებლობა; გ) ინფორმაციის მიწოდება რეკლამის განთავსების შესახებ.[21] საშუამავლო სერვისებმა, ასევე, უნდა შექმნან საერთო საკონტაქტო პუნქტი ელექტრონული კომუნიკაციისთვის.[22]

4.3.2. აღსრულება ეროვნული საზედამხედველო ორგანოების მიერ

ციფრული სერვისების აქტით ევროკავშირის წევრი ქვეყნები ვალდებულნი არიან გამოყონ სამართალდამცავი ორგანოები, რომლებიც ზედამხედველობას გაუწევენ სერვისის მიმწოდებლების მოქმედებებს. ხოლო „მსხვილი ონლაინ პლატფორმების“ მონიტორინგს განახორციელებს თავად ევროკომისარი.[23]

იქიდან გამომდინარე, რომ ციფრული სერვისების აქტი სხვადასხვა სამართლებრივ ინტერესს იცავს, ევროკავშირის წევრი ქვეყნების[24] რამდენიმე უწყება შეიძლება იყოს “DSA კოორდინატორი”. თუმცა, აუცილებელია, მკაფიოდ დარეგულირდეს უწყებების პასუხისმგებლობის ფარგლები, რათა თავიდან იქნას აცილებული მომხმარებელთა საჩივრების „უწყებათაშორისი პინგ-პონგი“.[25]

---

[19] იხ.: Art. 20, 53 of the DSA.
[20] Art.81 et seq. of the DSA.
[21] *Marx L*., Der Digital Services Act der Europäischen Kommission, AnwaltZertikat IT-und Medienrecht (AnwZert ITR), 4/2021, margin note 2.
[22] Art. 11 et seq. of the DSA.
[23] *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
[24] იხ.: Art. 3 of the DSA.
[25] იხ.: *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].

გერმანიაში ცენტრალური საჩივრებისა და კოორდინაციის განმხილველი ორგანოა ე.წ. "Bundesnetzagentur". გერმანიაში ზედამხედველობას, ასევე, ახორციელებს ე.წ. "Bundeszentrale für Kinder- und Jugendmedienschutz". მომხმარებელთა დაცვის ორგანიზაციებს განსაკუთრებული მნიშვნელობა ენიჭებათ მომხმარებელთა დაცვის თვალსაზრისით, რადგან ისინი კონსულტაციების და საჩივრების მიღების ფუნქციის გამო მომხმარებელთა მაჯისცემაზე უდევთ ხელი.

5. გერმანული კანონი: "Digitale-Dienste-Gesetz"

იქიდან გამომდინარე, რომ ციფრული სერვისების აქტი არის ევროპული რეგულაცია, იგი მოქმედებს ევროკავშირის წევრ ქვეყნებში. ევროპის დირექტივისგან განსხვავებით, მისი ეროვნული კანონმდებლობაში იმპლემენტაცია აღარ არის დამატებით საჭირო. მიუხედავად ამისა, ეროვნული კანონმდებლობა აქტთან შესაბამისობაში უნდა იყოს. დებულებების აღსრულების ვალდებულება თავად ევროკავშირის წევრ ქვეყნებს ეკისრებათ. გერმანიაში "DSA"-ს „თანმხლები" გახდა 2024 წლის 6 მაისის „ციფრული სერვისების კანონი (DDG)"[26]. ეს ფაქტი ხაზს უსვამს იმ სირთულეებს, რომლებიც "DSA"-ს იმპლემენტაციას ახლავს.

5.1. ციფრული სერვისების აქტის შევსება გერმანიის ეროვნული კანონით

2024 წლის 6 მაისის გერმანიის კანონი "DDG" მეტწილად ავსებს "DSA"-ს. აღნიშნულ კონტექსტში, ცვლის ეროვნულ კანონს ციფრული სერვისების შესახებ.[27]

განსაკუთრებული აღნიშვნის ღირსია ონლაინ პლატფორმების პასუხისმგებლობის საკითხი ვებგვერდის კონტენტზე, „მზა ჩანაწერების" დაყენებასა და ჯარიმებზე. "DDG" ფარავს პასუხისმგებლობის საკითხს „ჰოსტინგზე", „ქეშირებასა" და „ტრანსმისიაზე" (ე.წ. „ბრალზე დაფუძნებულ პასუხისმგებლობა"). ამ საკითხზე და ინტერნეტ ოპერატორების პასუხისმგებლობაზე რეგულაციები მოცემულია "DDG" მე-7 და მე-8 პარაგრაფებში. „მზა ჩანაწერების" დაყენებისას აუცილებელია მომხმარებლის მკაფიო თანხმობა ("cookie opt-in").

[26] Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinien 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.6.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Onlinevermittlungsdiensten und zur Änderung weiterer Gesetze vom 6.5.2024 (Digitale-Dienste-Gesetz), Federal Law Gazette 2024, 1.

[27] *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR) 14/2024, margin note 3.

საბოლოოდ, კანონით გათვალისწინებულია დებულებები ჯარიმების შესახებ. მაგალითად, დარღვევის შემთხვევაში ჯარიმა შეიძლება განისაზღვროს 50,000 - 300,000 ევროს ოდენობით.

5.2. ვებგვერდის შესახებ ინფორმაციის მიწოდების ვალდებულება ("Imprint Obligation")

"DDG"-ის ერთ-ერთი მთავარი აქცენტი ვებგვერდის შესახებ ინფორმაციის მიწოდების ვალდებულებაა ("Imprint Obligation"), რაც მოაზრებს სერვისის მიმწოდებლებს იდენტიფიკაციას[28]. აღნიშნული ვალდებულება განმტკიცებულია "DDG"-ის § 5 მუხლით და ვრცელდება კომერციულ ციფრულ სერვისებზე, რომლებიც ძირითადად გარკვეული საფასურის სანაცვლოდ სთავაზობენ მომხმარებლებს. თუმცა მე-5 პარაგრაფი შეეხება არა მხოლოდ ფასიან, არამედ უფასო სერვისებსაც. გადახდის კრიტერიუმი კომერციულ მიზანს გულისხმობს.[29]

ე.წ. „ინფლუენსერი" ვებსაიტებსაც აქვთ ზემოხსენებული ვალდებულება, თუ ისინი რეკლამას უკეთებენ პროდუქტებს ან სერვისებს. აღნიშნული არ მოიცავს მხოლოდ იმ ფულად შემოსავალს, რომელსაც კომპანია უხდის ინფლუენსერს რეკლამის განთავსებისთვის. ის, ასევე მოიცავს არაფულად შემოსავალს, მაგალითად, თუ კომპანიამ ინფლუენსერს უსასყიდლოდ მიაწოდა პროდუქტები ან გაუწია მომსახურება.[30]

"DDG" მე-5 პარაგრაფის შესაბამისად, სერვისის მიმწოდებლის იდენტიფიკაციის ვალდებულებასთან დაკავშირებით, ვებსაიტის ოპერატორებმა უნდა უზრუნველყონ შემდეგი ინფორმაციის ხელმისაწვდომობა:

- სერვისის მიმწოდებლის სახელი და მისამართი, სადაც იგი არის რეგისტრირებული;
- იურიდიული პირების შემთხვევაში, იურიდიული ფორმა, წარმომადგენელი, ნებისმიერი აქციათა კაპიტალი;
- საკონტაქტო ინფორმაცია, ელ-ფოსტა, ტელეფონი და, თუ საჭიროა, ფაქსი.

გარდა ამისა, სერვისის მიმწოდებლებს შესაძლოა მოუწიოთ საზედამხედველო ორგანოებისთვისა და მეწარმეთა რეესტრებისთვის დამატებითი ინფორმაციის მიწოდება.

დაბოლოს, საჭიროა, რომ საიტზე განთავსებული ინფორმაცია ხელმისაწვდომი მაქსიმუმ ორი დაწკაპუნებით გახდეს.

---

[28] For more information see *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR) 14/2024, margin note 3.

[29] იხ.: *Oberlandesgericht Hamburg*, decision of 3 April 2007 - 3 W 64/07, margin note 7; *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR) 14/2024, margin note 3.

[30] იხ.: *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR) 14/2024, margin note 3.

6. დასკვნა

მომავალ წლებში ნათელი გახდება, შეძლო თუ არა ციფრული სერვისების აქტმა დასახული მიზნის განხორციელება, მათ შორის, მონაცემთა დაცვის კანონმდებლობის თვალსაზრისით, რაც 2027 წლის დასაწყისამდე შეფასდება. "DSA"-ს წარმატება დიდწილად დამოკიდებული იქნება იმაზე, თუ რამდენად კარგად გაანაწილებენ ევროკავშირის წევრი ქვეყნები პასუხისმგებლობას.

"DSA"-ს რევოლუციური განვითარება ციფრული სერვისების სფეროში[31] დიდწილად დამოკიდებული იქნება აღსრულებასა და სანქციების საკანონმდებლო მოწესრიგებაზე, რომელიც პრინციპში ევროკავშირის წევრ სახელმწიფოების[32] კომპეტენციას წარმოადგენს.

დაფუძნების ადგილის პრინციპის გამო, საზედამხედველო ორგანოს იურისდიქცია დამოკიდებულია შესაბამისი შუამავალი სერვისის დაფუძნების ადგილმდებარეობაზე. მაგალითად, "GDPR"-ის კონტექსტში ეს დეცენტრალიზებული პრინციპი მრავალი ექსპერტის მიერ კრიტიკის საგანი ხდება, რადგან სხვადასხვა ეროვნული ორგანოები ზოგჯერ მოქმედებენ სხვადასხვა სისწრაფითა და თანმიმდევრობით.

ტექნოლოგიების განვითარების გათვალისწინებით, ონლაინ პლატფორმები თანდათანობით შეიძენენ ძალას და დაასუსტებენ ისეთ სფეროებს, როგორებიცაა: მონაცემთა, კონკურენციისა და მომხმარებელთა დაცვა.

[31] The *Economist* of 15/12/2020, <https://www.economist.com/business/2020/12/15/the -eu-unveils-its-plan-to-rein-in-big-tech.html> [15.11.2024].
[32] იხ.: Recital No. 79 of the DSA.

ბიბლიოგრაფია:

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC, OJ 2022 L 277.
2. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (DMA) and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ 2022 L 265.
3. Regulation (EU) 2016/679 of the European Parliament and of 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 (GDPR), OJ 2016 L 119.
4. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a Procedure for the Provision of Information in the field of Technical Regulations and of the Rules of Information Society Services, OJ 2015 L 241.
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (E-Commerce Directive), OJ 2000 L 178.
6. *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
7. *Beck W.*, Der Entwurf des Digital Services Act – Hintergrund, Ziele und Grundsätze künftiger Regulierung des virtuellen Raums in der EU, Deutsches Verwaltungsblatt (DVBl) 2021, 1000.
8. *Brauneck J.,* Das Verantwortungsbewusstsein der Plattformbetreiber im Digital Services Act, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2024, 377.
9. *Brorsen H., Falk R.*, Neue Compliance-Pflichten nach dem Digital Services Act, Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 2024, 32.
10. *Buchheim J., Schrenk M.*, Der Vollzug des Digital Services Act, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2024, 1.
11. *Legner S.*, Der Digital Services Act – Ein neuer Grundstein der Digitalregulierung, Zeitschrift für Urheber- und Medienrecht (ZUM) 2024, 99.
12. *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR) 14/2024, margin note 3.
13. *Marx L.*, Der Digital Services Act der Europäischen Kommission, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR) 4/2021, margin note 2.
14. *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, 2022.

თომას ჰიორენი*
ფილიპ მაიერი**
გესა შენქე***

პრინციპი "POENA SINE CULPA" მონაცემთა დაცვის სამართალში და მისი მოქმედების ფარგლები

2023 წელს "Deutsche Wohnen"-ის საქმეზე წინასწარი გადაწყვეტილების მიღებისას, ევროკავშირის მართლმსაჯულების სასამართლომ ("ECJ") განმარტა: მაშინ როდესაც საზედამხედველო ორგანოები ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის" ("GDPR") 83-ე მუხლის საფუძველზე ჯარიმას აწესებენ, ვალდებულნი არიან დაამტკიცონ, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი „დამნაშავეა".[1] იმისდა მიხედვით, თუ როგორ განიმარტება გადაწყვეტილება, სასამართლომ უარყო ავტომატური პასუხისმგებლობის იდეა.[2] ამავდროულად, ბერლინის სააპელაციო სასამართლომ, რომელმაც აღნიშნული საქმე გადასაწყვეტად ევროკავშირის მართლმსაჯულების სასამართლოს გადასცა, გაითვალისწინა გადაწყვეტილება და 2024 წლის 22 იანვრის განკარგულებით ბერლინის რეგიონულ სასამართლოს დაუბრუნა განსახილველად, რომელსაც ჯარიმის კანონიერების შესახებ უნდა ემსჯელა. სააპელაციო სასამართლოს გადაწყვეტილება "ECJ"-ს მიერ დადგენილი პრინციპების გადახედვის საფუძველს წარმოადგენს, რათა გამოიყენოს განსხვავებული დასაბუთება.

ბრალი, როგორც წინაპირობა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის" 83-ე

---

* პროფესორი, სამართლის დოქტორი, მიუნსტერის უნივერსიტეტის ინფორმაციის, ტელეკომუნიკაციებისა და მედია სამართლის ინსტიტუტის დირექტორი.
** მიუნსტერის უნივერსიტეტის ასისტენტ-მკვლევარი და დოქტორანტი.
*** საერთაშორისო იურიდიული ფირმის ასისტენტ-მკვლევარი.

[1] ECJ NJW 2024, 343 para. 68.

[2] *Brink S., Wybitul T.,* ZD 2024, 137 (142); *Korte K.,* ZD-Aktuell 2024, 01500; <https://www.lto.de/recht/hintergruende/h/eugh-c80721-deutsche-wohnen-dsgvo-bussgeld-erfolg-datenschutz-beauftragte-kartellrecht> [1.03.2024].

მუხლის მეთოდოლოგიურ, სწორ ინტერპრეტაციაზე დაყრდნობით წარმოიშვა, ასევე, "GDPR"-ის ზოგადი სისტემისა და მიზნის. შესაბამისად, მეორეული სამართლებრივი წყაროებიდან გამომდინარე დამტკიცდა.

სტატია მიმოიხილავს ბრალის პრინციპის ("culpability principle") მოქმედებას ევროკავშირის სამართალში და ადამიანის უფლებათა ევროპული სასამართლოს ("ECtHR") პრაქტიკას პრინციპთან „არ არსებობს სასჯელი დანაშაულის გარეშე" ("nulla poena sine culpa") დაკავშირებით.

საკვანძო სიტყვები: *ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია" ("GDPR"), საქმე "Deutsche Wohnen", ევროკავშირის მართლმსაჯულების სასამართლო, საზედამხედველო ორგანოები, ადმინისტრაციული ჯარიმა, „არ არსებობს სასჯელი დანაშაულის გარეშე", უდანაშაულობის პრეზუმფცია, ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია (ECHR).*

1. დანაშაულის პრინციპი ევროპის პირველად სამართალში

პრინციპის **"**nulla poena sine culpa" მიხედვით, სასჯელის დაკისრებისთვის ბრალეული ქმედებით დანაშაულის ჩადენა მთავარ წინაპირობას წარმოადგენს.[3] დანაშაული, როგორც განზრახი ან დაუდევარი ქმედება, დასაბუთების ფუნქციას ასრულებს სასჯელის დაკისრებისას და სისხლისსამართლებრივი სანქციის დაკისრების ლეგიტიმაციის საფუძველია (ბრალი, როგორც სასჯელის დასაბუთება).[4] ამავე დროს, სასჯელი შემოიფარგლება დანაშაულით, რაც იმას ნიშნავს, რომ სასჯელმა არ უნდა გადააჭარბოს დანაშაულით დადგენილ დონეს (ე.წ. "penalty assessment guilt").[5] ბრალის არსებობის ფუნქციას სასჯელის დასაბუთება და შეზღუდვა წარმოადგენს.[6] ბრალის დაკავშირება პირის მართვად ქმედებებთან

[3] BVerfGE 95, 96, 131 = NJW 1997, 929 (930); BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289); *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R.,* Europäisches Strafrecht, 2nd ed. 2014, § 55 para. 60. S*chönke A., Schröder H., Eisele J*., StGB, 30th ed. 2019, Vor. §§ 13 ff. para. 103; *Adam T., Schmidt F., Schumacher L.,* NStZ 2017, 7.

[4] BVerfGE 109, 133, 174 = NJW 2004, 739 (746); BVerfGE 128, 326, 376 = NJW 2011, 1931 (1938); *Roxin C., Greco L.,* Strafrecht AT I, 2020, § 19 para. 54.

[5] BVerfGE 95, 96, 140 = NJW 1997, 929 (932); *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R.,* Europäisches Strafrecht, 2nd ed. 2014, § 55 para. 60; *Roxin C., Greco L*., Strafrecht AT I, 2020, § 19 para. 9, 62.

[6] Cf*. Keil G.,* Willensfreiheit, 2nd ed. 2013, 157; *Globke*, in: *Brunhöber W., Höffler B., Kaspar F., Reinbacher R., Vormbaum M.* (eds.), Strafrecht und Verfassung, 2012, 67; *Engelhart H*., NZWiSt 2015, 201 (203); similarly *Satzger H*., ZRP 2010, 137 (139).; *Hörnle J.,* JZ 1999, 1080 (1088), მნიშვნელოვანია

გამოხატავს სახელმწიფოს მიერ ადამიანის ღირსების მიმართ პატივისცემას, რათა შეზღუდოს პირის სახელმწიფო კონტროლის ობიექტად გადაქცევა.[7] ამ მიზეზით, ფედერალური საკონსტიტუციო სასამართლო ბრალის პრინციპის ("principle of guilt") კონსტიტუციურ საფუძვლად კონსტიტუციის პირველი მუხლის პირველი პუნქტში გაწერილ ადამიანის ღირსების უფლებას მიიჩნევს, ასევე, ძირითადი კანონის მეორე მუხლის მე-2 პუნქტით განმტკიცებულ მოქმედების თავისუფლების ზოგად პრინციპსა და სამართლებრივი სახელმწიფოს პრინციპს (ძირითადი კანონის 20(3) მუხლი). აღნიშნული პრინციპები, ძირითადი კანონის 79(3) მუხლის შესაბამისად[8], სისხლის სამართლის ევროპეიზაციის საზღვრებს განსაზღვრავს.[9] ევროკავშირის საკონსტიტუციო სამართალში ბრალის პრინციპის დოგმატური საფუძველი, შინაარსი და ფარგლები შედარებით ბუნდოვანია.[10] აღსანიშნავია, რომ პრინციპი "*nulla poena sine culpa"* არც ადამიანის უფლებათა ევროპულ კონვენციაში ("ECHR") და არც ძირითად უფლებათა ქარტიაში ("CFR") არ არის პირდაპირ განსაზღვრული, თუმცა მისი აღიარების საკითხი ეჭვგარეშეა.[11] ევროკავშირის მართლმსაჯულების სასამართლო პრინციპს "*nulla poena sine culpa"* მხოლოდ ირიბად ითვალისწინებს, როდესაც საქმე ეხება ზოგადი პროპორციულობის ტესტს.[12] ამის საპირწონედ, ევროკომისიამ, ევროსაბჭომ და ევროპარლამენტმა აღიარა ბრალის პრინციპი.[13] გენერალური ადვოკატი, კოკოტი, ასევე, მიიჩნევს, რომ პრინციპი „არ არსებობს სასჯელი დანაშაულის გარეშე" აღიარებულია, როგორც ძირითად უფლებათა ქარტიის 48(1) მუხლით, ისე ადამიანის უფლებათა ევროპული კონვენციის ("ECHR") 6(2) მუხლით. იგი ხედავს ორივე ნორმას, როგორც პრინციპის პროცედურულ გამოხატულებებს.[14]

სისხლისსამართლებრივი პასუხისმგებლობისა და სისხლისსამართლებრივი დასაბუთების პასუხისმგებლობის განსხვავებისთვის.

[7] BVerfGE 30, 1, 41 = NJW 1971, 275 (282); on the object formula *Scholz* R., *Dürig* G., *Herzog* R., *Herdegen* M., GG (Vol. I), Art. 1 para. 36.

[8] BVerfGE 123, 267, 344 = NJW 2009, 2267 (2270).

[9] BVerfGE 123, 267, 348 = NJW 2009, 2267 (2271); see *Adam T., Schmidt F.*, *Schumacher L.*, NStZ 2017, 7 (8).

[10] *Böse M., Stuckenberg C.*, Europäisches Strafrecht (EnzEuR Bd. 11), 2nd ed. 2021, § 10 para. 17; *Globke* R., in: *Brunhöber B.*, *Höffler H., Kaspar J., Reinbacher T., Vormbaum M.* (eds.), Strafrecht und Verfassung, 2012, 66 f.; *Vogel J.*, JZ 1995, 331 (337).

[11] *Grabitz E., Hilf M., Nettesheim M., Vogel P., Eisele J., Das Recht der Europäischen Union, 80th ed. 2023, Art. 83 TFEU, para. 46; Sieber U., Satzger H., von Heintschel-Heinegg F., Killmann A.,* Europäisches Strafrecht, 2nd ed. 2014, § 11 para. 18; *Hochmayr G.,* ZIS 2016, 226 (230); *Fromm E.*, ZIS 2007, 279 (287); *Tiedemann K.,* NJW 1993, 23 (28).

[12] ECJ judgement of. 16.11.1983, Case 188/82, ECR 1983, 3721 para. 18 - *Thyssen*; ECJ judgement of 18.11.1987, Case 137/85, ECR 1987, 4587 para. 14 - *Maizena*; ECJ judgement of 11 July 2002, Case C-210/00, ECR 2002 I-6453 para. 44 - *Käserei Champignon Hofmeister*.

[13] See COM(2011) 573 final, 10; Council Doc. 16542/2/09 REV 2 No. 6-8; European Parliament resolution of 22 May 2012 on the EU approach to criminal law (2010/2310(INI)), C 264 E/9.

[14] Opinion GA Juliane Kokott, 28 February 2013, Case C-681/11, EU:C:2013:126, para. 41; იხ.: Opinion GA Carl Otto Lenz, 11 July 1992, Case C-143/91, EU:C:1990:381.

1.1. ადამიანის ძირითად უფლებათა ქარტიის (“CFR”) პირველი მუხლით დაცული ღირსების უფლება

ფედერალური საკონსტიტუციო სასამართლოს პრეცედენტული სამართალი ბრალის პრინციპის შესახებ გამოთქვამს ვარაუდს, რომ იგი უნდა იყოს გამყარებული პირველადი კანონმდებლობით, რომელიც მოცემულია ევროკავშირის ადამიანის ძირითად უფლებათა ქარტიის (“CFR“) პირველ მუხლში. საკონსტიტუციო სამართლის მიხედვით, ქარტიის პირველი მუხლი ადამიანის სოციალური ღირებულებისა და პატივისცემის დაცვის გარანტიას იძლევა.[15] ამრიგად, სახელმწიფოს თითოეული ქმედება, რომელიც არღვევს ადამიანის, როგორც სუბიექტის სტატუსს, წარმოადგენს არსებით ჩარევას უფლებაში და ლახავს მის ღირსებას.[16] სისხლის სამართლისა და კვაზი სისხლის სამართლის პროცესში ბრალდებულის ღირსებასთან კოლიზია ნებისმიერ შემთხვევაში წარმოიქმნება, თუ ბრალდებულის ქმედება სახელმწიფოს მხრიდან სოციალური ეთიკის თვალსაზრისით არ არის მისაღები.[17] ამის საპირისპიროდ, ბრალის დადგენა და დანაშაულის დასადგენად განხორციელებული ღონისძიებები არ ლახავს ადამიანის ღირსებას.[18] საინტერესოა, რომ ფედერალური საკონსტიტუციო სასამართლოს პრაქტიკის მიხედვით, დანაშაულის პრინციპი გამომდინარეობს გერმანიის ფედერალური კონსტიტუციით განმტკიცებული სამართლებრივი სახელმწიფოს, კანონის უზენაესობის პრინციპებიდან და არა მხოლოდ ადამიანის ღირსებიდან.[19] ბრალის პრინციპი, შესაბამისად, პირდაპირი გაგებით, არ ეფუძნება ადამიანის ღირსების უფლებას, რომელიც განმტკიცებულია გერმანიის ფედერალური კონსტიტუციის პირველი მუხლით.[20]

1.2. უდანაშაულობის პრეზუმფცია (ქარტიის 48-ე მუხლის პირველი პუნქტი; კონვენციის მე-6 მუხლის მე-2 პუნქტი)

ევროკავშირის ძირითად უფლებათა 48-ე მუხლის პირველი პუნქტი სისხლის სამართალში პროცედურულ გარანტიას ქმნის და იზიარებს ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის მე-6 მუხლის მე-2 პუნქტის შინაარსს.[21] ორივე დებულება

[15] *Jarass H. D.,* GRC, 4th ed. 2021, Art. 1 GRC para. 6, 7.
[16] *Jarass H. D.,* GRC, 4th ed. 2021, Art. 1 GRC para. 8.
[17] *Globke* R., in: *Brunhöber B., Höffler K., Kaspar J., Reinbacher T., Vormbaum M.,* (eds.), Strafrecht und Verfassung, 2012, 59; *Frister H.,* Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 25.
[18] *Rabe P.,* Das Verständigungsurteil des Bundesverfassungsgerichts und die Notwendigkeit von Reformen im Strafprozess, 2017, 147; *Frister H*., Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 25.
[19] The so-called Lisbon judgement BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289) is an exception.
[20] See *Schaut A. B*., Europäische Strafrechtsprinzipien, 2012, 228; *Vogel P*., JZ 1995, 331 (339); See also *Böse M., Satzger H.,* Europäisches Strafrecht (EnzEuR Bd. 9), 1st ed. 2013, § 2 para. 59.
[21] Explanations on the Charter of Fundamental Rights, OJ 2007 No. C 303/17, 30.

ამკვიდრებს უდანაშაულობის პრეზუმფციას, რომლის მიხედვითაც, სისხლის სამართლის პროცესებში, ბრალდებული უდანაშაულოდ ითვლება, მანამ სანამ საწინააღმდეგო არ დამტკიცდება.[22] უდანაშაულობის პრეზუმფცია ვრცელდება არა მხოლოდ ევროკავშირის მოქალაქეებზე, არამედ ის წარმოადგენს უფლებას, რომელიც შეიძლება გავრცელდეს იურიდიულ პირებზეც.[23] "GDPR"-ის 51(1) მუხლის თანახმად, ევროკავშირის თითოეული ორგანო, ორგანიზაცია და ინსტიტუტი ვალდებულია დაიცვას აღნიშნული პრინციპი და ხელი შეუწყონ კანონმდებლობაში მის ჯეროვან იმპლემენტაციას.[24] უდანაშაულობის პრეზუმფცია, ამდენად, ერთგვარად ზღუდავს სასჯელის დაკისრების შესაძლებლობას ბრალის დამტკიცების გარეშე.[25] უდანაშაულობის პრეზუმფციიდან გამომდინარე, ეჭვის საფუძველზე სასჯელის აკრძალვა წარმოადგენს ბრალის ფუნქციას, როგორც სასჯელის გამორიცხვის წინაპირობა.[26] ამდენად, ბრალის პრინციპი ირიბად უდანაშაულობის პრინციპის ნაწილია, რომელიც აღიარებულია ევროკავშირის ძირითად უფლებათა ქარტიის 48-ე მუხლის პირველი პუნქტითა და კონვენციის მე-6 მუხლის მე-2 პუნქტით.[27]

1.3. პროპორციულობის პრინციპი (ქარტიის 49-ე მუხლის მე-3 პუნქტი)

ევროკავშირის ძირითად უფლებათა ქარტიის 49-ე მუხლის მე-3 პუნქტი ამკვიდრებს პროპორციულობის პრინციპის სტანდარტს ევროკავშირის სამართალში სისხლისსამართლებრივი და ადმინისტრაციული სანქციებისთვის. პრინციპის მიზანია სასამართლოებისა და ადმინისტრაციული ორგანოების მიერ დაწესებული ჯარიმები პროპორციულობის უზრუნველყოფა.[28] სხვა სიტყვებით რომ ითქვას, ჯარიმები და სანქციები უნდა იყოს შესაბამისი, აუცილებელი და პროპორციული ჩადენილი დანაშაულის. დაწესებული ჯარიმა არ დააკმაყოფილებს პროპორციულობის კრიტერიუმს, თუ დანაშაულისა და ბრალის შესაბამისი არ არის. კონკრეტულ შემთხვევაში გათვალისწინებული უნდა იყოს, როგორც

[22] *Calliess C., Ruffert M., Blanke H., EUV/AEUV, 6th ed. 2022, Art. 48 CFR para. 1, 4; Meyer J., Hölscheidt S., Eser A., Kubiciel M., CFR, 5th ed. 2019, Art. 48 CFR para. 1.*

[23] *Calliess C., Ruffert M., Blanke H., EUV/AEUV*, 6th ed. 2022, Art. 48 CFR para. *2; Jarass H. D., CFR,* 4th ed. 2021, Art. 48 para. 12.

[24] *Meyer J., Hölscheidt S., Eser A., Kubiciel M.,* GRC, 5th ed. 2019, Art. 48 GRC para. 13; *Calliess* C., *Ruffert* M., *Blanke* H., EUV/AEUV, 6th ed. 2022, Art. 48 GRC para. 4.

[25] *Meyer J., Hölscheidt S., Eser A., Kubiciel M.*, GRC, 5th ed. 2019, Art. 48 GRC para. 6, 7; *Calliess* C., *Ruffert* M., *Blanke* H., EUV/AEUV, 6th ed. 2022, Art. 48 GRC para. 4.

[26] *Meyer J., Hölscheidt S., Eser A., Kubiciel M*., GRC, 5th ed. 2019, Art. 48 GRC para. 10.

[27] Cf. *Frister H.,* Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 89; *Engels H.,* Unternehmensvorsatz und Unternehmensfahrlässigkeit im Europäischen Kartellrecht, 2002, 71; *Böse M., Satzger C.,* Europäisches Strafrecht (EnzEuR vol. 9), 1st ed. 2013, § 2 para. 59; differentiated *Klaas A., Momsen C., Wybitul T*., 71; *Böse M., Satzger C.,* Europäisches Strafrecht (EnzEuR Bd. 9), 1st ed. 2013, § 2 para. 59; differentiated *Klaas A., Momsen C., Wybitul T., Cornelius K., Datenschutzsanktionenrecht*, 1st ed. 2023, § 2 para. 22.

[28] *Jarass H.D.,* GRC, 4th ed. 2021, Art. 49 GRC para. 17; *Pechstein M., Nowak R., Häde U., Schröder R.*, Frankfurter Kommentar EUV/AEUV/GRC, 2nd ed. 2023, Art. 49 para. 20.

დანაშაულის სიმძიმე, ისე სანქციის სიმკაცრე.[29] დანაშაულისა და სასჯელის პროპორციულობის პრინციპს, რომელიც განმტკიცებულია ქარტიის 49-ე მუხლის მე-3 პუნქტით აქვს სასჯელის შეზღუდვის ფუნქცია.[30] აღნიშნული ფუნქცია, ასევე, ბრალის პრინციპის ძირითადი ელემენტიც არის. ამ მხრივ, ბრალის პრინციპი ნაგულისხმევია 49-ე მუხლის მე-3 პუნქტშიც.[31]

1.4. შუალედური შედეგი

საბოლოო ჯამში, უნდა აღინიშნოს, რომ ბრალის პრინციპი (უდანაშაულობის პრეზუმფცია) ევროკავშირის ძირითად უფლებათა ქარტიის 48(1) მუხლით, ასევე, ადამიანის უფლებათა ევროპული კონვენციის 6(2) მუხლით არის განმტკიცებული.

2. ბრალის წარმოშობა გადაწყვეტილებაში "Deutsche Wohnen"

წინასწარ გადაწყვეტილებაზე მსჯელობისას, ევროკავშირის მართლმსაჯულების სასამართლოს ("ECJ") უნდა განეხილა საკითხი, მოითხოვს თუ არა "GDPR"-ის 83-ე მუხლი ბრალის (განზრახვით ან გაუფრთხილებლობით ჩადენილი დარღვევის) დამტკიცებას - იმ ფაქტის დადგენას, სადაც დამუშავებისთვის პასუხისმგებელმა პირმა, როგორც იურიდიულმა პირმა, განზრახ ან გაუფრთხილებლობით დაარღვია 83-ე მუხლის მე-4 და მე-6 პუნქტები.[32] მეორე საკითხთან დაკავშირებით, ევროკავშირის მართლმსაჯულების სასამართლომ, პირველ რიგში, დაადგინა, რომ "GDPR"-ის 83-ე მუხლი პირდაპირ არ ითვალისწინებს ჯარიმის დაკისრებას რეგულაციის გაუფრთხილებლობით ან ბრალეული დარღვევისას. ამის ნაცვლად, სასამართლო მიუთითებს 83(2) მუხლის მე-2 პუნქტის (ბ) ქვეპუნქტზე, რომლის მიხედვითაც, დარღვევის განზრახ ან გაუფრთხილებლობით ჩადენის ფაქტორი სათანადოდ უნდა იქნას გათვალისწინებული ჯარიმის დაკისრებისას.[33] "GDPR"-ის 83(2) მუხლის მე-2 პუნქტში აღნიშნული სხვა არცერთი კრიტერიუმი მიუთითებს იმაზე, რომ დამუშავებისთვის პასუხისმგებელი პირი ბრალის მიუხედავად არის პასუხისმგებელი.[34] უფრო მეტიც, "GDPR"-ის 83(3) მუხლი, ასევე, მიუთითებს მკაცრი პასუხისმგებლობის შესახებ, რომლის მიხედვითაც საჭიროა დამუშავებისთვის პასუხისმგებელი პირის მიერ ნორმის ბრალეული დარღვევა.[35] "GDPR"-ის 83-ე მუხლის ფორმულირება თანხვედრაშია

[29] *Jarass H.D.,* GRC, 4th ed. 2021, Art. 49 GRC para. 19; *Pechstein M., Nowak R., Häde U., Schröder R.,* Frankfurter Kommentar EUV/AEUV/GRC, 2nd ed. 2023, Art. 49 para. 20.
[30] *Meyer J., Hölscheidt S., Eser A., Kubiciel M.,* GRC, 5th ed. 2019, Art. 49 GRC para. 38.
[31] *Klaas A., Momsen C., Wybitul T., Cornelius K.,* Datenschutzsanktionenrecht, 1st ed. 2023, § 2 para. 36; Kaufmann, JURA 1986, 225 (227); *Schaut A.*, Europäische Strafrechtsprinzipien, 2012, 228.
[32] ECJ, NJW 2024, 343 para. 61.
[33] ECJ, NJW 2024, 343 para. 62.
[34] ECJ, NJW 2024, 343 para. 66.
[35] ECJ, NJW 2024, 343 para. 67.

რეგულაციის ზოგად მიზნებთან და სტრუქტურასთან. აღნიშნული დამუშავებისთვის პასუხისმგებელ პირებს ანიჭებს დისკრეციას ჯარიმის განსაზღვრისას ძირითადი რეგულაციის 58(2)(i) მუხლის მიხედვით, ამგვარად იქმნება სანქციების დიფერენცირებული სისტემა.[36] ევროკავშირის კანონმდებელმა განზრახ უარყო ბრალის გარეშე პასუხისმგებლობის საკითხი.[37] შედეგად, სასამართლოს შეფასებით, როგორც "GDPR"-ის 83-ე მუხლის ფორმულირება, ასევე, ძირითადი რეგულაციის სისტემა და მიზანი იზიარებს ბრალის ელემენტის საკითხს, რომელიც აუცილებელია ჯარიმის დაკისრებისას.

3. "GDPR"-ის ჯარიმები, როგორც სისხლის სამართლის ნაწილი

მიუხედავად იმისა, რომ ევროკავშირის მართლმსაჯულების სასამართლოს ("ECJ") ევროკავშირის სანქციების სისტემაში "GDPR"-ით განსაზღვრული ჯარიმების კლასიფიცირება არ მოუხდენია, სანქციის დაკისრებისას ბრალის დამტკიცების კომპონენტი მაინც აუცილებელია, რითაც არაპირდაპირ დასტურდება ბრალის პრინციპის მოქმედება. თუმცა ჩნდება კითხვა: გამომდინარეობს თუ არა დასკვნა, რომ "GDPR"-ით განსაზღვრული ჯარიმები, მათი სამართლებრივი ბუნებით, შეიძლება ფართო გაგებით სისხლის სამართალს განეკუთვნებოდეს?[38] აღნიშნული საკითხის გამოსაკვლევად, აუცილებელია სისხლისსამართლებრივი სანქციების ზოგადი მოთხოვნების შესწავლა და შემდგომ მათი განხილვა მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ ჯარიმებთან მიმართებით.

3.1. ენგელის კრიტერიუმი ("Engel Criteria")

ევროკავშირის მართლმსაჯულების სასამართლოს ("ECJ") მიერ დადგენილი პრაქტიკის თანახმად, სამართალდარღვევისა და სანქციის ხასიათს სამი ძირითადი ფაქტორი განსაზღვრავს: (1) როგორ კვალიფიცირდება დანაშაული ეროვნულ ან ევროკავშირის კანონმდებლობით, (2) დანაშაულის ბუნება და (3) დაწესებული სანქციის სიმკაცრე.[39] აღნიშნულთან მიმართებით ევროკავშირის მართლმსაჯულების სასამართლო ("ECJ") იყენებს ადამიანის უფლებათა ევროპული სასამართლოს ("ECtHR") მიერ დადგენილ ე.წ ენგელის პრაქტიკას, რომელიც განსაზღვრავს

[36] ECJ, NJW 2024, 343 para. 70, 73.
[37] ECJ, NJW 2024, 343 para. 74.
[38] Similarly, *Hochmayr G.*, ZIS 2016, 226.
[39] ECJ, BeckRS 2012, 81043 para. 37 - Bonda; ECJ, BeckRS 2018, 6055 para. 26 f. - Menci Luca; ECJ, BeckRS 2022, 5011 para. 25 - bpost; *Gassner K., Seith S.,* Ordnungswidrigkeitengesetz, 2nd ed. 2020, Introduction para. 6.

სისხლისსამართლებრივი დევნის კონცეფციას.[40] ლიტერატურაში ენგელის სახელით ცნობილი კრიტერიუმები ერთმანეთისგან დამოუკიდებელია.[41]

ა) კანონმდებლის ნება

პირველი კრიტერიუმის თანახმად, აუცილებელია შეფასდეს სახელმწიფოს შიდა კანონმდებლობის მიზნები და უნდა დადგინდეს კონკრეტული სანქცია და ზომები განეკუთვნება ადმინისტრაციულ თუ სისხლის სამართალს[42]. შიდასახელმწიფოებრივ დონეზე მიღებული გადაწყვეტილება საკმარისია, თუმცა არა სავალდებულო პირობა,[43] რადგან წინააღმდეგ შემთხვევაში, კატეგორიზაცია დამოკიდებული იქნებოდა წევრი ქვეყნების ან ხელშემკვრელი სახელმწიფოების თავისუფალ ნებაზე.[44]

ბ) დანაშაულის ბუნება

შემდგომ ეტაპზე უნდა შეფასდეს დანაშაულის ტიპი (დანაშაულის ბუნება) - არის თუ არა გამოყენებული სანქცია რეპრესიული ხასიათის[45] აღნიშნულის თანახმად, სისხლისსამართლებრივი სანქცია თავისი ბუნებით შეიძლება იყოს როგორც პრევენციული, ისე რეპრესიული.[46] გარდა ამისა, სისხლისსამართლებრივი სანქციის დამახასიათებელი თვისებად,[47] ასევე, მიიჩნევა მნიშვნელოვანი საზოგადოებრივი ინტერესის დაცვა.[48]

გ) სასჯელის სიმძიმე

სანქციების სიმძიმის მიხედვით, ერთმანეთისგან უნდა განვასხვაოთ ჯარიმა და თავისუფლების აღკვეთა. მიუხედავად იმისა, რომ თავისუფლების აღკვეთა უმეტესწილად სისხლის სამართლის სასჯელს წარმოადგენს, ჯარიმა და თავისუფლების შემზღუდველი სხვა ზომები უნდა შეფასდეს ინდივიდუალურად, შედეგების სიმძიმის მიხედვით.[49] სასჯელის სიმძიმის

[40] ECtHR, EuGRZ 1976, 221 - Engel et al. v Netherlands; ECtHR, BeckRS 2010, 21072 para. 53 - Zolotoukhine v Russia; ECJ, NJW 2024, 33, para. 45 - Volkswagen Italia SpA; *Grabenwarter C., Pabel K.*, ECHR, 6th ed. 2016, § 24 para. 19; critical *Wegner*, NZWiSt 2023, 401.

[41] მეორე და მესამე კრიტერიუმები კუმულაციურად გამოიყენება მხოლოდ იმ შემთხვევაში, თუ ცალკეული კრიტერიუმების გათვალისწინება არ იძლევა ნათელ შედეგს; *Meyer-Ladewig J., Nettesheim M., von Raumer S., Harrendorf H., König P., Voigt T.,* ECHR, 5th ed. 2023, ECHR Art. 6 para. 23.

[42] ECJ, BeckRS 2023, 8994 para. 40.

[43] ECJ, BeckRS 2022, 5011 para. 26; *Karpenstein U., Mayer F.C.,* ECHR, 3rd ed. 2022, Art. 6 para. 25.

[44] *Barrot W.,* ZJS 2010, 701, 702; *Gerhold S.*, 41st ed., Introduction to the OWiG para. 5.

[45] ECJ, BeckRS 2018, 6055 para. 31.

[46] ECJ, BeckRS 2023, 8994 para. 42; ECJ, BeckRS 2023, 24054 para. 49; *Grabenwarter C., Pabel K.*, ECHR, 6th ed. 2016, § 24 para. 21.

[47] *Dörr C., Grote H., Marauhn T.,* ECHR/GG, 3rd ed. 2022, ch. 14 para. 26; *Grabenwarter C., Pabel K.,* ECHR, 6th ed. 2016, § 24 para. 21.

[48] *Karpenstein U., Mayer F.C.,* ECHR, 3rd ed. 2022, Art. 6 para. 26.

[49] ECtHR, BeckRS 2010, 2107253 - Zolotoukhine v Russia; *Dörr C., Grote H., Marauhn T.*, ECHR/GG, 3rd ed. 2022, ch. 14 para. 26; *Barrot W.,* ZJS 2010, 701 (702).

ხარისხი ვლინდება კანონით გათვალისწინებული სასჯელის განსაზღვრისას.[50]

3.2. "GDPR"-ის 58-ე მუხლის მე-2 პუნქტის „ი" ქვეპუნქტი და 83-ე მუხლის მე-4 - მე-6 პუნქტები ენგელის კრიტერიუმების ჭრილში

მნიშვნელოვანია, დადგინდეს ენგელის კრიტერიუმების მიხედვით, წარმოადგენს თუ არა "GDPR"-ის 83-ე მუხლით გათვალისწინებული დარღვევა ფართო გაგებით სისხლის სამართლის დანაშაულს და გამომდინარეობს თუ არა, ბრალის არსებობის მოთხოვნის აუცილებლობა ევროკავშირის სამართალში.[51]

ა) კანონმდებლის ნება

ზემოაღნიშნულის გათვალისწინებით, განვიხილოთ ენგელის პირველი კრიტერიუმი, რომლის მიხედვით, ბრიუსელის სუპრანაციონალური კანონმდებლის ნების შესწავლა უნდა მოხდეს, თუ რა სამართლებრივ ბუნებას მიაკუთვნებს იგი მონაცემთა დაცვის სამართლის ჯარიმებს.[52] "GDPR"-ის 58-ე მუხლის მე-2(i) პუნქტის და 83-ე მუხლის მე-4 - მე-6 პუნქტების დებულებების ცალსახად სისხლის სამართლის კანონმდებლობისთვის მიკუთვნება შეუძლებელია, თუმცა ევროპულ ანტიმონოპოლიურ კანონმდებლობაში სხვაგვარი ვითარებაა. რეგულაციის ("Cart Regulation") 23-ე მუხლის მე-5 პუნქტის მიხედვით, 23-ე მუხლის პირველი და მე-2 პუნქტების დარღვევისთვის კომპანიებისთვის დაწესებული ჯარიმები არ განიხილება სისხლისსამართლებრივ დანაშაულად.[53] საკანონმდებლო პრაქტიკაში, ანტიმონოპოლიური ჯარიმები წარმოადგენს სანქციის მექანიზმს სამართლის სხვა სფეროებისთვის, რომლებიც ევროკავშირის კანონმდებლობით არის განსაზღვრული.[54] ანტიმონოპოლიურ სამართალსა ("antitrust law") და მონაცემთა დაცვის სამართალში დაკისრებულ ჯარიმებს შორის გარკვეული მსგავსებები არსებობს, რაც ცალსახად იკვეთება ძირითადი რეგულაციის პრეამბულის 150-ე პუნქტში. შესაბამისად, როდესაც ჯარიმა ეკისრება დამუშავებისთვის პასუხისმგებელ იმ პირებს, რომლებიც ამავდროულად კომპანიებიც არიან; სამართლებრივი შედეგების განსაზღვრისთვის საწარმოს ფუნქციური კონცეფცია მხედველობაში უნდა იქნეს მიღებული ("TFEU"-ის 101-

[50] სანქცია 500 ევროს ოდენობით არ არის საკმარისი; ECtHR, BeckRS 2010, 21072; ECJ, BeckRS 2023, 8994 para. 46; ECJ, BeckRS 2023, 24054 para. 53; *Grabenwarter C., Pabel K.,* ECHR, 6th ed. 2016, § 24 para. 22; *Jarass H.*, GRC, 4th ed. 2021, Art. 48 GRC para. 9.

[51] ECJ, NJW 2024, 343 para. 75, 78 - Deutsche Wohnen.

[52] *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P*., ECHR, 5th ed. 2023, ECHR Art. 6 para. 24.

[53] *Bechtold R., Bosch N., Brinker I., Bechtold R.,* EU-Kartellrecht, 4th ed. 2023, Regulation (EC) 1/2003, Art. 23 para. 91.

[54] *Ackermann T.,* ZEuP 2023, 529 (555 et seq.) ანტიმონოპოლიური კანონმდებლობით „ფუნქციური კონცეფციის" სამართლის სხვა სფეროებში გადატანის შესახებ; see also *Zelger F.,* EuR 2021, 478 (481 et seq.).

ე და 102-ე მუხლები). ამ მიდგომის თანახმად, ჯარიმის ოდენობა უნდა განისაზღვროს კომპანიის წინა წლის ბრუნვის საფუძველზე.[55] ამ აშკარა მსგავსების გათვალისწინებით, რომლებიც ანტიმონოპოლიურ სამართალში არსებულ ჯარიმებთან არსებობს, სავარაუდოა, რომ კანონმდებელი "GDPR"-ის მიღებისას ანალოგიურ მიდგომას იზიარებდა, ("GDPR"-ის 23(5) მუხლის მსგავსს), ამდენად, მონაცემთა დაცვის სამართლის ფარგლებში დაკისრებული ჯარიმები არც მან მიაკუთვნა სისხლის სამართალს.

წინამდებარე განმარტება შესაბამისობაშია ძირითად რეგულაციაში არსებულ მცირე მითითებებთან ჯარიმების სამართლებრივი ბუნების თაობაზე. მაგალითად, "GDPR"-ის 84-ე მუხლის პირველი პუნქტი და პრეამბულის 149-ე პუნქტი. ძირითადი რეგულაციის პრეამბულის 149-ე პუნქტი განსაზღვრავს, რომ წევრ სახელმწიფოებს უნდა შეეძლოთ წესების დადგენა, რომლებიც განსაზღვრავს სისხლის სამართლის პასუხისმგებლობას ძირითადი რეგულაციის დარღვევისთვის, განსაკუთრებით იმ შემთხვევაში, თუ აღნიშნულს არ ითვალისწინებს "GDPR"-ის 83-ე მუხლი. ეს დანაწესი გამოიყენა გერმანელმა კანონმდებლებმა და ნებაყოფლობით აისახა გერმანიის მონაცემთა დაცვის ფედერალურ აქტის 42-ე მუხლში.[56] თუ მონაცემთა დაცვის კანონმდებლობა სისხლისსამართლებრივ სანქციებს "GDPR"-ის 83-ე მუხლისგან დამოუკიდებლად მოიცავს, ეს ნიშნავს, რომ ევროპელი კანონმდებელი მონაცემთა დაცვის ჯარიმებს განსხვავებულად ("aliud") განიხილავს და მათ მხოლოდ ადმინისტრაციულ სანქციებად მოიაზრებს.[57] შესაბამისად, "GDPR"-ის პრეამბულის 150-ე და 152-ე პუნქტები ადმინისტრაციულ სანქციებს არასისხლისსამართლებრივ სანქციებად მიიჩნევს.[58] აღნიშნული დასკვნა შეესაბამება კანონშემოქმედებით პროცესს, რომლის მიხედვითაც "GDPR"-ი ეფუძნება მხოლოდ მე-16 მუხლის მე-2 პუნქტს და, შესაბამისად, სისხლის სამართლის გავრცელების საფუძველი არ არსებობს. ასეთი საფუძველი ევროკავშირის კანონმდებლობაში მხოლოდ ფინანსური სანქციებისთვის არსებობს ("TFEU"-ის 325(4) მუხლი).[59] შედეგად, შეიძლება ვივარაუდოთ, რომ ევროპელმა კანონმდებელმა მხოლოდ ადმინისტრაციული სანქციების დაწესება განიზრახა "GDPR"-ის 58-ე მუხლის 2-ე პუნქტის "i" და 83-ე მუხლების საფუძველზე.[60] ზემოაღნიშნულიდან გამომდინარე, ენგელის პირველი კრიტერიუმის მიხედვით, კანონმდებელს არ აქვს უფლება გადაწყვიტოს გამოიყენოს თუ არა საერთაშორისო და

[55] სასამართლომ ცხადყო, რომ ანტიმონოპოლიური კანონმდებლობის მიხედვით „ფუნქციონალური" პრინციპი არ არის რელევანტური პასუხისმგებლობის არსებითი დადგენის დონეზე. პირიქით, ანტიმონოპოლიური კანონმდებლობის მიხედვით ვალდებულების ცნება გამოიყენება მხოლოდ სამართლებრივი შედეგების დადგენისთვის; ECJ, NJW 2024, 343 para. 53, 57 - Deutsche Wohnen; see also LG Bonn, MMR 2021, 173 para. 30 on the use of the concept of an undertaking to establish liability.

[56] *Parigger M., Helm T., Stevens-Bartol E., Müller R.,* Labour and Social Criminal Law, 1st ed. 2021, Section 42 BDSG para. 1.

[57] See *Bülte J.*, StV 2017, 460 (461).

[58] See *Bülte J.*, StV 2017, 460 (461).

[59] *Sydow G., Marsch N., Sydow H*., DS-GVO/BDSG, 3rd ed. 2022, Introduction para. 21; cf. *Schwarze J., Becker U., Hatje A., Schoo J., Schoo M.*, EU Commentary, 4th ed. 2019, TFEU Art. 325 para. 27.

[60] See also *Bülte J*, StV 2017, 460, 461.

პირველადი სამართალში გათვალისწინებული სისხლის სამართლის გარანტიები, როგორიცაა ბრალის პრინციპი.[61]

ბ) დანაშაულის ბუნება

მაშასადამე, ენგელის მეორე კრიტერიუმს გადამწყვეტი მნიშვნელობა აქვს, რომლის მიხედვითაც უნდა შემოწმდეს სამართალდარღვევის ბუნება.

აა) ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციით განსაზღვრული ჯარიმების ადრესატები

მონაცემთა დაცვის კანონმდებლობის მიხედვით, ჯარიმები მიმართული არ არის ფართო საზოგადოებისთვის, არამედ წარმოადგენს სპეციალურ სამართალდარღვევას, უპირველეს ყოვლისა, დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების წინააღმდეგ, შესაბამისად, არ მიიჩნევა სისხლისსამართლებრივ სანქციად.[62] იქიდან გამომდინარე, რომ სანქციები მიმართულია შეზღუდულ პირთა წრის მიმართ, ძირითადი რეგულაციის 83-ე მუხლის მე-4 - მე-6 პუნქტები დისციპლინური სამართლის ("disciplinary law") მსგავსია, რაც ტრადიციულად არ არის მიჩნეული სისხლის სამართლის კატეგორიად "ECtHR"-ის პრეცედენტული სამართლის მიხედვით.[63] სტანდარტის გამოყენებისას, მნიშვნელოვანია გათვალისწინებული იქნეს, რომ "GDPR"-ი არ ადგენს რაიმე კონკრეტულ შეზღუდვას ადრესატის ბუნების შესახებ, რაც ნიშნავს იმას, რომ სამართალდამრღვევი შეიძლება იყოს როგორც ფიზიკური, ისე იურიდიული პირი (რეგულაციის მე-4 მუხლის მე-7 და მე-8 პუნქტები).[64] ამ ნიშნით მონაცემთა დაცვის სამართალი განსხვავდება დისციპლინური სამართლისგან.

ბბ) იურიდიული პირებისთვის სანქციის დაკისრება

კლასიკური სისხლის სამართლისგან კიდევ ერთი განსხვავება არსებობს - მონაცემთა დაცვის კანონის მიხედვით, იურიდიული პირებიც შეიძლება იყვნენ ჯარიმის ადრესატები. სისხლის სამართალში მხოლოდ ფიზიკური პირები განიხილებიან, როგორც დამნაშავეები, განსაკუთრებით გერმანული

[61] *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P*., ECHR, 5th ed. 2023, ECHR Art. 6 para. 24.

[62] On the classification of Art. 83 para. 4-6 GDPR as a special offence *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Data Protection Criminal Law para. 136.

[63] ECtHR, BeckRS 1976, 107962 para. 81 f.; *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P.,* ECHR, 5th ed. 2023, ECHR Art. 6 para. 25.

[64] Art. 4 No. 7 Hs. 1 GDPR; *Simitis S., Hornung G., Spiecker i., Petri T.,* Datenschutzrecht, 1st ed. 2019, GDPR Art. 4 No. 7 para. 23; *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, Chapter 17 Data Protection Criminal Law para. 137.

კანონმდებლობის მიხედვით.[65] ფედერალური საკონსტიტუციო სასამართლო აკავშირებს ბრალის პრინციპს ადამიანის ღირსებასთან კონსტიტუციის პირველი მუხლის პირველი პუნქტის შესაბამისად, რომელიც მხოლოდ და მხოლოდ ფიზიკური პირის უფლებაა და არა იურიდიული პირის, როგორც იურიდიული ფიქციის. შედეგად, გამოთქმული ვარაუდის მიხედვით, "nulla poena sine culpa" პრინციპის კონსტიტუციური საფუძველი გამორიცხავს საკორპორაციო სისხლის სამართლის ეროვნულ დონეზე დანერგვას.[66]

მიუხედავად ამისა, აღნიშნული ვარაუდი არ ეხება იურიდიული პირების მიმართ სანქციების კატეგორიზაციას ზენაციონალურ დონეზე. უკვე ხაზგასმით აღინიშნა, რომ "ECJ" ნებას რთავს ბრალის პრინციპის გამოყენებას პროპორციულობის პრინციპის ფარგლებში.[67] რეგულაციის ("Cartel Regulation") 23-ე მუხლის პირველი და მე-2 პუნქტებით, პასუხისმგებლობა ეფუძნება კომპანიის განზრახ ან გაუფრთხილებელ ქმედებას.[68] საბოლო ჯამში, რეგულაციის ("Cartel Regulation") 23-ე მუხლის მე-5 პუნქტი განმარტავს, რომ ევროკავშირს ამ სფეროში არ აქვს საკანონმდებლო კომპეტენცია და ამიტომ ფიზიკური პირებისთვის სისხლის სამართლებრივი სანქციის დაწესება არ განუზრახავს.[69] "ECJ", ასევე, აღიარებს იურიდიული პირების ბრალის პრინციპს "Deutsche Wohnen"-ის საქმეზე მიღებული გადაწყვეტილებით, რომელშიც, როგორც ანტიმონოპოლიურ კანონმდებლობაში, იგი მიუთითებს თავად კომპანიის ბრალზე.[70]

გგ) ადმინისტრაციული წარმოება და შესაძლებლობის პრინციპი

მონაცემთა დაცვის სამართალში ჯარიმების დაკისრება ადმინისტრაციული წარმოების ფარგლებში საზედამხედველო ორგანოს შეხედულებისამებრ ხდება ("GDPR"-ის 58(2)(i), 83-ე მუხლების შესაბამისად), მაშინ როცა სისხლის სამართლის გადაწყვეტილებებს, როგორც წესი, სასამართლო იღებს. აღნიშნული მნიშვნელოვანი ფაქტორია ჯარიმების კლასიფიკაციისთვის ენგელის მეორე კრიტერიუმის კონტექსტში.[71]

აღნიშნული ზეგავლენას ახდენს სანქცირების პროცესზე: სისხლის სამართალში (ვიწრო გაგებით) მოქმედებს კანონიერების პრინციპი (გერმანიის სისხლის სამართლის საპროცესო კოდექსის ("StPO") 152(2) პარაგრაფის შესაბამისად), ხოლო საზედამხედველო ორგანოებს აქვთ

[65] მიუხედავად ამისა, სისხლის სამართალი ვიწრო გაგებით გაერთიანებების წინააღმდეგ უკვე არსებობდა სხვა ქვეყნებში, რომლებიც საერთო სამართლის ოჯახს არ მიეკუთვნებოდნენ, როგორც ნიდერლანდებში 1951 წლიდან; *Mitsch W., Rogall K.,* KK OWiG, 5th ed. 2018, OWiG § 30 para. 258, 270.

[66] For example, *Geco*, GA 2015, 503 (504).

[67] *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R*., European Criminal Law, 2nd ed. 2014, § 55 para. 63.

[68] ევროპულ ანტიმონოპოლიურ სამართალში ბრალეულობის შესახებ იხ. *Schröter H., Jakob M., Klotz R., Mederer W., Kienapfel P.,* Europäisches Wettbewerbsrecht, 2nd ed. 2014, Art. 23 Kart-VO para. 39 f.

[69] გარდა ამისა, 23-ე მუხლის მე-5 პუნქტი უზრუნველყოფს, რომ ზოგიერთ ეროვნულ სამართლებრივ სისტემებში სისხლის სამართლის მოქმედების შედეგები გავრცელდება ანტიმონოპოლიურ ჯარიმებზე; *Bechtold R., Bosch W., Brinker I.,* EU-Kartellrecht, 4th ed. 2023, Art. 23 Cart Regulation para. 91.

[70] ECJ, NJW 2024, 343, 347 para. 68, 78 - Deutsche Wohnen.

[71] *Ehmann E., Selmayr M., DS-GVO, 2nd ed. 2018, Art. 58 DS-GVO para. 18, 27.*

შეხედულებისამებრ მოქმედების უფლებამოსილება, რის გამოც მოქმედებს ე.წ. „შესაძლებლობის პრინციპი" ("principle of opportunity"). აღნიშნულს მოწმობს "BDSG"-ის 41(2) მუხლის 1-ელ წინადადებაში "OWiG"-ის 47-ე მუხლზე გაკეთებული მითითება.[72] შესაძლებლობის პრინციპი, ასევე, ასახულია "GDPR"-ის პრეამბულის 148-ე პუნქტში, რომლის მიხედვითაც, „თუ სახეზეა მცირე დარღვევა ან თუ ჯარიმა ფიზიკურ პირს არაპროპორციულ ტვირთს აკისრებს, ჯარიმა შეიძლება ჩაანაცვლოს საყვედურმა."[73]

თუმცა აღნიშნული არ იწვევს არსებით განსხვავებას მონაცემთა დაცვის სამართალსა და სისხლის სამართლის ძირითად პრინციპებს შორის. მონაცემთა დაცვის სამართალში შესაძლებლობის პრინციპი უნდა განიმარტოს დამოუკიდებლად ისე, რომ საზედამხედველო ორგანოების დისკრეცია, მაქსიმალურად შემცირდეს ევროკავშირის სამართლის ეფექტიანად აღსრულების უზრუნველსაყოფად. მხოლოდ გამონაკლის შემთხვევებშია შესაძლებელი ჯარიმის არ დაკისრება, რის შედეგადაც შესაძლებლობის პრინციპი პრაქტიკაში კანონიერების პრინციპს უახლოვდება.[74] გარდა ამისა, ადმინისტრაციულ წარმოებაში დაკისრებული სანქციებიც შეიძლება ფართო გაგებით მიეკუთვნოს სისხლის სამართალს. სისხლის სამართლის ვიწრო გაგებით, მონოპოლია მხოლოდ ეროვნულ სასამართლოებს აქვთ.[75]

დდ) ჯარიმის რეპრესიული მიზანი

ბოლოს, მნიშვნელოვანია შეფასდეს, იყენებს თუ არა ევროპელი კანონმდებელი მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ ჯარიმებს რეპრესიული მიზნებისთვის.[76] "GDPR"-ის 83(1) მუხლის სიტყვასიტყვითი განმარტებით შეიძლება ითქვას, რომ რეგულაციით გათვალისწინებულ სანქციებს გააჩნიათ პრევენციული მიზნები. შესაბამისად, თითოეული საზედამხედველო ორგანო ვალდებულია გაითვალისწინოს, რომ ყოველ კონკრეტულ შემთხვევაში "GDPR"-ის მოთხოვნების დარღვევისთვის შეფარდებული სანქცია იყოს ეფექტიანი, პროპორციული და პრევენციული ხასიათის. ამ უკანასკნელ კრიტერიუმს, მონაცემთა დაცვის კანონმდებლობასთან სამომავლო შესაბამისობის უზრუნველსაყოფად აქვს, როგორც კონკრეტული (მიემართება დამრღვევ პირს), ისე ზოგადი მიზნები

[72] ე.წ. შესაძლებლობების პრინციპის შესახებ *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Datenschutzstrafrecht para. 280-282; *Kühling J., Buchner B., Bergt M.*, DS-GVO/BDSG, 4th ed. 2024, Section 41 BDSG para. 16; *Barthe C., Gericke J., Diemer H.*, StPO, 9th ed. 2023, Section 152 StPO para. 4.

[73] *Bülte J.*, StV 2017, 460 (463).

[74] იხ.: *Böttger M., Zoch S.*, Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Data Protection Criminal Law para. 282; *Gola P.,* CR 2018, 353 (355 f.).

[75] *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P.*, ECHR, 5th ed. 2023, Art. 6 ECHR para. 23.

[76] ECJ, BeckRS 2023, 8994 para. 42; ECJ, BeckRS 2023, 24054 para. 49; BeckRS 2023, 24054 para. 49; *Grabenwarter C., Pabel K.* ECHR, § 24 para. 21.

(აფრთხილებს სხვა შესაძლო სამართალდამრღვევს).[77] გარდა ამისა, "GDPR"-ის 58(2)(i) და 83 მუხლები მიზნად ისახავს მონაცემთა დაცვის კანონმდებლობის დარღვევისთვის რეპრესიული სანქციის შერჩევას, რათა დაცულ იქნას "TFEU" მე-16 მუხლისა და თანამეგობრობის კანონის მე-7 და მე-8 მუხლების ფუნდამენტური მნიშვნელობა.[78]

ბოლოს, ჯერ კიდევ ძველი რომის კანონმდებლობით აღიარებული "*ultra posse nemo obligatur"* პრინციპის თანახმად, ქცევა შეიძლება გაკონტროლდეს მხოლოდ ჯარიმებით, თუკი ბრალი შეიძლება დადასტურდეს სისხლის სამართლის კანონმდებლობით მოქმედი ბრალეულობის პრინციპის შესაბამისად.[79] არავის შეიძლება მოეთხოვოს შეუძლებელი. თუკი მევალეს არ აქვს სხვა ალტერნატივა და, შესაბამისად, არ მოქმედებს ბრალეულად, იგი სამომავლოდ არ შეცვლის საკუთარ ქცევას. შედეგად, ჯარიმა ვერ ხელმძღვანელობს ქცევას (არ არის მართვადი) და არ აქვს ლეგიტიმაცია.[80]

ეე) შუალედური შედეგი

თუნდაც ბოლო არგუმენტი ადასტურებდეს, რომ "GDPR"-ის ჯარიმები სისხლისსამართლებრივ ბუნებას ატარებს ბრალი პრინციპის გამო, ასევე უნდა განიხილებოდეს სხვა არგუმენტები, რათა დასაბუთდეს სანქციების სისხლისსამართლებრივი ბუნება**.**

გ) სასჯელის სიმძიმე

რაც შეეხება მესამე კრიტერიუმს, "GDPR"-ის 58-ე მუხლის მე-2 პუნქტის „i" ქვეპუნქტის და 83-ე მუხლის მიხედვით ჯარიმის მაქსიმალური ოდენობა უნდა იყოს საკმაოდ დიდი. "GDPR"-ის 83-ე მუხლის მე-5 და მე-6 პუნქტების შესაბამისად, ჯარიმის (პოტენციური) ოდენობა, შეიძლება იყოს ფინანსური გასული წლიური ბრუნვის 4%, რომელიც წარმოადგენს მაქსიმალურ სანქციას, რომელიც მნიშვნელოვანი სიმძიმისაა.[81] ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ ახლახან დააკისრა 1.2 მილიარდი ევროს ოდენობით ჯარიმა სოციალურ ქსელს, რაც ნათელია, რომ მახვილ ხმალს წარმოადგენს კომპანიისთვის.[82]

[77] *Parigger M., Helm T., Stevens-Bartol E., Müller R.,* Labour and Social Criminal Law, 1st ed. 2021, Art. 83 GDPR para. 92.
[78] იხ.: recitals 148 and 152 GDPR; *Sydow G., Marsch N.*, DS-GVO/BDSG, 3rd ed. 2022, Art. 83 GDPR para. 2.
[79] *Hassemer W.,* ZRP 2011, 192, პრინციპის შესახებ, რომელსაც ჯერ კიდევ *პუბლიუს იუვენციუს ცელსუსი* აღნიშნავდა.
[80] *Heckmann D.*, MMR 2023, 816 (818); in a different context on the validity of the principle of *ultra posse nemo obligatur* in data protection law *Hacker,* MMR 2018, 779 (784).
[81] *Paal B., Pauly D. A., Frenzel E.*, DS-GVO/BDSG, 3rd ed. 2021, Art. 83 DS-GVO para. 18-26; *Jarass H.*, GRC, 4th ed. 2021, Art. 48 GRC para. 9.
[82] *Klaas A., Basar B.*, ZD 2023, 477.

3.3. შედეგი

ენგელის მეორე და მესამე კრიტერიუმის მიხედვით, "GDPR"-ის 83-ე მუხლით გათვალისწინებული ჯარიმები უნდა ჩაითვალოს სისხლისსამართლებრივ სანქციებად. ამიტომ, "nulla poena sine culpa" პრინციპი იმოქმედებს. აქედან გამომდინარე, საზედამხედველო ორგანოებს უნდა ჰქონდეთ ვალდებულება დაამტკიცონ დამუშავებისთვის პასუხისმგებელი ან უფლებამოსილი პირის ბრალი ჯარიმის დაკისრებისას.[83]

4. გადაწყვეტილების "Deutsche Wohnen" დაკარგული პოტენციალი

ბრალის საკითხის მონაცემთა დაცვის სანქციებთან დაკავშირება დოგმატურად მნიშვნელოვანია.[84] ერთ-ერთ საქმეში, სადაც იტალიის კონკურენციის სააგენტოს მიერ კომპანიას დაეკისრა ჯარიმა, ევროკავშირის მართლმსაჯულების სასამართლომ დაადგინა, რომ უსამართლო კონკურენციის კანონმდებლობის შესაბამისად დაწესებული ჯარიმები ფართო გაგებით წარმოადგენს სისხლის სამართალს, რაც ამტკიცებს "*ne bis in idem"* პრინციპის (ორმაგი დასჯის აკრძალვა - აკრძალულია ერთი და იმავე დანაშაულისათვის ერთი და იმავე პირის ორჯერ გასამართლება და დასჯა.) ვალიდობას ევროკავშირის ძირითად უფლებათა ქარტიის 50-ე მუხლის მიხედვით.[85]

ორმაგი დასჯის აკრძალვა არც მონაცემთა დაცვის სამართლისთვის არის უცხო, რასაც "GDPR"-ის 84-ე მუხლი და პრეამბულის 149-ე პუნქტიც მოწმობს, რომლის მიხედვით წევრ სახელმწიფოებს შეუძლიათ დაადგინონ წესები, რომლებიც განსაზღვრავს სისხლის სამართლის პასუხისმგებლობას.[86] სასურველია, "ECJ"-ის განემარტა, რომ აღნიშნული სამართლებრივი პრინციპი დაცულია ძირითადი უფლებების ქარტიით (Art. 50 CFR) და მონაცემთა დაცვის სანქციები სისხლის სამართალს წარმოადგენს ფართო გაგებით. იგივე ეხება კანონიერების პრინციპს (ქარტიის 49-ე მუხლის პირველი პუნქტი და კონვენციის მე-7 მუხლის პირველი პუნქტი). მიუხედავად "GDPR"-ის

[83] ძირითადი რეგულაციით განსაზღვრული ჯარიმა, როგორც სისხლის სამართლის სანქცია, *Drewes S., Walchner W.*, CR 2023, 163 (168); with further comments *Sydow G., Marsch N.,* DS-GVO/BDSG. Third ed. 2022, Art. 83 GDPR para. 3; *Wolff H. A., Brink S.,* von *Ungern-Sternberg M. A., Holländer*, Data Protection Law, 46th edition 2021, Art. 83 GDPR para. 4.2.

[84] *Vogel*, JZ 1995, 331 (337).

[85] ECJ, NJW 2024, 33 para. 55.

[86] *Klaas A., Momsen C., Wybitul T., Klaas A.,* Datenschutzsanktionenrecht, 1st ed. 2023, § 27 para. 34.

ჯარიმებთან დაკავშირებისა, ხშირად ეჭვქვეშ დგას განსაზღვრულობის პრინციპი.[87]

გარდა ამისა, კანონმდებლობა უზრუნველყოფს სხვადასხვა სამართლებრივ გარანტიებს: უდანაშაულობის პრეზუმფცია (კონვენციის მე-6 მუხლის მე-2 პუნქტი და ქარტიის 48-ე მუხლის პირველი პუნქტი), სამართლიანი სასამართლოს უფლება (მე-6 მუხლის პირველი პუნქტი, "ECHR") და თვითინკრიმინაციის აკრძალვა (*"nemo teneur se ipsum accusare"*), რომელიც ასევე დაცული უნდა იყოს მონაცემთა დაცვის კანონმდებლობით.[88]

5. დასკვნა

ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებაში "Deutsche Wohnen", სასამართლომ სწორად აღნიშნა, რომ ძირითადი რეგულაციით განსაზღვრული სანქცია მხოლოდ იმ შემთხვევაში შეიძლება დაეკისროს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, თუ იგი დამნაშავეა. სამწუხაროდ, ლუქსემბურგი მხოლოდ მონაცემთა დაცვის სანქციების სისტემასა და მიზანს ითვალისწინებს. გარდა ამისა, ბრალის პრინციპის გამოყენება უკვე აუცილებელია, რადგან "GDPR"-ის ჯარიმები სისხლისსამართლებრივ სანქციას წარმოადგენს. როგორც კი "ECJ" უგულებელყოფს სამართლებრივი ბუნების საკითხს, ის ამცირებს თავის გადაწყვეტილების მოქმედების არეალს მონაცემთა დაცვის სანქცირების სამართლის სახელმწიფო უფლებების გარანტიების შესახებ. თუმცა, "ECJ"-ს გადაწყვეტილების ერთი ასპექტი სრულიად ცალსახაა: პრინციპი *"nulla poena sine culpa",* ასევე, ვრცელდება ძირითადი რეგულაციის მოქმედების ფარგლებში.

ბიბლიოგრაფია:

1. *Ackermann T.,* ZEuP 2023, 529 (555 et seq.).
2. *Adam T., Schmidt F., Schumacher L.*, NStZ 2017, 7-8.
3. *Barrot W.,* ZJS 2010, 701-702.
4. *Barthe C., Gericke J., Diemer H.*, StPO, 9th ed. 2023, Section 152 StPO para. 4.
5. *Bechtold R., Bosch N., Brinker I., Bechtold R.,* EU-Kartellrecht, 4th ed. 2023, Regulation (EC) 1/2003, Art. 23 para. 91.

[87] ეხება პირდაპირი პასუხისმგებლობის აღიარებას; ECJ, NJW 2024, 343, 347 para. 60 - Deutsche Wohnen; *Sydow G., Marsch N.*, DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 3 f.; *Gola P., Heckmann D.,* DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 24.

[88] თვითინკრიმინაციის აკრძალვის შესახებ იხ. Section 43 (4) BDSG in conjunction with Art. 33 GDPR. Art. 33 GDPR; *Klaas A., Momsen C., Wybitul T., Cornelius K.*, Datenschutzsanktionenrecht, 1st ed. 2023, § 2 Grundlagen para. 126; *Sydow G., Marsch N.* DS-GVO/BDSG, 3rd ed. 2022, Art. 83 GDPR para. 3.

6. *Böse M., Satzger H.*, Europäisches Strafrecht (EnzEuR Bd. 9), 1st ed. 2013, § 2 para. 59.
7. *Böse M., Stuckenberg C.*, Europäisches Strafrecht (EnzEuR Bd. 11), 2nd ed. 2021, § 10 para. 17.
8. *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Data Protection Criminal Law para. 282; *Gola,* CR 2018, 353 (355 f.).
9. *Brink S., Wybitul T.,* ZD 2024, 137 (142).
10. *Bülte J*, StV 2017, 460 (461).
11. *Calliess C., Ruffert M., Blanke H.*, EUV/AEUV, 6th ed. 2022, Art. 48 CFR para. 1-2, 4.
12. COM(2011) 573 final, 10; Council Doc. 16542/2/09 REV 2 No. 6-8.
13. *Dörr C., Grote H., Marauhn T.,* ECHR/GG, 3rd ed. 2022, ch. 14 para. 26.
14. *Drewes S., Walchner W.*, CR 2023, 163 (168).
15. *Dürig G., Herzog R., Herdegen M.,* GG (Vol. I), Art. 1 para. 36.
16. *Ehmann E., Selmayr M.,* DS-GVO, 2nd ed. 2018, Art. 58 DS-GVO para. 18, 27.
17. *Engelhart H.,* NZWiSt 2015, 201, 203.
18. *Engels H.*, Unternehmensvorsatz und Unternehmensfahrlässigkeit im Europäischen Kartellrecht, 2002, 71.
19. European Parliament resolution of 22 May 2012 on the EU approach to criminal law (2010/2310(INI)), C 264 E/9.
20. Explanations on the Charter of Fundamental Rights, OJ 2007 No. C 303/17, 30.
21. *Frister H.*, Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 25, 89.
22. *Fromm E.*, ZIS 2007, 279, 287.
23. *Gassner K., Seith S.,* Ordnungswidrigkeitengesetz, 2nd ed. 2020, Introduction para. 6.
24. *Geco*, GA 2015, 503 (504).
25. *Gerhold S.*, 41st ed., Introduction to the OWiG para. 5.
26. *Globke*, in: *Brunhöber W., Höffler B., Kaspar F., Reinbacher R., Vormbaum M.,* (eds.) Strafrecht und Verfassung, 2012, 59, 66, 67.
27. *Gola P., Heckmann D.,* DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 24.
28. *Grabenwarter C., Pabel K.*, ECHR, § 24 para. 19, 21, 22.
29. *Grabenwarter C., Pabel K.*, ECHR, 6th ed. 2016, § 24 para. 21.
30. *Grabitz E., Hilf M., Nettesheim M., Vogel P., Eisele J.,* Das Recht der Europäischen Union, 80th ed. 2023, Art. 83 TFEU, para. 46.
31. *Hassemer W.,* ZRP 2011, 192.
32. *Heckmann D.,* MMR 2023, 816 (818); in a different context on the validity of the principle of *ultra posse nemo obligatur* in data protection law *Hacker,* MMR 2018, 779, 784.
33. *Hochmayr G.*, ZIS 2016, 226, 230.
34. *Hörnle J.*, JZ 1999, 1080 (1088), is critical of the differentiation between criminal liability and criminal justification liability.
35. *Jarass H.*, CFR, 4th ed. 2021, Art. 48 para. 9, 12, 19.

36. *Karpenstein U., Mayer F.C.,* ECHR, 3rd ed. 2022, Art. 6 para. 25, 26.
37. *Keil G.*, Willensfreiheit, 2nd ed. 2013, 157.
38. *Klaas A., Momsen C., Wybitul T*., Datenschutzsanktionenrecht, 1st ed. 2023, § 2 para. 22.
39. *Korte K.*, ZD-Aktuell 2024, 01500; https://www.lto.de/recht/hintergruende/h/eugh-c80721-deutsche-wohnen-dsgvo-bussgeld-erfolg-datenschutz-beauftragte-kartellrecht/ (last accessed on 1 March 2024).
40. *Kühling J., Buchner B., Bergt M.*, DS-GVO/BDSG, 4th ed. 2024, Section 41 BDSG para. 16.
41. KG Berlin BeckRS 2024, 2154; see on the question referred KG Berlin ZD 2022, 156.
42. *Meyer J., Hölscheidt S., Eser A., Kubiciel M.,* CFR, 5th ed. 2019, Art. 48 CFR para. 1, 6-7, 10, 13, 38.
43. *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P.*, ECHR, 5th ed. 2023, Art. 6 ECHR para. 23-25.
44. *Mitsch W., Rogall K,* KK OWiG, 5th ed. 2018, OWiG § 30 para. 258, 270.
45. Opinion GA Carl Otto Lenz, 11 July 1992, Case C-143/91, EU:C:1990:381.
46. Opinion GA Juliane Kokott, 28 February 2013, Case C-681/11, EU:C:2013:126, para. 41.
47. *Paal B., Pauly D. A., Frenzel E.*, DS-GVO/BDSG, 3rd ed. 2021, Art. 83 DS-GVO para. 18-26.
48. *Parigger M., Helm T., Stevens-Bartol E., Müller R.,* Labour and Social Criminal Law, 1st ed. 2021, Section 42 BDSG para. 1.
49. *Pechstein M., Nowak R., Häde U., Schröder R.*, Frankfurter Kommentar EUV/AEUV/GRC, 2nd ed. 2023, Art. 49 para. 20.
50. *Rabe P.*, Das Verständigungsurteil des Bundesverfassungsgerichts und die Notwendigkeit von Reformen im Strafprozess, 2017, 147.
51. *Roxin C., Greco L*., Strafrecht AT I, 2020, § 19 para. 9, 62.
52. *Satzger H.,* ZRP 2010, 137, 139.
53. *Schaut A.*, Europäische Strafrechtsprinzipien, 2012, 228.
54. S*chönke A., Schröder H., Eisele J*., StGB, 30th ed. 2019, Vor. §§ 13 ff. para. 103.
55. *Schröter H., Jakob M., Klotz R., Mederer W., Kienapfel P.,* Europäisches Wettbewerbsrecht, 2nd ed. 2014, Art. 23 Kart-VO para. 39 f.
56. *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R.,* Europäisches Strafrecht, 2nd ed. 2014, § 55 para. 60, 63.
57. *Simitis S., Hornung G., Spiecker i., Petri T.,* Datenschutzrecht, 1st ed. 2019, GDPR Art. 4 No. 7 para. 23.
58. *Sydow G., Marsch N.* , DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 2, 3 f.
59. *Tiedemann K.*, NJW 1993, 23, 28.
60. *Vogel P.*, JZ 1995, 331 (337).
61. *Wolff H. A., Brink S., von Ungern-Sternberg M. A.,* Data Protection Law, 46th edition 2021, Art. 83 GDPR para. 4.2.

62. *Zelger F.,* EuR 2021, 478 (481 et seq.).
63. BVerfGE 109, 133, 174 = NJW 2004, 739 (746).
64. BVerfGE 128, 326, 376 = NJW 2011, 1931 (1938).
65. BVerfGE 123, 267, 348 = NJW 2009, 2267 (2271).
66. BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289).
67. BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289).
68. BVerfGE 30, 1, 41 = NJW 1971, 275 (282).
69. BVerfGE 95, 96, 131 = NJW 1997, 929 (930).
70. BVerfGE 95, 96, 140 = NJW 1997, 929 (932).
71. ECJ judgement of 11 July 2002, Case C-210/00, ECR 2002 I-6453 para. 44 – *Käserei Champignon Hofmeister*.
72. ECJ judgement of 18.11.1987, Case 137/85, ECR 1987, 4587 para. 14 – *Maizena*.
73. ECJ judgement of. 16.11.1983, Case 188/82, ECR 1983, 3721 para. 18 – *Thyssen*.
74. ECJ NJW 2024, 343 para. 68.
75. ECJ, BeckRS 2012, 81043 para. 37 – Bonda.
76. ECJ, BeckRS 2018, 6055 para. 26 f. - Menci Luca.
77. ECJ, BeckRS 2018, 6055 para. 31.
78. ECJ, BeckRS 2022, 5011 para. 25 – bpost.
79. ECJ, BeckRS 2022, 5011 para. 26.
80. ECJ, BeckRS 2023, 24054 para. 49, 53.
81. ECJ, BeckRS 2023, 8994 para. 40, 42, 46.
82. ECJ, NJW 2024, 33, para. 45 - Volkswagen Italia SpA.
83. ECJ, NJW 2024, 343 para. 55, 60, 61, 62, 66, 67,70, 73, 74, 75, 78.
84. ECJ, NJW 2024, 343, 347 para. 68, 78 - Deutsche Wohnen.
85. ECtHR, BeckRS 1976, 107962 para. 81 f.
86. ECtHR, BeckRS 2010, 21072 para. 53 - Zolotoukhine v Russia.
87. ECtHR, BeckRS 2010, 21072.
88. ECtHR, BeckRS 2010, 2107253 - Zolotoukhine v Russia.
89. ECtHR, EuGRZ 1976, 221 - Engel et al. v Netherlands.

ოთარ ჩახუნაშვილი[*]

პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოების პრინციპები

პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლა პერსონალურ მონაცემთა დაცვის სამსახურის ერთ-ერთი მთავარი ფუნქციაა და მოიცავს როგორც პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული განცხადებების განხილვას, ისე პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმებას (ინსპექტირებას). სტატია ეთმობა პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლისას არსებულ იმ პრინციპებს, რომლებიც გამომდინარეობს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონითა და საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით განსაზღვრული მოთხოვნებიდან და რომელთა შესაბამისადაც პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ხორციელდება თითოეული საქმის წარმოების პროცესი.

საკვანძო სიტყვები: *პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლა, ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოება, ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოების პრინციპები.*

1. შესავალი

პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში საქმის წარმოების პროცესის სათანადოდ განხორციელების

[*] სამართლის დოქტორი, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასისტენტ-პროფესორი, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის პირველი მოადგილე.

მიზნით, კრიტიკულად მნიშვნელოვანია დაცული იყოს ის პრინციპები, რომლებიც მკაფიოდ არის დადგენილი მოქმედი კანონმდებლობით ან გამომდინარეობს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით ან შესაბამისი კანონქვემდებარე ნორმატიული აქტებით განსაზღვრული დებულებების მიხედვით.

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის 52-ე მუხლის თანახმად, თუ პერსონალურ მონაცემთა დაცვის სამსახური გამოავლენს ადმინისტრაციულ სამართალდარღვევას, იგი უფლებამოსილია შეადგინოს ადმინისტრაციული სამართალდარღვევის ოქმი და, შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს ან/და დამუშავებაზე უფლებამოსილ პირს დააკისროს ადმინისტრაციული პასუხისმგებლობა ამ კანონითა და საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით დადგენილი წესით. ამასთან, ხსენებული კანონის 58-ე მუხლის მე-3 პუნქტის მიხედვით, სამსახურის უფროსის უფლებამოსილება და საქმის წარმოების წესი განისაზღვრება ამ კანონით, საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით, სხვა საკანონმდებლო აქტებითა და სამსახურის უფროსის ნორმატიული აქტებით, ხოლო ამავე მუხლის მე-4 პუნქტის შესაბამისად, საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსისა და ამ კანონის ნორმების ურთიერთმიმართებისას უპირატესობა ენიჭება ამ კანონით განსაზღვრულ ნორმებს.

2023 წელს მიღებულმა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონმა, მთელ რიგ სიახლეებთან ერთად, ახლებურად ჩამოაყალიბა კანონის მოთხოვნათა დარღვევისთვის ადმინისტრაციული პასუხისმგებლობის დაკისრების წესი და თუ მანამდე მოქმედ რედაქციაში ადმინისტრაციული სახდელის დაკისრება ძირითადად ხდებოდა საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით გათვალისწინებული დებულებების მიხედვით, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს მოქმედი კანონი განახლებული ფორმით, დარგის თავისებურებების გათვალისწინებით, ადგენს ყველა იმ წესს, რომელიც დაცული უნდა იყოს საქმის წარმოების პროცესში.

ნაშრომში განხილულია პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლისას საქმის წარმოების თითოეული ის პრინციპი, რომელიც ასახულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონსა და საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსში, რომელთა განუხრელი დაცვის გარეშე შეუძლებელია ადმინისტრაციული სამართალდარღვევის საქმეზე სათანადო გადაწყვეტილების მიღება.

2. კანონიერება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 39-ე მუხლის მე-3 პუნქტი განსაზღვრავს უშუალოდ პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის პრინციპებს, რომლის პირველივე პრინციპად კანონიერებაა დადგენილი, რაც, თავის მხრივ, გულისხმობს იმას, რომ პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოებისას, თითოეული მოქმედება შესაბამისობაში უნდა იყოს ზემოთ მითითებულ საკანონმდებლო აქტებთან.

პერსონალურ მონაცემთა დაცვის სამსახური საქმიანობის განხორციელებისას ხელმძღვანელობს საქართველოს კონსტიტუციით, საქართველოს საერთაშორისო ხელშეკრულებებით, საერთაშორისო სამართლის საყოველთაოდ აღიარებული პრინციპებითა და ნორმებით, ამ კანონითა და სხვა სათანადო სამართლებრივი აქტებით.[1]

ადმინისტრაციული სამართალდარღვევებისათვის ზემოქმედების ზომათა შეფარდებისას კანონიერების უზრუნველყოფას განსაზღვრავს ადმინისტრაციულ სამართალდარღვევათა კოდექსიც, რომლის მე-8 მუხლის თანახმად, „არავის არ შეიძლება შეეფარდოს ზემოქმედების ზომა ადმინისტრაციული სამართალდარღვევების გამო, თუ არა კანონმდებლობით დადგენილ საფუძველზე და წესით. ადმინისტრაციულ სამართალდარღვევათა საქმეებს აწარმოებენ კანონიერების მკაცრი დაცვის საფუძველზე. საამისოდ უფლებამოსილი ორგანოები და თანამდებობის პირნი ადმინისტრაციული ზემოქმედების ზომებს შეუფარდებენ თავიანთი კომპეტენციის ფარგლებში, კანონმდებლობის ზუსტი შესაბამისობით.“

კანონიერების პრინციპის დაცვა ასევე გათვალისწინებულია კოდექსის 33-ე მუხლის შემადგენლობითაც, რომელიც ადგენს ადმინისტრაციული სახდელის დადების ზოგად წესს. კერძოდ, აღნიშნული მუხლის მიხედვით, „ადმინისტრაციული სამართალდარღვევისათვის სახდელი დაედება იმ ნორმატიული აქტით დაწესებულ ფარგლებში, რომელიც ითვალისწინებს პასუხისმგებლობას ადმინისტრაციულ სამართალდარღვევათა შესახებ ამ კოდექსის და ადმინისტრაციულ სამართალდარღვევათა შესახებ სხვა აქტების ზუსტი შესაბამისობით.“

3. ადამიანის უფლებათა და თავისუფლებათა დაცვა

ადამიანის უფლებათა და თავისუფლებათა დაცვის პრინციპი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პირველივე მუხლშია განსაზღვრული, კერძოდ, „ამ კანონის მიზანია პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური

[1] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 39-ე მუხლის მე-2 პუნქტი.

ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების, დაცვა.“

შესაბამისად, ადმინისტრაციულ სამართალდარღვევათა წარმოების თითოეულ ეტაპზე ზედმიწევნით უნდა იქნას დაცული საქართველოს კონსტიტუციითა და საერთაშორისო ნორმებით საყოველთაოდ აღიარებული ადამიანის ძირითადი უფლებები და თავისუფლებები.

4. დამოუკიდებლობა და პოლიტიკური ნეიტრალიტეტი

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ფუნქციები და მოვალეობები გამორჩეულია ქვეყანაში არსებულ ადმინისტრაციულ ორგანოებს შორის, რისი ძირითადი განმაპირობებელი არის მისი სამართლებრივი მოწყობის ფორმა. ამ მხრივ, პირველ რიგში, აღსანიშნავია პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს დამოუკიდებლობა და პოლიტიკური ნეიტრალიტეტი, რომელიც როგორც საერთაშორისო, ასევე ეროვნული კანონმდებლობით არის განმტკიცებული.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“General Data Protection Regulation“) მიხედვით[2], მონაცემთა დაცვის საზედამხედველო ორგანოები არიან სრულიად დამოუკიდებელნი თავიანთი ამოცანების შესრულებისა და უფლებამოსილების განხორციელებისას, ხოლო, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, დამოუკიდებლობა და პოლიტიკური ნეიტრალიტეტი, სამსახურის საქმიანობის ერთ-ერთი ძირითადი პრინციპია. შესაბამისად, პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოებისას სამსახურის თანამშრომელი მოქმედებს დამოუკიდებლად და უფლება არ აქვს, თავისი სამსახურებრივი მდგომარეობა პარტიული (პოლიტიკური) მიზნებისათვის ან/და ინტერესებისათვის გამოიყენოს.

ზემოაღნიშნულ პრინციპს პრაქტიკაში ასევე განამტკიცებს კანონის 55-ე მუხლი, რომელიც განსაზღვრავს პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლის სამართლებრივ დაცვას და ადგენს რომ „კანონის მიხედვით, არავის არა აქვს უფლება, ჩაერიოს პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლის სამსახურებრივ საქმიანობაში, გარდა კანონით გათვალისწინებული შემთხვევებისა.“ ასევე, ამავე მუხლის თანახმად, „პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლის მიერ სამსახურებრივი მოვალეობის შესრულებისას მისთვის ხელის შეშლა, მისი პატივისა და ღირსების შელახვა, მისთვის წინააღმდეგობის გაწევა, მის მიმართ მუქარა, ძალადობა ან მისი სიცოცხლის, ჯანმრთელობის ან ქონების ხელყოფა იწვევს საქართველოს კანონმდებლობით დადგენილ პასუხისმგებლობას. სამსახურებრივი უფლებამოსილებების

[2] პერსონალურ მონაცემთა დაცვის სამსახური, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”) - ქართული თარგმანი.

განხორციელებასთან დაკავშირებით პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის პირველი მოადგილის ან მოადგილის, პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლის ან მისი ოჯახის წევრის სიცოცხლის, ჯანმრთელობისა და ქონების ხელყოფის შესახებ ინფორმაციის მიღების შემთხვევაში სახელმწიფო ორგანოები ვალდებული არიან განახორციელონ კანონით გათვალისწინებული ღონისძიებები მისი/მათი პირადი და ქონებრივი უსაფრთხოების დასაცავად.“[3]

ამასთან, გარდა იმისა, რომ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსისთვის ან სამსახურის უფლებამოსილი პირისთვის კანონით განსაზღვრული უფლების განხორციელებაში ხელის შეშლა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიხედვით[4] წარმოადგენს ადმინისტრაციულ სამართალდარღვევას და ადმინისტრაციული სახდელის სახით პირს შესაძლოა დაეკისროს ფულადი ჯარიმა 1 000 ლარიდან 6 000 ლარამდე ოდენობით, აღსანიშნავია ისიც, რომ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსზე ან სამსახურის მოსამსახურეზე ზემოქმედება არის საქართველოს სისხლის სამართლის კოდექსით[5] გათვალისწინებული დანაშაულებრივი ქმედება და იწვევს სისხლისსამართლებრივ პასუხისმგებლობას.

5. ობიექტურობა და მიუკერძოებლობა

ობიექტურობა და მიუკერძოებლობა მჭიდროდ უკავშირდება ზემოთ განხილულ დამოუკიდებლობას და პოლიტიკური ნეიტრალიტეტს, თუმცა იგი დამოუკიდებელ პრინციპს წარმოადგენს და ცალკე არის განსაზღვრული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, როგორც პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის ერთ-ერთი საფუძველი.

საგულისხმოა, რომ მოქმედი ადმინისტრაციულ სამართალდარღვევათა კოდექსი მიუკერძოებლობის პრინციპს მკაფიოდ არ განსაზღვრავს და საქმის წარმოებისას მისი დაცვის ვალდებულება ირიბად გამომდინარეობს კოდექსის 233-ე მუხლის ჩანაწერიდან, რომლის მიხედვითაც „ადმინისტრაციული სამართალდარღვევის საქმეს განიხილავენ კანონის და საქმის განმხილველი ორგანოს (თანამდებობის პირის) წინაშე ყველა მოქალაქის თანასწორობის საწყისებზე წარმოშობის, სოციალური და ქონებრივი მდგომარეობის, რასობრივი და ეროვნული კუთვნილების, სქესის, განათლების, ენის, რელიგიისადმი დამოკიდებულების, საქმიანობის სახეობისა და ხასიათის, საცხოვრებელი ადგილისა და სხვა გარემოებათა მიუხედავად.“

[3] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 55-ე მუხლის მე-3 პუნქტი.

[4] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 88-ე მუხლი.

[5] საქართველოს სისხლის სამართლის კოდექსი, 22/07/1999, 352[1] მუხლი.

6. თანაზომიერება

თითოეული შემზღუდველი ხასიათის ღონისძიება, რომლის გამოყენებაც ხდება შესაბამისი ადმინისტრაციული ორგანოს მხრიდან, უნდა იყოს თანაზომიერი. თანაზომიერების პრინციპი კრძალავს მმართველობითი ღონისძიების ადრესატის შეუსაბამო შეზღუდვას. ეს პრინციპი თავის მხრივ გამომდინარეობს სამართლებრივი სახელმწიფოს კონსტიტუციური პრინციპიდან, რომლის თანახმადაც, ადმინისტრაციულ-სამართლებრივი ურთიერთობის მონაწილე რომელიმე მხარის კონსტიტუციური უფლების შეზღუდვა იმდენად არის დასაშვები, რამდენადაც ის საჯარო ინტერესების დაცვისათვის გარდაუვალი საშუალებაა.[6]

თანაზომიერების პრინციპი ფასდება ადმინისტრაციული ორგანოს მიერ გამოყენებულ საშუალებასა და მისაღწევ მიზანს შორის არსებული დამოკიდებულება. საშუალებასა და მიზანს შორის თანაზომიერების შემოწმება ხდება ოთხი ნაბიჯის გავლით[7]: მიზნის დადგენა, შესაფერისობის დადგენა, აუცილებლობის დადგენა, პროპორციულობის დადგენა. აღნიშნული ნაბიჯები კი, დეტალურადაა განხილული ქართულ მეცნიერებაში.[8]

ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოების დროს თანაზომიერების პრინციპის სათანადოდ გამოყენებას საკმაოდ დიდი მნიშვნელობა აქვს, განსაკუთრებით საქმის განმხილველი უფლებამოსილი ორგანოს მხრიდან შესაბამისი ადმინისტრაციული სახდელის თუ მონაცემთა დამუშავებაზე პასუხისმგებელი პირისთვის სავალდებულოდ შესასრულებელი დავალების გაცემის შერჩევასთან დაკავშირებული გადაწყვეტილების მიღებისას.

აღნიშნული პრინციპის დაცვის მნიშვნელობას ხაზს უსვამს ისიც, რომ „ევროპის პერსონალურ მონაცემთა დაცვის ზედამხედველის“ მიერ შემუშავებულ იქნა სახელმძღვანელო დოკუმენტი გამოსაყენებელი ზომების პროპორციულობის შესახებ, სადაც აღნიშნულია, რომ თანაზომიერების/პროპორციულობის პრინციპი ზღუდავს ორგანოებს უფლებამოსილების განხორციელებაში, რადგან მოითხოვს ბალანსის დაცვას გამოყენებულ საშუალებებსა და დასახულ მიზანს (ან მიღწეულ შედეგს) შორის.[9]

[6] *Detterbeck S.,* Allgemeines Verwaltungsrecht, 2004, 67.
[7] იქვე, 68-72.
[8] *ტურავა პ., წკეპლაძე ნ.,* ზოგადი ადმინისტრაციული სამართლის სახელმძღვანელო, 2010, 27.
[9] European Data Protection Supervisor, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, *2021, retrieved from <https://edps.europa.eu> [10.02.2025].*

7. კანონის წინაშე თანასწორობა

საქართველოს კონსტიტუციის თანახმად[10], „ყველა ადამიანი სამართლის წინაშე თანასწორია. აკრძალულია დისკრიმინაცია რასის, კანის ფერის, სქესის, წარმოშობის, ეთნიკური კუთვნილების, ენის, რელიგიის, პოლიტიკური ან სხვა შეხედულებების, სოციალური კუთვნილების, ქონებრივი ან წოდებრივი მდგომარეობის, საცხოვრებელი ადგილის ან სხვა ნიშნის მიხედვით.“

ზემოაღნიშნული პრინციპი გაზიარებულია საქართველოს ზოგად ადმინისტრაციული კოდექსში, რომლის მე-4 მუხლის თანახმად, ყველა თანასწორია კანონისა და ადმინისტრაციული ორგანოს წინაშე. დაუშვებელია ადმინისტრაციულ-სამართლებრივი ურთიერთობის მონაწილე რომელიმე მხარის კანონიერი უფლებისა და თავისუფლების, კანონიერი ინტერესის შეზღუდვა ან მათი განხორციელებისათვის ხელის შეშლა, აგრეთვე მათთვის კანონმდებლობით გაუთვალისწინებელი რაიმე უპირატესობის მინიჭება ან რომელიმე მხარის მიმართ რაიმე დისკრიმინაციული ზომების მიღება. ამავე მუხლის მე-3 ნაწილის მიხედვით კი, საქმის გარემოებათა იდენტურობის შემთხვევებში დაუშვებელია სხვადასხვა პირის მიმართ განსხვავებული გადაწყვეტილების მიღება, გარდა კანონით გათვალისწინებული საფუძვლის არსებობისას.

კანონის წინაშე თანასწორობის ეს ზოგადი დებულება გულისხმობს სახელმწიფო აპარატის მხრიდან თვითნებობის აკრძალვას. დაუშვებელია არსებითად იდენტური საქმის გარემოებების თვითნებურად არათანაბრად შეფასება და პირიქით, არსებითად არათანაბარი საქმის გარემოებების თვითნებურად თანაბარი შეფასება და აქედან გამომდინარე, უკანონო გადაწყვეტილების მიღება. ამ კონსტიტუციური პრინციპის ზოგად ადმინისტრაციულ კოდექსში ასახვა ემსახურება ადმინისტრაციულ-სამართლებრივი ურთიერთობის მონაწილეთა უფლებების დაცვას, რამდენადაც ის გულისხმობს, რომ დაუშვებელია ამ ურთიერთობის რომელიმე მხარის კანონიერი უფლებისა და თავისუფლების, კანონიერი ინტერესის შეზღუდვა ან მათი განხორციელებისათვის ხელის შეშლა, აგრეთვე მათთვის კანონმდებლობით გაუთვალისწინებელი რაიმე უპირატესობის მინიჭება, ან რომელიმე მხარის მიმართ რაიმე დისკრიმინაციული ზომების მიღება. ამ მოთხოვნის დარღვევა გვაქვს სახეზე, როდესაც არ იკვეთება ადმინისტრაციულ-სამართლებრივი ურთიერთობის ერთ-ერთი მხარის შეზღუდვის ან მისთვის უპირატესობის მინიჭების გონიერი, საქმის არსიდან გამომდინარე საფუძველი, არამედ აშკარაა შეუსაბამობა განხორციელებულ ღონისძიებასა და საქმის ფაქტობრივ გარემოებებს შორის.[11]

საქმის განხილვას მოქალაქეთა თანასწორობის საწყისებზე ითვალისწინებს ადმინისტრაციულ სამართალდარღვევათა კოდექსის 233-ე

[10] საქართველოს კონსტიტუცია, 1995, მე-11 მუხლი.
[11] *ტურავა პ., წკეპლაძე ნ.,* ზოგადი ადმინისტრაციული სამართლის სახელმძღვანელო, 2010, 27.

მუხლი, რომელიც, როგორც ზემოთ აღინიშნა, ადგენს, რომ ადმინისტრაციული სამართალდარღვევის საქმეს განიხილავენ კანონის და საქმის განმხილველი ორგანოს (თანამდებობის პირის) წინაშე ყველა მოქალაქის თანასწორობის საწყისებზე წარმოშობის, სოციალური და ქონებრივი მდგომარეობის, რასობრივი და ეროვნული კუთვნილების, სქესის, განათლების, ენის, რელიგიისადმი დამოკიდებულების, საქმიანობის სახეობისა და ხასიათის, საცხოვრებელი ადგილისა და სხვა გარემოებათა მიუხედავად.

კანონის წინაშე თანასწორობის პრინციპი „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით გათვალისწინებულ და ნაშრომში განხილულ საქმიანობის პრინციპებთან პირდაპირ კავშირშია, რასაც ცხადყოფს ასევე ის გარემოება, რომ კანონი პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის ერთ-ერთ მნიშვნელოვან პრინციპად პროფესიონალიზმს განსაზღვრავს. აღნიშნული ასევე მოიაზრებს იმას, რომ სამსახურის თანამშრომელი პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში ხელმძღვანელობს პროფესიული ცოდნის, უნარ-ჩვევებისა და გამოცდილების შესაბამისად და გადაწყვეტილებას იღებს საჯარო ინტერესების გათვალისწინებით, კონკრეტული სამართლებრივი საფუძვლის ზუსტი შესაბამისობით.

8. საიდუმლოებისა და კონფიდენციალურობის დაცვა

გარდა იმისა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა უსაფრთხოების დაცვის ვალდებულებას აკისრებს მონაცემთა დამმუშავებელ ორგანიზაციებს და მათ ავალებს მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრას, ის ასევე ადგენს უშუალოდ დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის იმ თანამშრომლის ვალდებულებას, რომელიც მონაწილეობს მონაცემთა დამუშავებაში ან რომელსაც აქვს მონაცემებზე წვდომა, რომ არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ.

ამასთან, გასათვალისწინებელია, რომ მონაცემთა უსაფრთხოების დაცვა უზრუნველყოფილია პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლის მხრიდანაც და დადგენილი სტანდარტია, რომ იგი საიდუმლოებისა და კონფიდენციალობის სრული დაცვით ახორციელებს საქმიანობას. აღნიშნული დადგენილია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის 51-ე მუხლით, რომლის თანახმად, „პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომელი ვალდებულია დაიცვას ნებისმიერი სახის საიდუმლოების შემცველი ინფორმაციის უსაფრთხოება და არ გაამჟღავნოს საიდუმლო ინფორმაცია, რომელიც მისთვის სამსახურებრივი მოვალეობის შესრულების დროს გახდა ცნობილი. ეს ვალდებულება

პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომელს უფლებამოსილების შეწყვეტის შემდეგაც უნარჩუნდება.“ აღნიშნული ვალდებულება ასევე დადგენილია „პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 1 მარტის №34 ბრძანებით.[12]

9. ინკვიზიციურობა

ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოების ერთ-ერთი მთავარი თავისებურება საქმის განმხილველი ორგანოს მიერ ინკვიზიციურობის პრინციპის შესაბამისად მოქმედებაა. მიუხედავად იმისა, რომ ადმინისტრაციულ სამართალდარღვევათა კოდექსით ინკვიზიციურობის პრინციპი ცალსახად არ არის განსაზღვრული, ადმინისტრაციული სამართალწარმოებისთვის იგი უცხო არაა.

ზოგადად, ინკვიზიციურობის პრინციპი გულისხმობს, საქმის განმხილველი უფლებამოსილი ორგანოს მხრიდან ადმინისტრაციული სამართალდარღვევის საქმის წარმოების დაწყებას და საკუთარი ინიციატივით გამოკვლევას. ამასთან, ხსენებული ორგანო აფასებს, როგორც პირის სამართალდარღვევის ჩადენაში მამხილებელ, აგრეთვე შესაბამისი პასუხისმგებლობისგან განმათავისუფლებელ გარემოებებს და ვალდებულია ორივე გარემოება შეაფასოს ობიექტურად.[13]

მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ ინკვიზიციურობის პრინციპის გამოყენება დარგისათვის დამახასიათებელი ერთ-ერთი მთავარი თავისებურებაა და ასახულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-7 თავში, რომელიც ადგენს პერსონალურ მონაცემთა დაცვის სამსახურის უფლებამოსილებებს მონაცემთა დაცვის სფეროსა დაფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის სფეროში.

მონაცემთა დაცვის სფეროში პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის ძირითადი მიმართულება პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლაა. პერსონალურ მონაცემთა დაცვის სამსახური უფლებამოსილია არა მხოლოდ დაინტერესებული პირის განცხადების საფუძველზე, არამედ საკუთარი ინიციატივითაც განახორციელოს ნებისმიერი დამუშავებისთვის პასუხისმგებელი პირის ან/და დამუშავებაზე უფლებამოსილი პირის შემოწმება[14], რაც პირდაპირ განსაზღვრავს სამსახურის მხრიდან მონაცემთა დამუშავების კანონიერების

[12] „პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 1 მარტის №34 ბრძანების მე-10 მუხლის მესამე პუნქტის „გ“ ქვეპუნქტი.

[13] *Bohnert J.,* Ordnungswidrigkeitenrecht, 4th ed. 2010, 5.

[14] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 51-ე მუხლის პირველი პუნქტი.

შესაფასებლად აქტიური ჩართულობისა და ინკვიზიციურობის უფლებამოსილებას. შესაბამისად, სამსახური არა თუ მხოლოდ კონკრეტული მომართვის ან გავრცელებული ინფორმაციის საფუძველზე, საკუთარი ინიციატივით იწყებს ადმინისტრაციული სამართალდარღვევის საქმის წარმოებას არამედ, ყოველი წლის დასაწყისში სამსახურის უფროსის ბრძანებით მტკიცდება წლის მანძილზე ჩასატარებელი შემოწმებების გეგმა, რომლის შემუშავების და სამსახურის უფროსისათვის წარდგენის ვალდებულება გააჩნია სამსახურის გეგმური ინსპექტირების დეპარტამენტს, რომელიც 2023 წელს შეიქმნა და მხოლოდ გასულ წელს მონაცემთა დამუშავების კანონიერების 83 გეგმური შემოწმება განახორციელა[15].

აღსანიშნავია, რომ შემოწმებების წლიური გეგმის შემუშავების მიზანს წარმოადგენს ყოველდღიურ ცხოვრებაში მონაცემთა დამუშავების პროცესების მრავალფეროვნების, დინამიკურობისა და კომპლექსურობის პირობებში სამსახურის საქმიანობის ეფექტიანობისა და თანამიმდევრულობის უზრუნველყოფა. წლიური გეგმა დგება მონაცემთა დამუშავების კანონმდებლობისა და პრაქტიკის შესწავლის გზით, საქართველოს სხვადასხვა რეგიონებში პრიორიტეტული და მაღალრისკიანი სფეროების/მონაცემთა დამუშავების პროცესების გამოკვეთისა და ამ პროცესებისთვის დამახასიათებელი რისკების ანალიზის შედეგების საფუძველზე, რაც ემსახურება სამსახურის რესურსების მიზნობრივ და ეფექტიან გამოყენებას.[16]

ინკვიზიციურობის პრინციპის გამოვლინება ასევე სახეზეა არაგეგმური ინსპექტირებების ჩატარების ნაწილშიც, რადგან ის ამა თუ იმ მონაცემთა დამუშავების კანონიერების პროცესის შესწავლის მიზნით სამსახურის ინიციატივის საფუძველზე ხორციელდება და ხაზგასასმელია რომ 2024 წელს 182 არაგეგმური ინსპექტირება იქნა ჩატარებული.[17]

10. განმეორებით სახდელის დაკისრების აკრძალვის პრინციპი ("ne bis in idem")

სამართალდამრღვევის ორმაგად დასჯის საფრთხე პრაქტიკაში საკმაოდ რეალურია, თუმცა აღნიშნული ცალსახად ეწინააღმდეგება ადამიანის საყოველთაოდ აღიარებულ უფლებებს. დამრღვევის ორმაგად დასჯა ერთი მართლსაწინააღმდეგო ქმედების ჩადენისთვის დაუშვებელია არამხოლოდ მისთვის სხვადასხვა სამართლის დარგებით (მაგალითად, სისხლის სამართლის და ადმინისტრაციულ სამართალდარღვევათა კოდექსებით)

[15] პერსონალურ მონაცემთა დაცვის სამსახური. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის საქმიანობის ანგარიში. <https://pdps.ge/ka/content/988/angariSebi> [10.02.2025].
[16] პერსონალურ მონაცემთა დაცვის სამსახური. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის საქმიანობის ანგარიში. <https://pdps.ge/ka/content/988/angariSebi> [10.02.2025].
[17] პერსონალურ მონაცემთა დაცვის სამსახური. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 12 თვის საქმიანობის სტატისტიკა. ხელმისაწვდომია: https://pdps.ge/ka/content/988/angariSebi [10.02.2025].

გათვალისწინებული პასუხისმგებლობის ზომების შეფარდებით, არამედ იგი ასევე გულისხმობს პირისთვის სახდელის დაკისრების შემდეგ, განმეორებით, თუნდაც იგივე დარგით გათვალისწინებული სახდელის დაკისრების აკრძალვას.

დამრღვევის განმეორებით დასჯის ამკრძალავი - *"ne bis in idem"* პრინციპი ასახულია ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის მე-7 დამატებითი ოქმის მე-4 მუხლის პირველ ნაწილში, რომლის თანახმად, დაუშვებელია სისხლის სამართლის წესით პირის ხელმეორედ გასამართლება ან დასჯა ერთი და იმავე სახელმწიფოს იურისდიქციის ფარგლებში იმ დანაშაულისათვის, რომლისთვისაც იგი ერთხელ უკვე იქნა საბოლოოდ გამართლებული ან მსჯავრდებული ამ სახელმწიფოს კანონისა და სისხლის სამართლის პროცედურის შესაბამისად.[18]

ზემოაღნიშნულ მიდგომას იზიარებს საქართველოს კანონმდებლობაც. კერძოდ, საქართველოს კონსტიტუციის 42-ე მუხლის მე-4 პუნქტის თანახმად, არავის შეიძლება განმეორებით დაედოს მსჯავრი ერთი და იმავე დანაშაულისათვის. ხსენებული კონსტიტუციური დებულება განამტკიცებს განმეორებითი დასჯის აკრძალვის კონსტიტუციურ პრინციპს. გასათვალისწინებელია ისიც, რომ კონსტიტუციის აღნიშნული დანაწესი იმპერატიული ხასიათისაა და რაიმე გამონაკლისს ამ გარანტიის შეზღუდვის თვალსაზრისით არ ითვალისწინებს.

ამასთან, გასათვალისწინებელია, რომ საქართველოს საკონსტიტუციო სასამართლოს არაერთხელ აქვს დაფიქსირებული თავისი პოზიცია *"ne bis in idem"* პრინციპის შესახებ, რომელმაც განმარტა, რომ აღნიშნული პრინციპი ერთი მხრივ იცავს ინდივიდს ერთი და იმავე ქმედების გამო განმეორებითი სისხლისსამართლებრივი დევნისა და მსჯავრდებისგან, მეორე მხრივ კი, ემსახურება სისხლისსამართლებრივი მართლმსაჯულების პროცესში მიღებული საბოლოო გადაწყვეტილებებით სახელმწიფო ორგანოების ბოჭვას.[19]

განმეორებითი მსჯავრდების აკრძალვა სამართლებრივი სახელმწიფოს ფუნდამენტური პრინციპის არსებითი გამოვლინებაა, კერძოდ, სისხლისსამართლებრივი მართლმსაჯულების პროცესში სახელმწიფო ორგანოების ბოჭვა, მათ მიერვე მიღებული საბოლოო გადაწყვეტილებებით, არ განახორციელონ ერთი და იმავე ქმედებისათვის პირის განმეორებითი დევნა, პირდაპირ უკავშირდება სამართლებრივი განსაზღვრულობისა და

[18] ადამიანის უფლებათა ევროპული კონვენცია, 1950.
ხელმისაწვდომია: <https://www.echr.coe.int/Documents/Convention_KAT.pdf> [10.02.2025].

[19] საქართველოს საკონსტიტუციო სასამართლოს 2015 წლის 29 სექტემბრის №3/1/608,609 გადაწყვეტილება საქმეზე „საქართველოს უზენაესი სასამართლოს კონსტიტუციური წარდგინება საქართველოს სისხლის სამართლის საპროცესო კოდექსის 306-ე მუხლის მე-4 ნაწილის კონსტიტუციურობის თაობაზე და საქართველოს უზენაესი სასამართლოს კონსტიტუციური წარდგინება საქართველოს სისხლის სამართლის საპროცესო კოდექსის 297- ე მუხლის „ზ“ ქვეპუნქტის კონსტიტუციურობის თაობაზე“, II-35 https://matsne.gov.ge/ka/document/view/3017013?publication=0 [10.02.2025].

უსაფრთხოების პრინციპებს. ინდივიდის უფლებაშემზღუდავი კანონმდებლობით გათვალისწინებული სამართლებრივი შედეგის განჭვრეტადობა, მისი სამართლებრივი განსაზღვრულობის ხარისხი მნიშვნელოვნად არის დამოკიდებული იმაზე, თუ რამდენად და რა ფარგლებში ხდება მართლმსაჯულების პროცესში მიღებული საბოლოო ხასიათის გადაწყვეტილებების პატივისცემა. „თუ პირს კანონით დადგენილი პასუხისმგებლობა ერთი ქმედებისთვის რამდენჯერმე შეიძლება დაეკისროს და ხელისუფლება არ იზღუდება ამ მიმართებით, იმპერატიული მოთხოვნა, რომ პირმა წინასწარ იცოდეს, რა სასჯელი დაეკისრება კონკრეტული ქმედებისთვის და შეეძლოს საკუთარი ქცევის შესაბამისად კონტროლი, თავისთავად აზრს მოკლებული ხდება.[20]

ადმინისტრაციულ სამართალდარღვევათა ჭრილში, *“ne bis in idem”* პრინციპის არსებობის მხრივ, საგულისხმოა, რომ გერმანიის ადმინისტრაციულ სამართალდარღვევათა კანონმდებლობის მიხედვით, განმეორებით დევნის აკრძალვა მოქმედებს აგრეთვე ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოებისას.[21]

საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსის 232-ე მუხლის თანახმად კი, ადმინისტრაციული სამართალდარღვევის საქმის წარმოება არ შეიძლება დაიწყოს, ხოლო დაწყებული საქმე უნდა შეწყდეს თუ არსებობს იმავე ფაქტზე ადმინისტრაციულ პასუხისგებაში მიცემული პირის მიმართ კომპეტენტური ორგანოს (თანამდებობის პირის) დადგენილება ადმინისტრაციული სახდელის დადების შესახებ ან ამხანაგური სასამართლოს გაუუქმებელი გადაწყვეტილება, თუ მასალები ამხანაგურ სასამართლოს გადასცა იმ ორგანომ (თანამდებობის პირმა), რომელსაც აქვს მოცემულ საქმეზე ადმინისტრაციული სახდელის დადების უფლება, ან გაუუქმებელი დადგენილება ადმინისტრაციული სამართალდარღვევის საქმის შეწყვეტის შესახებ, აგრეთვე ამავე ფაქტზე სისხლის სამართლის საქმის არსებობისას.

აღსანიშნავია, რომ ზემოთ ხსენებული პრინციპი, პირდაპირ არის გათვალისწინებული „პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 1 მარტის №34 ბრძანებაში, რომლის მე-18 მუხლის პირველი პუნქტის მიხედვით მონაცემთა დამუშავების კანონიერების შესწავლის გამომრიცხავი გარემოებებია:

- სასამართლოს გადაწყვეტილების ან განჩინების არსებობა იმავე დარღვევის ფაქტზე და იმავე მხარეებთან დაკავშირებით, რაზეც უნდა დაიწყოს ან მიმდინარეობს მონაცემთა დამუშავების კანონიერების შესწავლა;

[20]საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 29 დეკემბრის №2/7/636 გადაწყვეტილება. <https://matsne.gov.ge/ka/document/view/3544820?publication=0> [10.02.2025]
[21] *Bohnert J.,* Ordnungswidrigkeitenrecht, 4th ed. 2010, 5.

- სამსახურის მიერ მიღებული გადაწყვეტილების არსებობა იმავე ფაქტზე და იმავე მხარეებთან დაკავშირებით, რაზეც უნდა დაიწყოს ან მიმდინარეობს მონაცემთა დამუშავების კანონიერების შესწავლა;
- სისხლის სამართლის საქმის არსებობა იმავე ფაქტზე, რაზეც უნდა დაიწყოს ან მიმდინარეობს მონაცემთა დამუშავების კანონიერების შესწავლა.

11. დასკვნა

სტატიაში განხილულ იქნა პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში ადმინისტრაციულ სამართალდარღვევათა საქმის წარმოების ძირითადი პრინციპები, რომელთა გათვალისწინება უზრუნველყოფს მონაცემთა სუბიექტის უფლებების დაცვის მიზნით ხსენებული წარმოების სათანადოდ წარმართვას.

კანონიერების პრინციპის განსაზღვრავს საქმის წარმოებისას თითოეული მოქმედების ზუსტ შესაბამისობას კანონით განსაზღვრულ სტანდარტებთან, რომელთა დაცვის გარეშე შეუძლებელია წარმოების შესაბამისობის უზრუნველყოფა ეროვნულ კანონმდებლობით და საერთაშორისო სტანდარტებით დადგენილ ნორმებთან.

ადამიანის უფლებათა და თავისუფლებათა დაცვის პრინციპის დაცვა მნიშვნელოვანია არა მხოლოდ პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში, არამედ აღნიშნული სამართლებრივი სახელმწიფოს ფუნქციონირების ერთ-ერთი ძირითადი პრინციპია.

დამოუკიდებლობისა და პოლიტიკური ნეიტრალიტეტის პრინციპი არის მთავარი გარანტორი იმისა, რომ პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესი თავისუფალია რაიმე სახის ზეგავლენისგან, რაც აუცილებელია სამართლიანობისა და გამჭვირვალობისთვის.

ობიექტურობისა და მიუკერძოებლობის პრინციპების დაცვა მიღების პროცესში გამორიცხავს მიკერძოებული გადაწყვეტილებების მიღებას და სამართლიანი ადმინისტრაციული წარმოების ჩატარების მნიშვნელოვან გარანტიას წარმოადგენს.

თანაზომიერების პრინციპი უზრუნველყოფს, რომ საქმეზე მიღებული გადაწყვეტილებები იქნება პროპორციული და შესაბამისი მონაცემთა სუბიექტის უფლებების დაცვის მიზნით. ის ასევე გამორიცხავს უფლებამოსილების გადამეტების რისკს და უზრუნველყოფს, რომ საჯარო ინტერესები მაქსიმალურად იქნეს დაბალანსებული ინდივიდის უფლებებთან მიმართებით.

კანონის წინაშე თანასწორობის პრინციპი განსაზღვრავს, რომ ყველა პირი უნდა სარგებლობდეს თანაბარი უფლებებით და ვალდებულებებით, მიუხედავად სოციალური, სამართლებრივი ან სხვა მახასიათებლებისა. ადმინისტრაციული სამართალდარღვევათა საქმის წარმოებისას თანასწორობის დაცვა უზრუნველყოფს, რომ გადაწყვეტილებები

ეფუძნებოდეს მხოლოდ სამართლებრივ საფუძვლებს და არ იქნეს მიღებული რაიმე სახის უსამართლო მიდგომის შედეგად.

საიდუმლოების და კონფიდენციალურობის დაცვის უზრუნველყოფა მონაცემთა დამუშავების პროცესის განუყოფელი ნაწილია ასევე საქმის წარმოების დასრულების შემდეგაც და როგორც აღინიშნა, აღნიშნული ვალდებულება აკისრიათ როგორც დამუშავებაზე პასუხისმგებელი პირების, ასევე პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლებსაც.

ინკვიზიციურობის პრინციპი ხაზს უსვამს ადმინისტრაციული ორგანოს ვალდებულებას, რომ ის არ შემოიფარგლოს მხოლოდ სუბიექტის მიერ მოწოდებული ინფორმაციით თუ დოკუმენტაციით და თავადაც აქტიურად შეისწავლოს საქმისათვის არსებითი მნიშვნელობის მქონე ყველა ფაქტობრივი გარემოება.

განმეორებითი სახდელის დაკისრების აკრძალვის პრინციპი გულისხმობს, რომ ერთსა და იმავე სამართალდარღვევისთვის პირი არ შეიძლება ორჯერ დაეკისროს ადმინისტრაციულ პასუხისმგებლობაა. ეს პრინციპი მნიშვნელოვანია სამართლებრივი გარემოს უზრუნველსაყოფად, რათა მოქალაქეებს ჰქონდეთ გარანტია, რომ მათ არ დაეკისრებათ ზედმეტი და არამართლზომიერი სანქციები. მისი დაცვა აუცილებელია როგორც კონსტიტუციური პრინციპების დაცვისთვის, ასევე ადმინისტრაციული საქმის წარმოების ლეგიტიმურობის შესანარჩუნებლად.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, ნათელია რომ სტატიაში განხილული თითოეული პრინციპის ზედმიწევნით დაცვა უზრუნველყოფს ადმინისტრაციული სამართალდარღვევათა საქმის წარმოების ეფექტიანობასა და კანონიერი გადაწყვეტილებების მიღებას, რომლის გარეშეც შეუძლებელია დაცული იყოს მონაცემთა სუბიექტის უფლებები.

ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, 24/08/1995.
2. საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსი, 15/12/1984.
3. საქართველოს სისხლის სამართლის კოდექსი, 13/08/1999.
4. ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია;
5. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023.
6. „პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 1 მარტის №34 ბრძანება.
7. *ტურავა პ. წკეპლაძე ნ.,* ზოგადი ადმინისტრაციული სამართლის სახელმძღვანელო, 2010.
8. პერსონალურ მონაცემთა დაცვის სამსახური, ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”) - ქართული თარგმანი.
9. პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის საქმიანობის ანგარიში.
10. პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 12 თვის საქმიანობის სტატისტიკა.
11. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 29 დეკემბრის გადაწყვეტილება საქმეზე: №2/7/636.
12. საქართველოს საკონსტიტუციო სასამართლოს 2015 წლის 29 სექტემბრის გადაწყვეტილება საქმეზე №3/1/608,609.
13. *Bohnert J., Bülte J.,* Ordnungswidrigkeitenrecht. 5. Auflage. 2016.
14. *Detterbeck S.,* Allgemeines Verwaltungsrecht, 2004.
15. European Data Protection Supervisor, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*,* 2021.

სერგი ჯორბენაძე*

პერსონალურ მონაცემთა დამუშავების ფარგლები საადვოკატო საქმიანობის განხორციელებისას

ადვოკატი პროფესიული საქმიანობისას ამუშავებს სხვადასხვა ინფორმაციას, რაც გულისხმობს პერსონალურ მონაცემებთან წვდომის მაღალ ალბათობას. მეტიც, უმეტეს შემთხვევაში ეს შეიძლება იყოს განსაკუთრებული კატეგორიის პერსონალური მონაცემებიც, რა დროსაც, ადვოკატს სიფრთხილე და კანონთან შესაბამისი ქმედება მართებს. ერთმანეთისგან გასამიჯნია პირადი და სამსახურებრივი მიზნით მონაცემთა დამუშავების საკითხი, ასევე, უსაფრთხოების დაცვა, თუ კლიენტის ინტერესის გათვალისწინება.

ვინაიდან საადვოკატო საქმიანობა არ ნიშნავს შეუზღუდავ უფლებამოსილებას, ადვოკატის მიერ პერსონალურ მონაცემთა არასათანადო დამუშავებამ შესაძლებელია, რომ ერთგვარი ჯაჭვური რეაქცია გამოიწვიოს. კერძოდ, კონკრეტული ქმედებით შეიძლება დაირღვეს პერსონალურ მონაცემთა დამუშავების წესი და ასევე, პროფესიული სტანდარტი.

წინამდებარე ნაშრომი ეხება დადგენილი პრაქტიკის შეჯერებასა და ანალიზს, რომლის ფარგლებშიც წარმოდგენილია (საადვოკატო საქმიანობასთან მიმართებით) პერსონალურ მონაცემთა დამუშავების კანონიერებისა თუ სტანდარტის დარღვევის ცალკეული შემთხვევები.

საკვანძო სიტყვები: *ადვოკატი, პერსონალური მონაცემები, მონაცემთა დამუშავება, პროფესიული სტანდარტი.*

* სამართლის დოქტორი, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასოცირებული პროფესორი, ადვოკატი.

1. შესავალი

ადვოკატს თავისი პროფესიული საქმიანობის განხორციელებისას ხშირად უწევს პერსონალურ მონაცემებთან შეხება. ეს შეიძლება იყოს როგორც თავისი მარწმუნებლის, ისე – მოწინააღმდეგე მხარის მონაცემები. ამ მხრივ, ადვოკატი (ისევე, როგორც, მისი მარწმუნებელი) დაცულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტით, რომელიც სამართალწარმოების მიზნებისთვის პასუხისმგებლობისგან ათავისუფლებს პირს. თუმცა, აღნიშნული ისე არ უნდა იქნეს გაგებული, რომ ადვოკატს პერსონალურ მონაცემთა დამუშავების თვალსაზრისით აბსოლუტური თავისუფლება გააჩნია. პირიქით, მისმა ქმედებამ, თუნდაც იგი კლიენტის ინტერესისკენ იყოს მიმართული, შეიძლება რომ დაარღვიოს ზემოთ დასახელებული კანონი.

საქართველოში საინტერესო პრაქტიკა დამკვიდრდა პერსონალურ მონაცემთა დაცვასთან დაკავშირებით. ამ მხრივ, გვხვდება არაერთი შემთხვევა, როდესაც პერსონალურ მონაცემთა დაცვის სამსახურს (შემდგომში – სამსახური) განხილული აქვს ცალკეული განცხადებები და დადგენილი აქვს სამართალდარღვევის ფაქტები. წინამდებარე ნაშრომი უპირატესად სწორედ სამსახურის პრაქტიკას დაეფუძნება, რომელიც არაერთ საინტერესო პრეცედენტს იცნობს. წინდაწინ უნდა აღინიშნოს ორი ასპექტი: ა) სტატიის მიზნებისთვის გამოთხოვილ იქნა საჯარო ინფორმაცია სამსახურიდან. შესაბამისად, სამსახურის გადაწყვეტილებების გასაჩივრების შემთხვევები მასში არაა განხილული[1] და ბ) მიუხედავად საკანონმდებლო ცვლილებისა,[2] ძირითადი არსი, რაც თუნდაც უკვე ძალადაკარგული კანონის[3] საფუძველზე მიღებულ გადაწყვეტილებებშია მოცემული, ახალი კანონის ფარგლებშიც გაზიარებულია.[4]

[1] ამდენად, დასაშვებია, რომ სასამართლო პრაქტიკით განსხვავებულ მიდგომასაც ჰქონდეს ადგილი.

[2] იგულისხმება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომელიც მიღებულია 2023 წლის 14 ივნისს, ხოლო, გამოქვეყნებულია 2023 წლის 3 ივლისს (დოკუმენტის ნომერი: 3144-XIმს-Xმპ, სარეგისტრაციო კოდი: 010100000.05.001.020936) და წინამდებარე სტატიის გამოქვეყნებისას სრულადაა ამოქმედებული.

[3] იგულისხმება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომელიც მიღებულია 2011 წლის 28 დეკემბერს, გამოქვეყნებულია 2012 წლის 16 იანვარს, ხოლო, ძალის დაკარგვის თარიღია 2024 წლის 1 მარტი (დოკუმენტის ნომერი: 5669-რს, სარეგისტრაციო კოდი: 010100000.05.001.016606).

[4] ახალი კანონი კიდევ უფრო მეტადაა დაახლოებული დასავლურ სტანდარტებთან, ასევე, მასში გაზიარებულია ძველი კანონით მოქმედი არსებითი საკითხები/პრინციპები.

2. ზოგადად ადვოკატის საქმიანობის ფარგლების შესახებ და მისი მიმართება პერსონალურ მონაცემთა დაცვასთან

„ადვოკატთა შესახებ“ საქართველოს კანონის პირველი მუხლის მე-2 პუნქტით, ადვოკატი ემორჩილება კანონსა და პროფესიული ეთიკის ნორმებს. ამავე კანონის 36-ე მუხლით, „ადვოკატს სამართალდარღვევის ჩადენისათვის დაეკისრება პასუხისმგებლობა საქართველოს კანონმდებლობით დადგენილი საერთო წესით“. აღნიშნული ჩანაწერი არ შემოფარგლავს ადვოკატის პასუხისმგებლობას მხოლოდ პროფესიული ეთიკის კოდექსით, რაც თავის თავში გულისხმობს, მაგალითად, პერსონალურ მონაცემთა დაცვის ნორმათა უგულებელყოფას თუ სხვა სამართალდარღვევებს.[5] აღნიშნულის საილუსტრაციოდ გამოდგება შემდეგი: კლიენტის ინტერესის გათვალისწინებით, მასთან ურთიერთობისას დავალების ხელშეკრულებით განსაზღვრულ ვალდებულებათა შესრულება,[6] მათ შორის, დოკუმენტაციის მიწოდება თუ საკითხის თაობაზე კლიენტის საქმის კურსში ჩაყენება, არ წარმოადგენს ადვოკატის მხრიდან რაიმე სახის გადაცდომას. თუმცა მნიშვნელოვანია ის, თუ რა გზით მოიპოვებს ადვოკატი ამგვარ ინფორმაციას და როგორ აწვდის მას მარწმუნებელს. ამ მხრივ შეიძლება ყველაზე გავრცელებული მაგალითის განხილვა, რომელიც საჯარო ინფორმაციის გამოთხოვას ეხება: მიუხედავად კონსტიტუციით გარანტირებული უფლებისა, მნიშვნელოვანია, რომ ასეთი ინფორმაციის გამოთხოვის თაობაზე შესაბამისი განცხადების შინაარსი არ იყოს პერსონალურ მონაცემთა დამრღვევი. პრაქტიკაში გვხვდება პრეცედენტი, როდესაც ადვოკატმა მიმართა შესაბამის ორგანოს და მოითხოვა გარკვეული ინფორმაციის მისგან მიღება. განცხადებას დაურთო სასამართლოში არსებული დავის ფარგლებში მოწინააღმდეგე მხარის მიერ წარდგენილი დოკუმენტაცია, რომელიც შეიცავდა პირთა პერსონალურ მონაცემებს. სამსახურის მხრიდან ასეთი დოკუმენტაციის წარდგენის გათვალისწინებით დადგინდა დარღვევა.[7]

რა თქმა უნდა, მოყვანილი მაგალითი არ ნიშნავს, რომ ადვოკატს არ შეუძლია გამოითხოვოს საჯარო ინფორმაცია. პირიქით, მას შეუძლია მოთხოვნა დააყენოს მისთვის სასურველი შინაარსით და მოთხოვნილი ინფორმაცია შეიძლება პირის პერსონალურ მონაცემებსაც შეეხებოდეს. ასეთი ქმედება *a priori* არ გულისხმობს ადვოკატის მიერ უფლების დარღვევას.[8] ამ თვალსაზრისით საინტერესო შემთხვევა გვხვდება პრაქტიკაში, როდესაც ადვოკატმა გამოითხოვა საჯარო ინფორმაცია, რომელიც არასრულწლოვანს

[5] შესაბამისად, თითოეული დარღვევის პროპორციულად შეიძლება დადგეს ნეგატიური სამართლებრივი შედეგი ადვოკატისთვის.

[6] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 5 მარტის №გ-1/046/2024 გადაწყვეტილება.

[7] პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 30 ივნისის №გ-1/149/2023 გადაწყვეტილება.

[8] ადვოკატის სურვილს შეიძლება წარმოადგენდეს სასამართლოში დამატებით მტკიცებულებად ასეთი ინფორმაციის წარდგენა. იხ. პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 6 ოქტომბრის №გ-1/130/2022 გადაწყვეტილება – ის, თუ რამდენად მიიღებს სასამართლო ამ გზით მოპოვებულ მტკიცებულებას, ცალკე დავისა და განხილვის საგანია და სცდება სამსახურის კომპეტენციას.

ეხებოდა.[9] საჯარო დაწესებულებამ კი მას იმგვარად მიაწოდა აღნიშნული ინფორმაცია, რომ შესაბამისი თანხმობა მიღებული არ ჰქონდა მონაცემთა შესაბამისი სუბიექტისგან.[10] შესაბამისად, საჯარო დაწესებულებამ არ დაიცვა კანონმდებლობა და სამსახურის მიერ მას დაუდგინდა სამართალდარღვევა.[11]

3. პირადი მიზნის გამიჯვნა სამსახურებრივი მოვალეობის შესრულებისგან

ის, რაც შეიძლება წარმოადგენდეს კლიენტის პირად მიზანს, ვერ იქნება ადვოკატის პირად მიზნად მიჩნეული. მაგალითად, თუ ადვოკატის მხრიდან დარღვევას ექნება ადგილი მაშინ, როდესაც იგი გაავრცელებს კონკრეტული საქმის დეტალებს პირთა იდენტიფიცირების შესაძლებლობით,[12] იდენტური ქმედებისთვის მსგავსი შედეგი უპირობოდ არ დადგება კლიენტისთვის.[13] რა თქმა უნდა, აუცილებლად გამოსაკვლევი საკითხია, რომ ნამდვილად იკვეთება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის რომელიმე წინაპირობა[14]/კანონიერი ინტერესი.[15]

4. კლიენტის ინტერესებიდან გამომდინარე მოქმედების ფარგლები

კლიენტის ინტერესის დაცვა ადვოკატის უპირატესი პრინციპია, რომელიც ადვოკატმა კანონმდებლობის შესაბამისად უნდა განახორციელოს.[16] „ადვოკატთა შესახებ“ საქართველოს კანონის მე-6 მუხლის პირველი პუნქტის მიხედვით, „ადვოკატს უფლება აქვს კლიენტის ინტერესების დასაცავად გამოიყენოს ყველა საშუალება, რომელიც აკრძალული არ არის კანონმდებლობით ან პროფესიული ეთიკის ნორმებით“. შესაბამისად, კლიენტის დაცვა უნდა მოხდეს იმგვარად, რომ არ დაირღვეს კანონმდებლობა. ეს კი ნიშნავს შემდეგს: თუ ადვოკატის მხრიდან რაიმე გადაცდომას ექნება ადგილი, მას დაეკისრება პასუხისმგებლობა ამ გადაცდომის მომწესრიგებელი ნორმებიდან გამომდინარე.[17]

---

[9] არასრულწლოვანთან დაკავშირებით სპეციალური წესია გათვალისწინებული კანონმდებლობით და საკითხიც განსხვავებულადაა წარმოჩენილი. ამ საკითხზე იხ. *ხუბულია ნ.,* არასრულწლოვნის პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული გამოწვევები, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი №1, 2024, 62-71.

[10] არც კანონიერი წარმომადგენლისგან და ლოგიკურად, არც არასრულწლოვნისგან.

[11] პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 20 თებერვლის №გ-1/024/2023 გადაწყვეტილება.

[12] მსჯელობისთვის იხ. პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 5 აგვისტოს №გ-1/081/2022 გადაწყვეტილება.

[13] ცალკეულ გარემოებებთან ერთობლიობის გათვალისწინებით. იხ. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 21 აპრილის №გ-1/137/2020 გადაწყვეტილება.

[14] იხ. სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №გ-1/207/2021 გადაწყვეტილება.

[15] იხ. მაგალითად, სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 28 აპრილის №გ-1/147/2020 გადაწყვეტილება.

[16] იხ. ადვოკატთა პროფესიული ეთიკის კოდექსის მე-5 მუხლი.

[17] ეს შეიძლება იყოს ასევე სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაულიც.

ა. კანონის დარღვევის დაუშვებლობა, თუნდაც დავის გარემოებები მოითხოვდეს შესაბამის აქტივობას

შესაძლებელია, რომ საქმის გარემოებებიდან გამომდინარე იკვეთებოდეს სასამართლოში დამატებითი მტკიცებულებების წარდგენის აუცილებლობა. შესაბამისად, საჭირო იყოს კონკრეტული ორგანოსთვის მიმართვა, საკითხის დაზუსტება და სხვ. ასეთ დროს, მხოლოდ კლიენტის ინტერესებიდან გამომდინარე მოქმედება ვერ გაამართლებს ადვოკატის ქმედებას.[18] მაგალითისთვის შეიძლება სამსახურის თანამედროვე პრაქტიკის მოხმობა, როდესაც ადვოკატმა ერთ-ერთ ორგანოს მიმართა წერილით და მასში მიუთითა კონკრეტულ პირებზე, ასევე, შესაბამისი პირის ოჯახურ მდგომარეობაზე. სამსახურმა ამგვარ ქმედებაზე დაადგინა სამართალდარღვევა.[19] მეტიც, საქმისწარმოების მიმდინარეობისას სამსახურმა ადვოკატს მოსთხოვა მიეწოდებინა მისთვის ინფორმაცია იმის თაობაზე, თუ საიდან დაადგინა ის მონაცემი, რაც წერილში ასახა. მაგალითად, ოჯახური მდგომარეობა/ნათესაური კავშირი – იყო ეს საქმის მასალებიდან გამომდინარე მოპოვებული ინფორმაცია, ქცევის ანალიზის შედეგი, კლიენტის მოსაზრებები თუ რამე სხვა სახის გარემოება, რაც ამგვარი დასკვნის საფუძველს მისცემდა მას. ამასთან, სამსახურმა მოითხოვა ადვოკატისგან, დაესახელებინა ის საშუალება, რა გზითაც ხელმისაწვდომი გახდა მისთვის ინფორმაცია. საინტერესოა, რომ ადვოკატმა არ მიაწოდა სამსახურს ამგვარი ინფორმაცია, რაც საბოლოოდ გადაწყვეტილების მიღების წინაპირობა გახდა.[20]

ბ. ვიდეო-აუდიომონიტორინგი ადვოკატის მიერ

საინტერესო შემთხვევას ვხვდებით პრაქტიკაში, რომელიც საადვოკატო საქმიანობის ფარგლებში იქნა განხორციელებული: ადვოკატის კლიენტს

[18] ვინაიდან, მონაცემთა დამუშავების პრინციპებისა და საფუძვლების ერთობლიობა უნდა იკვეთებოდეს. იხ. მაგალითად, პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 7 აგვისტოს №გ-1/191/2024 გადაწყვეტილება.

[19] პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 7 ივლისის №გ-1/153/2023 გადაწყვეტილება.

[20] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 51-ე მუხლის მე-3 პუნქტით, სამსახურის უფლებამოსილებას განეკუთვნება ინფორმაციის გამოთხოვა. შესაბამისად, აღნიშნული არ ეწინააღმდეგება „ადვოკატთა შესახებ“ საქართველოს კანონის 38-ე მუხლის პირველი პუნქტის მეორე წინადადებასთან: „ადვოკატი საადვოკატო საქმიანობას დამოუკიდებლად ახორციელებს. დაუშვებელია ადვოკატის საქმიანობაში არამართლზომიერი ჩარევა, ადვოკატის საქმიანობისათვის ხელის შეშლა, ადვოკატზე სახელმწიფო ორგანოს ან/და სხვა პირის არასათანადო ზემოქმედება, მისი დაშინება, შევიწროება, იძულება, დევნა, მასზე ზეწოლა, მისთვის მორალური ან/და მატერიალური ზიანის მიყენება, მის მიმართ ძალადობა ან ძალადობის მუქარა, აგრეთვე ნებისმიერი სხვა ქმედება, რომელმაც შეიძლება ხელყოს ადვოკატის დამოუკიდებლობა“. აღნიშნული მსჯელობა მოცემულია გადაწყვეტილებაში.

ჰქონდა სატელეფონო ზარი მოწინააღმდეგე მხარესთან. ამ დროს კლიენტი იმყოფებოდა ადვოკატთან ოფისში. საუბარი მიმდინარეობდა ე.წ. „ხმამაღალ რეჟიმში“[21] და გარშემომყოფებს ესმოდათ იგი. ოთახში, სადაც მიმდინარეობდა საუბარი, ხორციელდებოდა ვიდეო-აუდიომონიტორინგი. მართალია, სივრცეში გამოკრული იყო შესაბამისი აღმნიშვნელი ინფორმაცია, თუმცა, საუბრის მონაწილისთვის ეს გარემოება (ჩაწერა) არ იყო ცნობილი და არც გაფრთხილებული ჰყავდა მხარეს. მხარემ (მაშასადამე, ვისთანაც განხორციელდა ზარი) მოგვიანებით ნახა სასამართლოში წარდგენილ სარჩელში (ფაქტობრივ გარემოებაში), რომ მითითება იყო საუბარზე, რომლის ჩაწერაც არ იყო შეთანხმებული მასთან. შესაბამისად, სამსახურის მიერ დადგინდა სამართალდარღვევა, მათ შორის, პერსონალურ მონაცემთა არასათანადო თანადამუშავებისთვის.[22]

გ. შენახვის კანონიერება

ადვოკატის მხრიდან შეხვედრის (კრების) ჩაწერა, შენახვა და გამჟღავნება ისე, რომ არ ჰქონდეს მიღებული მონაცემთა სუბიექტისგან თანხმობა, კანონდარღვევას წარმოადგენს. ამ მხრივ გვხვდება პრაქტიკაში შემთხვევა, როდესაც აქციონერთა კრების ჩაწერა მოხდა იმგვარად, რომ თანხმობა არ განუცხადებიათ დამსწრე აქციონერებს, ხოლო, შემდეგ ეს ჩანაწერი გამჟღავნდა.[23] ამ ორი ქმედებისთვის სამართალდარღვევას არ ჰქონია ადგილი ხანდაზმულობის გამო, თუმცა, ქმედებისთვის, რომელსაც დენადი ხასიათი გააჩნდა, საადვოკატო ბიუროს პასუხისმგებლობა დაეკისრა. საუბარი ეხება ამავე (მაშასადამე, თანხმობის გარეშე გაკეთებული) ჩანაწერის შენახვას. სამსახურის პოზიციით, პროცესუალური მიზნებისთვის მტკიცებულებათა კანონიერების საკითხის შესწავლა სცდება მის კომპეტენციას, თუმცა თუ საადვოკატო ბიუროს პოზიცია იქნებოდა ამ მტკიცებულების წარდგენა სასამართლოში, მხოლოდ სამართალწარმოების მიზნით უნდა მომხდარიყო ჩანაწერის დამუშავება. ამის შემდგომ კი აუცილებლად უნდა მომხდარიყო ჩანაწერის დაუყოვნებლივი წაშლა, რასაც არ ჰქონდა მოცემულ შემთხვევაში ადგილი.

5. კავშირი პროფესიული ეთიკის სტანდარტებთან

პერსონალური მონაცემების დარღვევასთან ერთად ადვოკატის ქმედებამ შეიძლება დაარღვიოს პროფესიული ეთიკის კოდექსით გათვალისწინებული ვალდებულებანი. მაგალითად, საჯაროდ გაავრცელოს ინფორმაცია

[21] ინგლისურად: “Loudspeaker”.
[22] პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 14 აგვისტოს №გ-1/198/2024 გადაწყვეტილება.
[23] პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 6 ოქტომბრის №გ-1/130/2022 გადაწყვეტილება.

კოლეგაზე,[24] ისევე, როგორც – მოწინააღმდეგე მხარეზე[25] და შეურაცხყოფა მიაყენოს მას.[26] ასეთ დროს, პროფესიული სტანდარტის ფარგლებში ცალკე მოხდება ადვოკატის ქმედების შეფასება, ხოლო, თუ პირთა იდენტიფიცირებით იგი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონსაც არღვევს, მაშინ, სამსახურის მხრიდან დამოუკიდებლად შეფასდება საკითხი.[27]

საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისია ადვოკატის მხრიდან პროფესიული ეთიკის კოდექსის დარღვევის საკითხს დამოუკიდებლად სწავლობს. სწორედ ეთიკის კომისიის საქმიანობასთან დაკავშირებით განიხილა სამსახურმა შემდეგი საქმე: ეთიკის კომიისიის თავმჯდომარემ ერთ-ერთ კოლეგიას წერილით აცნობა, რომ მათ მიერ განსახილველი საქმის მსგავსი საქმე სხვა კოლეგიაში მიმდინარეობდა და რომ აღნიშნული გაეთვალისწინებინა ადრესატ კოლეგიას. ადვოკატმა მიმართა სამსახურს და მიიჩნია, რომ ადგილი ჰქონდა კანონდარღვევას ამგვარი ინფორმაციის მიწოდების გამო. სამსახურის გადაწყვეტილებით, სამართალდარღვევა არ დაფიქსირებულა, ვინაიდან ეთიკის კომისიის თავმჯდომარეს კანონმდებლობით შეეძლო განეხორციელებინა აღნიშნული ქმედება, რაც მის კომპეტენციაში ექცეოდა.[28]

6. მონაცემთა დეპერსონალიზაცია ადვოკატის მიერ

მონაცემთა დეპერსონალიზაცია მონაცემთა სუბიექტის დასაცავად მნიშვნელოვან გარანტიას წარმოადგენს.[29] აღნიშნულში იგულისხმება მონაცემთა იმგვარი დამუშავება, როდესაც მონაცემთა სუბიექტის იდენტიფიცირებაა შესაძლებელი ან ასეთი იდენტიფიცირება არაპროპორციულად დიდ ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს. ამგვარი საკანონმდებლო დათქმა („პერსონალურ მონაცემთა დაცვის შესახებ“

[24] საჯაროდ კოლეგის მიმართ კანონსაწინააღმდეგო ქმედებაზე იხ. მაგალითად, საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისიის 2024 წლის 31 ივლისის №078/23 გადაწყვეტილება.

[25] მოწინააღმდეგე მხარესთან მიმართებით კანონსაწინააღმდეგო ქმედებაზე იხ. მაგალითად, საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისიის 2024 წლის 8 თებერვლის №056/22 გადაწყვეტილება; ასევე, საქართველოს უზენაესი სასამართლოს სადისციპლინო პალატის 2024 წლის 11 აპრილის №სსდ-02-24 გადაწყვეტილება.

[26] ზოგადად ადვოკატის მხრიდან შეურაცხმყოფელი ქმედების თაობაზე იხ. მაგალითად, საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისიის 2024 წლის 23 თებერვლის №097/18 გადაწყვეტილება; ასევე, საქართველოს უზენაესი სასამართლოს სადისციპლინო პალატის 2022 წლის 14 აპრილის №სსდ-01-22 გადაწყვეტილება.

[27] საილუსტრაციოდ გამოდგება შემთხვევა, როდესაც ადვოკატმა მიმართა ეთიკის კომისიას კოლეგა ადვოკატის მიმართ ეთიკის სტანდარტის დარღვევის თაობაზე და საჩივარში ისეთ ინფორმაციაზე (მონაცემებზე) გაამახვილა ყურადღება, რის გამოც მის მიმართ დადგინდა სამართალდარღვევა. იხ. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 7 ივლისის №გ-1/153/2023 გადაწყვეტილება.

[28] პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 29 თებერვლის №გ-1/042/2024 გადაწყვეტილება.

[29] *არჩუაძე თ.*, პერსონალურ მონაცემთა დეპერსონალიზაცია, როგორც მონაცემთა სუბიექტის დაცვის გარანტია, საკონსტიტუციო სამართლის მიმოხილვა, №11, 2017, 101.

საქართველოს კანონის მე-3 მუხლის „ც“ ქვეპუნქტით) ხაზს უსვამს მთავარ ფაქტორს: მესამე პირისთვის არ უნდა იყოს აღქმადი მონაცემი. დეპერსონალიზაციის კლასიკური გამოვლინებაა ე.წ. ინიციალების მითითება, თუმცა მხოლოდ ამგვარი ფორმალური აქტი ვერ ჩაითვლება კანონის დაცვის წინაპირობის მქონედ.[30] მსჯელობისთვის შეიძლება ორი მაგალითის მოყვანა:

პირველი მათგანი ეხება საადვოკატო ბიუროს მხრიდან სოციალურ მედიაში გამოქვეყნებულ ინფორმაციას საქმის თაობაზე, რომელიც კლიენტის (მაშასადამე, რომელსაც წარმოადგენდა პროცესში ადვოკატი/საადვოკატო ბიურო) სასარგებლოდ დასრულდა. საადვოკატო ბიურომ სოციალურ მედიაში გამოაქვეყნა ინფორმაცია, რომელშიც მარწმუნებლის ინიციალები და საქმესთან დაკავშირებული დეტალები იყო მითითებული.[31] სამსახურის განმარტებით, აღნიშნული ერთობლიობაში იძლეოდა განმცხადებლის იდენტიფიცირების შესაძლებლობას. სამსახურმა არ გაითვალისწინა საადვოკატო ბიუროს განმარტება, რომლითაც იგი აღნიშნავდა, რომ იდენტიფიცირება შესაძლებელი იყო მხოლოდ პირთა ვიწრო წრისთვის (მოწმეებისა და საქმეში ჩართული მხარეების ოჯახის წევრებისთვის) და მიიჩნია, რომ არსებული ინფორმაცია შესაძლებლობას ქმნიდა, რომ ზედმეტი ძალისხმევის გარეშე მომხდარიყო მონაცემთა სუბიექტის იდენტიფიცირება.[32]

მეორე მაგალითი ეხება ადვოკატს, რომელმაც კოლეგის მიმართ ადვოკატთა ეთიკის კომისიაში შეიტანა საჩივარი და მიუთითა კოლეგა ადვოკატსა და ამავე კოლეგა ადვოკატის მეუღლის შესახებ. ადვოკატის შესახებ სახელი და გვარი მითითებული იყო, ხოლო, მისი მეუღლის შესახებ მხოლოდ ინიციალები ჰქონდა წარდგენილი. მიუხედავად ამისა, სამსახურის მხრიდან დარღვევად იქნა აღნიშნული ქმედება დაკვალიფიცირებული. აღნიშნულის საფუძველი გახლდათ ის, რომ საჩივარში ინიციალებთან ერთად მითითება იყო შემდეგზე: მეუღლის პროფესიის, ერთ-ერთ კომპანიაში დაკავებული პოზიციის, სამუშაო გამოცდილების, ჩაბარებული გამოცდების, ენის ფლობის, კომპანიასთან დავაში ყოფნის ფაქტის, დავის საგნის, სამსახურის მისამართის შესახებ. ამდენად, მიუხედავად დეპერსონალიზაციისა, ფაქტების/მტკიცებულებათა ერთობლიობა იძლეოდა შესაძლებლობას, რომ მომხდარიყო პირის იდენტიფიცირება. საჩივრისთვის კი ამგვარ იდენტიფიცირებას არ გააჩნდა რაიმე სახის სამართლებრივი დანიშნულება.[33]

[30] ამ საკითხზე დეტალური მსჯელობისთვის იხ. იქვე, 115.

[31] კერძოდ, პროცესში მონაწილე მხარეებს შორის არსებული ნათესაობრივი ურთიერთობის შესახებ ინფორმაცია, ოჯახის წევრების საცხოვრებელი ადგილის შესახებ ინფორმაცია და სხვ.

[32] პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 5 აგვისტოს №გ-1/081/2022 გადაწყვეტილება.

[33] პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 7 ივლისის №გ-1/153/2023 გადაწყვეტილება.

7. პერსონალურ მონაცემთა უსაფრთხოების დაცვა ადვოკატის მიერ

ადვოკატები (საადვოკატო ბიურო) ხშირად ინახავენ საქმის მასალებს თავის ოფისში, რომელზეც წვდომა აქვს არაერთ ადამიანს და მათ შორის, კოლეგებს, თუ სხვა თანამშრომლებს. ხშირად, ადვოკატის მიერ მიღებული ინფორმაცია შეიცავს განსაკუთრებული კატეგორიის პერსონალურ მონაცემს და შესაბამისად, იგი კიდევ უფრო მეტ დაცულობას საჭიროებს.[34] ამ მხრივ, სამსახურის პრაქტიკაში გვხვდება შემთხვევა, როდესაც ადვოკატსა და საადვოკატო ბიუროს დაევალა, რომ უზრუნველყოთ ორგანიზაციული და ტექნიკური ზომების შემუშავება, რაც პერსონალურ მონაცემთა უსაფრთხოების დაცვის გარანტი გახდებოდა.[35] აღნიშნულის მაგალითია, შესაბამისი საკეტით დაცულ ადგილზე განთავსება, დამცავი სისტემის განსაზღვრა მაშინ, თუ მონაცემები ელექტრონულადაა შენახული, საჯარო ხელმისაწვდომობის შეზღუდვა და სხვ.

8. კავშირი სხვა სამართლებრივ ინსტიტუტებთან

პერსონალურ მონაცემთა უკანონო დამუშავებით შესაძლებელია, რომ დაირღვეს პირის სხვა უფლებები.[36] აღნიშნულის კლასიკური მაგალითია არაქონებრივ უფლებათა დარღვევა, რომელიც შეიძლება გამოიხატოს პირის შეურაცხყოფაში, ასევე, ცილისწამებაში და სხვ. თუნდაც არაქონებრივი უფლებების დარღვევა პერსონალურ მონაცემთა უკანონო დამუშავებასთან ერთად იკვეთებოდეს, სამსახური შესაძლებლობასაა მოკლებული, რომ ეს საკითხი შეისწავლოს.[37] კერძოდ, განიხილოს, ვთქვათ, გავრცელებული მონაცემების სინამდვილე და სიზუსტე და სხვ.[38] ასეთ დროს მოთხოვნა ინდივიდუალურად დგება ადვოკატის მიმართ. მაგალითად, „სიტყვისა და გამოხატვის თავისუფლების შესახებ“ საქართველოს კანონიდან გამომდინარე[39] და სხვ.

---

[34] მით უმეტეს, მისი გასაჯაროება დაუშვებელია. იხ. მაგალითად, სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 26 აპრილის №გ-1/121/2021 გადაწყვეტილება.

[35] პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის საქმიანობის ანგარიში, 109.

[36] ამ შემთხვევაში ერთმანეთისგან უნდა განვასხვავოთ უფლების დარღვევა პირისთვის პასუხისმგებლობის დაკისრებისგან. შესაბამისად, მაგალითად, ადვოკატის პროფესიულ სტანდარტზე ამ შემთხვევაში არ მოხდება ხაზგასმა.

[37] საკითხზე სრული სურათისთვის იხ. საქართველოს უზენაესი სასამართლოს 2020 წლის 22 ოქტომბრის №ბს-921(კ-19) განჩინება.

[38] პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 29 თებერვლის №გ-1/042/2024 გადაწყვეტილება.

[39] ადვოკატთან მიმართებით, მისი პროფესიის გათვალისწინებით, გამოხატვის თავისუფლების სტანდარტი არ შეიძლება იყოს სხვა პროფესიის წარმომადგენლებთან მიმართებით დადგენილი სტანდარტის მსგავსი. იხ. ამ თემაზე, *Morice v. France [GC]*, [2015] ECHR, №29369/10, საქართველოს უზენაესი სასამართლოს 2020 წლის 6 აპრილის №ას-1366-2019 განჩინება, ასევე, საქართველოს უზენაესი სასამართლოს 2023 წლის 5 ივლისის №ას-622-2022 განჩინება.

9. დასკვნა

ადვოკატს (საადვოკატო ბიუროს) მმართებს, რომ პერსონალურ მონაცემთა დამუშავებისას საკითხს ყურადღებით მოეკიდოს. საადვოკატო საქმიანობა შეზღუდულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, იქნება ეს საკუთარი თავის/მომსახურების რეკლამირება, ინფორმაციის გავრცელება თუ დოკუმენტაციის მოპოვება. მეტიც, ადვოკატის ქმედებამ შესაძლებელია, რომ დაარღვიოს ერთობლივად როგორც ზემოთ დასახელებული კანონი,[40] ისე – პროფესიული ეთიკის კოდექსით გათვალისწინებული სტანდარტები[41] და სხვ. ქართული პრაქტიკა ამ მხრივ საინტერესოდაა განვითარებული. სამსახურის გადაწყვეტილებებში ვხვდებით არაერთ მიდგომას, როდესაც ადვოკატის მოქმედება სამართალდარღვევად იქნა მიჩნეული.[42]

ამდენად, ადვოკატმა წინდახედულად უნდა განსაზღვროს ის, თუ რა ფარგლებში აქვს მას უფლებამოსილება, დაამუშაოს პერსონალური მონაცემები. მხოლოდ ფორმალური მიდგომა (მაგალითად, დეპერსონალიზაციის (როდესაც მონაცემთა სუბიექტის იდენტიფიცირება მაინც შესაძლებელია), თუ კლიენტის ინტერესის საფუძვლის თვალსაზრისით), ვერ გახდება ადვოკატის პასუხისმგებლობისგან გათავისუფლების საფუძველი.

[40] შესაბამისად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დარღვევისთვის მას შეიძლება დაეკისროს ზიანის ანაზღაურება და აღნიშნული ეფუძნებოდეს როგორც საქართველოს ზოგადი ადმინისტრაციული კოდექსის 207-ე და 208-ე მუხლებს, ისე – საქართველოს სამოქალაქო კოდექსის მე-18, თუ 413-ე მუხლს. საილუსტრაციოდ იხ. საქართველოს უზენაესი სასამართლოს 2023 წლის 11 ივლისის №ბს-194(კ-23) განჩინება.

[41] იგივე რეკლამირების დროსაც. ამ საკითხზე იხ. მაგალითად, საქართველოს უზენაესი სასამართლოს სადისციპლინო პალატის 2024 წლის 5 ნოემბრის №სსდ-09-24 გადაწყვეტილება. ადვოკატის რეკლამირებასთან მიმართებით იხ. ასევე, *ბუბულური თ.,* იურიდიული საქმიანობის რეკლამირების განვითარება აშშ-ში (XIX-XX სს), ივანე სურგულაძე 120, საიუბილეო კრებული, გეგენავა (რედ.), 2024, 123-140.

[42] იხ. მაგალითად, სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 26 აპრილის №გ-1/121/2021 გადაწყვეტილება.

ბიბლიოგრაფია:

1. საქართველოს კანონი „ადვოკატთა შესახებ“, 20/06/2001.
2. საქართველოს სამოქალაქო კოდექსი, 26/06/1997.
3. საქართველოს სისხლის სამართლის კოდექსი, 22/06/1999.
4. საქართველოს კანონი „სიტყვისა და გამოხატვის თავისუფლების შესახებ“, 24/06/2004.
5. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 28/12/2011.
6. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
7. *არჩუაძე თ.*, პერსონალურ მონაცემთა დეპერსონალიზაცია, როგორც მონაცემთა სუბიექტის დაცვის გარანტია, საკონსტიტუციო სამართლის მიმოხილვა, №11, 2017, 101, 115.
8. *ხუბულია ნ.,* არასრულწლოვნის პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული გამოწვევები, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი №1, 2024, 62-71.
9. *ხუბულური თ.,* იურიდიული საქმიანობის რეკლამირების განვითარება აშშ-ში (XIX-XX სს), ივანე სურგულაძე 120, საიუბილეო კრებული, გეგენავა (რედ.), 2024, 123-140.
10. პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის საქმიანობის ანგარიში, 109.
11. საქართველოს უზენაესი სასამართლოს 2020 წლის 6 აპრილის №ას-1366-2019 განჩინება.
12. საქართველოს უზენაესი სასამართლოს 2020 წლის 22 ოქტომბრის №ბს-921(კ-19) განჩინება.
13. საქართველოს უზენაესი სასამართლოს სადისციპლინო პალატის 2022 წლის 14 აპრილის №სსდ-01-22 გადაწყვეტილება.
14. საქართველოს უზენაესი სასამართლოს 2023 წლის 5 ივლისის №ას-622-2022 განჩინება.
15. საქართველოს უზენაესი სასამართლოს 2023 წლის 11 ივლისის №ბს-194(კ-23) განჩინება.
16. საქართველოს უზენაესი სასამართლოს სადისციპლინო პალატის 2024 წლის 11 აპრილის №სსდ-02-24 გადაწყვეტილება.
17. საქართველოს უზენაესი სასამართლოს სადისციპლინო პალატის 2024 წლის 5 ნოემბრის №სსდ-09-24 გადაწყვეტილება.
18. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 21 აპრილის №გ-1/137/2020 გადაწყვეტილება.
19. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 28 აპრილის №გ-1/147/2020 გადაწყვეტილება.
20. სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №გ-1/207/2021 გადაწყვეტილება.

21. სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 26 აპრილის №გ-1/121/2021 გადაწყვეტილება.
22. პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 5 აგვისტოს №გ-1/081/2022 გადაწყვეტილება.
23. პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 6 ოქტომბრის №გ-1/130/2022 გადაწყვეტილება.
24. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 20 თებერვლის №გ-1/024/2023 გადაწყვეტილება.
25. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 7 ივლისის №გ-1/153/2023 გადაწყვეტილება.
26. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 29 თებერვლის №გ-1/042/2024 გადაწყვეტილება.
27. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 29 თებერვლის №გ-1/042/2024 გადაწყვეტილება.
28. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 5 მარტის №გ-1/046/2024 გადაწყვეტილება.
29. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 30 ივნისის №გ-1/149/2023 გადაწყვეტილება.
30. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 7 აგვისტოს №გ-1/191/2024 გადაწყვეტილება.
31. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 14 აგვისტოს №გ-1/198/2024 გადაწყვეტილება.
32. საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისიის 2024 წლის 8 თებერვლის №056/22 გადაწყვეტილება.
33. საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისიის 2024 წლის 23 თებერვლის №097/18 გადაწყვეტილება.
34. საქართველოს ადვოკატთა ასოციაციის ეთიკის კომისიის 2024 წლის 31 ივლისის №078/23 გადაწყვეტილება.
35. *Morice v. France [GC]*, [2015] ECHR, №29369/10.

ბექა მელაძე*

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება - გამოწვევები და შესაძლებლობები

ჩვენ ვცხოვრობთ რეალობაში, სადაც თითოეული გადაწყვეტილება ეფუძნება გარშემო არსებული ინფორმაციის ნაკადს. მონაცემთა სწორი და სწრაფი ანალიზი აძლიერებს ინდუსტრიებს, გარდაქმნის საზოგადოებას და აჩქარებს პროგრესს. ამ ტრანსფორმაციაში განსაკუთრებული როლი უკავია ღრუბლოვან სისტემებს ("Cloud Systems"). აღნიშნული ტექნოლოგია უამრავ შესაძლებლობას ქმნის და სახელმწიფოს, ბიზნეს სექტორსა თუ ფიზიკურ პირს ყოველდღიურ საქმიანობას უმარტივებს. მიუხედავად ამისა, არსებობს მრავალი გამოწვევაც, რომელიც დაკავშირებულია პერსონალური მონაცემების კანონიერ და ეთიკურ დამუშავებასთან.

საკვანძო სიტყვები: *პერსონალური მონაცემები, ღრუბლოვანი სისტემები, დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირი, მონაცემთა საერთაშორისო გადაცემა, მონაცემთა უსაფრთხოება.*

1. შესავალი

ღრუბლოვანი სისტემები ბოლო ათწლეულის ერთ-ერთი ყველაზე მზარდი ტექნოლოგიაა, რომელიც ტრადიციულ, ფიზიკურ ინფრასტრუქტურასთან დაკავშირებული შეზღუდვების საპირწონედ, ხელს უწყობს მონაცემთა სწრაფ და ეფექტიან დამუშავებას. აღნიშნული მოდელი გვთავაზობს მოქნილ მიდგომას, რაც დღევანდელ ციფრულ სამყაროში არსებული მზარდი მოცულობის მონაცემთა სამართავად აუცილებელია. მხოლოდ 2024 წელს ექვსას მილიარდზე მეტი[1] დაიხარჯა ღრუბლოვანი

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

[1] Public cloud services end-user spending worldwide from 2017 to 2024,

სისტემების მომსახურებაზე და პროგნოზების თანახმად, ის 2027 წლისთვის დაახლოებით 1 ტრილიონ დოლარს მიაღწევს. ზრდა გამოწვეულია სხვადასხვა ინდუსტრიაში ღრუბლოვანი სერვისების დანერგვით, რადგან კომპანიები უპირატესობას ანიჭებენ ღრუბლოვანი სისტემების ხარჯთ-ეფექტიანობას[2].

მოქნილობისა და სისწრაფის პარალელურად, წარმოიშობა არაერთი გამოწვევა, რომელიც დაკავშირებულია მესამე პირის სერვერების მეშვეობით პერსონალური მონაცემების დამუშავებასთან, მათ შორის, სუბიექტების სტატუსის და უსაფრთხოების ნაწილში მათი ფუნქციების განსაზღვრა. ამასთან, განსაკუთრებულ სირთულეს წარმოადგენს მონაცემთა დამუშავების ადგილმდებარეობის დადგენა, რაც შესაძლოა დაკავშირებული იყო სხვადასხვა ვალდებულებასთან.

წინამდებარე ნაშრომი შეისწავლის პერსონალური მონაცემების დამუშავების პროცესში ღრუბლოვანი სისტემების გამოყენებას, განიხილავს მათ შესაძლებლობებსა და გამოწვევებს, რომლებიც დაკავშირებულია კონფიდენციალობასა და უსაფრთხოებასთან.

2. ღრუბლოვანი სისტემების არსი

ღრუბლოვანი სისტემები ნებისმიერ პირს აძლევს საშუალებას ინტერნეტის გამოყენებით ისარგებლოს შესაბამისი მომსახურების მიმწოდებელი კომპანიის ინფრასტრუქტურით, კერძოდ, შეინახოს ან სხვაგვარად დაამუშაოს საკუთარი მონაცემები მსოფლიოს ნებისმიერი წერტილიდან.

მარტივად რომ ითქვას, ღრუბლოვანი სისტემები მომხმარებელს აძლევს საშუალებას მონაცემები, ფაილები, ფოტო/ვიდეო მასალა თუ სხვადასხვა აპლიკაციები ინტერნეტის გამოყენებით, განათავსონ რომელიმე კომპანიის სერვერებზე, ნებისმიერ დროს მასზე წვდომისა და რედაქტირების შესაძლებლობით, სასურველი მოწყობილობის გამოყენებით. დღესდღეობით მსოფლიოს მასშტაბით არაერთ კომპანიას აქვს შექმნილი ღრუბლოვანი სისტემები, რომლებიც სხვადასხვა მიზნით გამოიყენება. აღნიშნულ სფეროში წამყვანი პოზიციები აქვთ ღრუბლოვანი სისტემების პროვაიდერებს: “Amazon Web Services”, “Microsoft Azure” და “Google Cloud Platform (GCP)”.

აშშ-ს სტანდარტებისა და ტექნოლოგების ნაციონალური ინსტიტუტის (“NIST”) განმარტებით ღრუბლოვან სისტემებს გააჩნია 5 თვისება[3]:

<https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].

[2] NexQloud ღრუბლოვანი ტექნოლოგიების ბაზარზე რევოლუციას დეცენტრალიზებული პლატფორმით მოახდენს, 2024, <https://forbes.ge/nexqloud-set-to-disrupt-cloud-computing-with-decentralized-platform/> [21.02.2025].

[3] National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012, 800-146.

1. მყისიერი წვდომა - მომხმარებელს შეუძლია სასურველ დროს ისარგებლოს მომსახურებით (მაგალითად, გახსნას და მიიღოს წვდომა საკუთარ ბაზაზე) ინფრასტრუქტურის მესაკუთრე კომპანიის თანხმობის ან/და დახმარების გარეშე;
2. ფართო ქსელზე წვდომა ("Broad Network Access") - მომხმარებელს შეუძლია საკუთარ მონაცემებზე წვდომა (რედაქტირება, წაშლა, დამატება და სხვა) პარალელურად, რამდენიმე მოწყობილობის მეშვეობით;
3. სისტემის პროვაიდერი საკუთარ ინფრასტრუქტურულ რესურსებს მრავალ მომხმარებელს შორის ანაწილებს მათივე მოთხოვნის შესაბამისად;
4. მოქნილობა - მომხმარებელს აქვს შესაძლებლობა საჭიროების შესაბამისად გაზარდოს ან შეამციროს რესურსები, მაგალითად, "Google Drive"-ზე შეიძინოს სტანდარტული მოცულობისგან განსხვავებული რესურსის რაოდენობა;
5. პერსონალიზებული საფასური - მომსახურების საფასური განისაზღვრება გამოყენებული რესურსის შესაბამისად.

აქვე, უნდა აღინიშნოს, რომ ღრუბლოვანი სისტემები საკმაოდ მრავალფეროვანია და მოიცავს რამდენიმე განსხვავებულ სერვისს, კერძოდ:

- პროგრამული უზრუნველყოფა, როგორც მომსახურება ("Software as a Service") - ონლაინ რეჟიმში მომუშავე ელექტრონული ფოსტის და დოკუმენტების შენახვის სისტემა ("Google Drive", "Dropbox", "Gmail", "Outlook 365" და სხვა);
- პლატფორმა, როგორც მომსახურება ("Platform as a Service") - გამოიყენება დეველოპერების მიერ ღრუბლოვან სისტემაში აპლიკაციების შესაქმნელად, ("Google App Engine");
- ინფრასტრუქტურა, როგორც მომსახურება ("Infrastructure as a Service") - ძირითად შემთხვევაში გამოიყენება იურიდიული პირების მიერ, რომლებიც საკუთარი სერვერის შექმნის ნაცვლად იყენებენ ღრუბლოვანი სისტემების პროვაიდერი კომპანიის ინფრასტრუქტურას.

აქვე, უნდა აღინიშნოს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ"[4] საქართველოს კანონის მე-2 მუხლის პირველი პუნქტის თანახმად, კანონის მოქმედება ვრცელდება საქართველოს ტერიტორიაზე მონაცემთა ავტომატური საშუალებებით დამუშავებასა და ნახევრად ავტომატური საშუალებებით დამუშავებაზე. შესაბამისად, თუკი პირი პერსონალურ მონაცემებს ამუშავებს საქართველოს ტერიტორიაზე, მათ შორის, აქვს მხოლოდ წვდომა ღრუბლოვან სისტემაზე, აღნიშნულზე ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მოქმედება, მიუხედავად იმისა, თუ სად არის განთავსებული ან რომელ იურისდიქციაში ექცევა ღრუბლოვანი სისტემა ან/და მისი პროვაიდერი

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

კომპანია[5] (ღრუბლოვანი სისტემის ადგილმდებარეობის და შესაბამისი იურისდიქციის საკითხთან დაკავშირებული იხილეთ წინამდებარე სტატიის 4.2. თავი).

მიუხედავად ღრუბლოვანი სისტემების გამოყენების მრავალფეროვნებისა, პერსონალური მონაცემების დამუშავების მხრივ, განსაკუთრებით საინტერესოა პროგრამული უზრუნველყოფა, როგორც სერვისი, რადგან იგი ყველაზე ხშირად გამოიყენება დამუშავებისთვის პასუხისმგებელი პირების მიერ პერსონალური მონაცემების შენახვის, გაზიარების და სხვაგვარი დამუშავებისთვის.

3. სუბიექტების სამართლებრივი სტატუსი

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება მეტად კომპლექსური თემაა, სადაც რამდენიმე მხარეა ჩართული. ხშირ შემთხვევაში, რესურსების დისბალანსისა და დომინანტური მდგომარეობიდან გამომდინარე, რთულია განისაზღვროს, რომელი მხარე წარმოადგენს დამუშავებისთვის პასუხისმგებელ პირს და რომელი დამუშავებაზე უფლებამოსილ პირს. ამ კუთხით, მნიშვნელოვანია შეფასდეს, ერთი მხრივ, ღრუბლოვანი სისტემის პროვაიდერი კომპანიის, ხოლო მეორე მხრივ, მისი პროდუქტის მომხმარებლის როლი და ფუნქცია.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „ო“ ქვეპუნქტის თანახმად, „დამუშავებისთვის პასუხისმგებელი პირი არის ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას“, ამავე მუხლის „ჟ“ ქვეპუნქტის თანახმად კი „დამუშავებაზე უფლებამოსილი პირი არის ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით“.

ღრუბლოვანი სისტემებით სარგებლობისას მომხმარებელი თავად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, შესაბამისად, სწორედ იგი არის დამუშავებისთვის პასუხისმგებელი პირი, ხოლო, მეორე მხრივ, ღრუბლოვანი სისტემის პროვაიდერ კომპანიას მომხმარებლის მონაცემთა დამუშავების ნაწილში პირადი მიზანი არ გააჩნია და მოქმედებს მხოლოდ დამუშავებისთვის პასუხისმგებელი პირი მიზნებისთვის, შესაბამისად იგი გვევლინება, როგორც დამუშავებაზე უფლებამოსილი პირი[6].

[5] შეად.: EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.

[6] შეად.: The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.

აქვე, უნდა აღინიშნოს, რომ, მონაცემთა დამუშავების პროცესში, როგორც წესი, დამუშავებისთვის პასუხისმგებელი პირი განსაზღვრავს „თამაშის წესებს“ და დამუშავებაზე უფლებამოსილი პირი „ემორჩილება“ მას. მიუხედავად ამისა, ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავებისას უმეტეს შემთხვევაში, სერვისის პროვაიდერის დომინანტური როლიდან და მისი რესურსებიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელი პირი თანხმდება დამუშავებაზე უფლებამოსილი პირის წესებსა და პირობებს. მაგალითად, თუკი მომხმარებელს სურს ისარგებლოს “Google Cloud Platform”-ით, მომხმარებელი ვერ განუსაზღვრავს ასეთ მასშტაბურ კომპანიას „თამაშის წესებს“, თუმცა მონაცემთა დამუშავების მიზნებს და საშუალებებს კვლავ მომხმარებელი განსაზღვრავს, რაც უმთავრეს კრიტერიუმს წარმოადგენს სამართლებრივი სტატუსის დადგენისას[7].

4. პერსონალური მონაცემების დამუშავება ღრუბლოვან სისტემებში

მონაცემთა დამუშავების ეფექტიანობიდან გამომდინარე, ღრუბლოვან სისტემებს აქტიურად იყენებენ როგორც კომპანიები, ისე სახელმწიფო ორგანოები. ამასთან, ღრუბლოვანი სისტემები მომხმარებლებს აძლევს შესაძლებლობას დაზოგონ ხარჯები და გააუმჯობესონ სერვისები.

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება რამდენიმე მნიშვნელოვან ეტაპად შეიძლება დაიყოს. პირველ რიგში, უნდა აღინიშნოს, რომ დამუშავებისთვის პასუხისმგებელი ნებისმიერი პირი თავად წყვეტს როგორ, რა ფორმით და რა მოცულობით ატვირთავს ღრუბლოვან სისტემაში მონაცემებს.

ღრუბლოვან სისტემებში მონაცემთა დამუშავების ყველაზე გავრცელებული სახე მათი შენახვაა (“Data at Rest”), რა დროსაც მნიშვნელოვანია გათვალისწინებული იყოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლით გათვალისწინებული უსაფრთხოების ზომები, როგორც პროვაიდერის მხრიდან, ისე დამუშავებისთვის პასუხისმგებელი პირის მხრიდან.

შენახვის გარდა, ღრუბლოვანი სისტემები გამოიყენება მონაცემთა სხვაგვარი დამუშავებისთვისაც (“Data in Use”), მაგალითად, მათი გადმოწერისთვის, გაზიარებისთვის, ანალიტიკისთვის, ხელოვნური ინტელექტის სწავლებისთვის და სხვა. ასეთ დროს, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, რომ ღრუბლოვანი სისტემის გამოყენება მას არ ათავისუფლებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული ვალდებულებებისგან, მათ შორის, დაიცვას უსაფრთხოების ტექნიკური თუ ორგანიზაციული ზომები და

[7] შეად. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].

რაც მთავარია მონაცემები დაამუშაოს შესაბამისი სამართლებრივი საფუძვლისა და პრინციპების შესაბამისად.

5. გამოწვევები და რისკები

არაერთხელ აღინიშნა, რომ ღრუბლოვანი სისტემები კომპანიებს და სახელმწიფოებს ეხმარება მონაცემთა ეფექტურ და მოქნილ დამუშავებაში, თუმცა, მეორე მხრივ, იგი ქმნის არაერთ პრობლემურ საკითხს, რომელიც დაკავშირებულია პერსონალურ მონაცემთა დამუშავების კანონიერებასთან. გამოწვევათაგან უმნიშვნელოვანესია უსაფრთხოებასთან და სისტემების ადგილმდებარეობასთან დაკავშირებული საკითხები.

5.1. ღრუბლოვანი სისტემის ადგილმდებარეობა და საერთაშორისო გადაცემის ასპექტი

ღრუბლოვანი სისტემების მთავარ განმასხვავებელ ნიშანს წარმოადგენს ის, რომ მომხმარებელს შეუძლია ინტერნეტის გამოყენებით ისარგებლოს სერვის პროვაიდერი კომპანიის ინფრასტრუქტურითა და დაამუშაოს მონაცემები მსოფლიოს ნებისმიერი წერტილიდან. შესაბამისად, როდესაც დამუშავებისთვის პასუხისმგებელი პირი იყენებს ღრუბლოვან სისტემებს, შესაძლოა, მონაცემები ინახებოდეს (ან სხვაგვარად მუშავდებოდეს) საქართველოს ფარგლებს გარეთ, გამომდინარე იქიდან, რომ ღრუბლოვანი სისტემების პროვაიდერი კომპანიების უმეტესობას, მათ შორის, “Google”-ს, “Amazon”-სა და “Microsoft”-ს საკუთარი ბაზები/ინფრასტრუქტურა განლაგებული აქვთ სხვადასხვა ქვეყნებში[8]. ასეთ დროს მნიშვნელოვანია გათვალისწინებულ იქნეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე მუხლი, რომლის თანახმადაც მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ არსებობს მონაცემთა დამუშავების ამ კანონით გათვალისწინებული მოთხოვნები და შესაბამის სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.[9]

აქვე უნდა აღინიშნოს, „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23

[8] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012, 16.

[9] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 37-ე მუხლი.

ბრძანება.[10] აღნიშნულ ბრძანებაში მოცემულია ქვეყნების ჩამონათვალი, სადაც მონაცემთა გადაცემა დასაშვებია დამატებითი საფუძვლის გარეშე.

ზემოაღნიშნული საკანონმდებლო ნორმიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელმა პირმა, პირველ რიგში, დეტალურად უნდა მოიკვლიოს თუ კონკრეტულად რომელ ქვეყანაში/ქვეყნებში ინახება მონაცემები[11].

შესაბამისი ინფორმაციის მიღების შემდეგ, თუკი დადგინდა, რომ მონაცემთა გადაცემა ხდება საქართველოს საზღვრებს გარეთ ისეთ ქვეყანაში, რომელიც არ არის სათანადო გარანტიების მქონე ქვეყნების ნუსხაში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს და მოითხოვოს ნებართვა მონაცემთა საერთაშორისო გადაცემაზე[12] ან მოიპოვოს მონაცემთა სუბიექტების წერილობითი თანხმობა[13].

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებით საინტერესოა ევროკავშირის მონაცემთა დაცვის ზედამხედველის (“EDPS”) 2024 წლის 8 მარტის გადაწყვეტილება[14], რომლის ფარგლებშიც დადგინდა, რომ ევროკომისია (“European Commission”) იყენებდა “Microsoft 365”-ის პროგრამას, მონაცემებს ამუშავებდა ღრუბლოვანი სისტემის მეშვეობით, ხოლო სერვერები განლაგებული იყო აშშ-ში, აქედან გამომდინარე, ადგილი ჰქონდა მონაცემთა საერთაშორისო გადაცემას შესაბამისი სამართლებრივი საფუძვლის გარეშე.

5.2. უსაფრთხოება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის თანახმად, უსაფრთხოება მონაცემთა დამუშავების ერთ-ერთ პრინციპს წარმოადგენს, ამასთან, 27-ე მუხლის მე-2 პუნქტის თანახმად, „დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან მიიღონ მონაცემთა დამუშავების შესაძლო და თანამდევი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომები (მათ შორის, მონაცემთა ფსევდონიმიზაცია, მონაცემებზე წვდომის აღრიცხვა,

[10] „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანება.

[11] Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].

[12] უნდა აღინიშნოს, რომ ნებართვის მოპოვების შედეგად მონაცემთა საერთაშორისო გადაცემა არის ერთ-ერთი საფუძველი და ალტერნატივად, მონაცემთა დამუშავების სპეციფიკიდან გამომდინარე, შესაძლოა არსებობდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე მუხლის მეორე პუნქტით გათვალისწინებული სხვა საფუძველიც.

[13] სავალდებულოა, რომ წერილობითი თანხმობა აკმაყოფილებდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 32-ე და 37-ე მუხლის მეორე პუნქტი „დ“ ქვეპუნქტის მოთხოვნებს.

[14] EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.

ინფორმაციული უსაფრთხოების მექანიზმები (კონფიდენციალობა, მთლიანობა, ხელმისაწვდომობა) და სხვა), რომლებიც უზრუნველყოფს მონაცემთა დაცვას მონაცემთა დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან“.

ზემოაღნიშნული ჩანაწერიდან გამომდინარე, უსაფრთხოების უზრუნველყოფა ევალება, როგორც დამუშავებაზე უფლებამოსილ პირს - ღრუბლოვანი სისტემების პროვაიდერს, ისე დამუშავებისთვის პასუხისმგებელ პირს - სისტემის მომხმარებელს.

სისტემის სპეციფიკიდან გამომდინარე, ტექნიკური უსაფრთხოების უზრუნველყოფის უმთავრესი ნაწილი სერვისის პროვაიდერი, ანუ დამუშავებაზე უფლებამოსილი პირის ვალდებულებაა, კერძოდ, პირველ რიგში, მან უნდა უზრუნველყოს სისტემის იმგვარი წყობა, რომ სხვადასხვა მომხმარებლებს ერთმანეთის მონაცემებზე წვდომის შესაძლებლობა არ ჰქონდეთ. გარდა ამისა, სისტემა უნდა იყენებდეს დაშიფვრის იმგვარ ტექნოლოგიას (“Public” და “Private key”-ის გამოყენებით), რომ თავად პროვაიდერსაც არ ჰქონდეს, როგორც შენახული (“data at Rest”) ისე „მოძრავ“ (“Data in Use”) მონაცემებზე წვდომის შესაძლებლობა[15].

ჩვენს რეალობაში, საქართველოს კანონმდებლობა, როგორც წესი, ვრცელდება ღრუბლოვანი სერვისის მომხმარებლებზე, ანუ დამუშავებისთვის პასუხისმგებელ პირებზე, რადგან ღრუბლოვანი სისტემების პროვაიდერი ლიდერი კომპანიების საქმიანობა სცილდება საქართველოს იურისდიქციას. აღნიშნულიდან გამომდინარე, მნიშვნელოვანია, განისაზღვროს, უსაფრთხოების დაცვის კუთხით, რა ვალდებულებები გააჩნიათ ღრუბლოვანი სისტემების გამოყენებისას დაშვებისთვის პასუხისმგებელ პირებს.

პირველ რიგში, აუცილებელია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა მოიკვლიოს და შეაფასოს სხვადასხვა ღრუბლოვანი სისტემის უსაფრთხოების მექანიზმები და მხოლოდ ამის შემდგომ აირჩიოს სანდო და უსაფრთხო პროვაიდერი[16].

გარდა ამისა, ღრუბლოვანი სისტემის მომხმარებელმა უნდა უზრუნველყოს უსაფრთხოების ორგანიზაციული ნორმები და შესაბამის მონაცემებზე წვდომა მიანიჭოს მხოლოდ იმ პირებს, რომელსაც ამისი უფლებამოსილება, შესაბამისი საფუძველი და საჭიროება აქვთ[17], ამასთან, განახორციელონ სათანადო ღონისძიებები თანამშრომელთა მიერ მონაცემთა უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, მათ შორის, უზრუნველყონ თანამშრომელთა ინფორმირება მონაცემთა უსაფრთხოების დაცვის საკითხების შესახებ[18].

[15] CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012, 10.

[16] შეად. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 13-14, <https://ico.org.uk/> [10.03.2025].

[17] შეად. EU Data Protection Code of Conduct for Cloud Service Providers, 2020, 17-20.

[18] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 27-ე მუხლის მე-6 პუნქტი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის მე-4 პუნქტის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა. როგორც წესი, ღრუბლოვანი სისტემებს ე.წ. „ლოგირების“ ფუნქცია გააჩნია, მიუხედავად ამისა, დამუშავებისთვის პასუხისმგებელი პირი, ვალდებულია შექმნას რამდენიმე ინდივიდუალური მომხმარებელი, რათა, საჭიროების შემთხვევაში, დადგენადი იყოს კონკრეტულად ვის მიერ მოხდა მონაცემთა რედაქტირება, წაშლა, დამატება და სხვა მოქმედება[19].

6. დასკვნა

დასკვნის სახით შეიძლება ითქვას, რომ ღრუბლოვანი სისტემის პოპულარობის ზრდა, გარდაუვალია, რადგან იგი მონაცემთა სწრაფი და მოქნილი დამუშავების ერთ-ერთი საუკეთესო ტექნოლოგიაა, რომელიც კომპანიებს, სახელმწიფოებს თუ ფიზიკურ პირებს აძლევს შესაძლებლობას დაზოგონ ხარჯები, გაზარდონ ეფექტიანობა და მიიღონ მონაცემებზე წვდომა მსოფლიოს ნებისმიერი წერტილიდან, სხვადასხვა მოწყობილობის მეშვეობით.

ღრუბლოვანი სისტემების შესაძლებლობებს თან ახლავს არაერთი გამოწვევა, რომელიც დაკავშირებულია პერსონალური მონაცემების დამუშავების სამართლებრივ თუ ეთიკურ საკითხებთან.

გამოწვევებისთვის დასაძლევად, სავალდებულოა, რომ დამუშავებისთვის პასუხისმგებელმა/დამუშავებაზე უფლებამოსილმა პირებმა დაიცვან უსაფრთხოების ზომები, კერძოდ, სისტემის პროვაიდერმა იქონიოს მონაცემთა დაშიფვრის ძლიერი ტექნოლოგია, ხოლო მომხმარებელმა, თავის მხრივ, მონაცემებზე წვდომა მიანიჭოს მხოლოდ უფლებამოსილ პირებს და დაიცვას სხვა ორგანიზაციული ნორმები.

გარდა ამისა, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განსაზღვრონ მონაცემთა შენახვის ადგილმდებარეობა და საჭიროების შემთხვევაში შეიქმნან შესაბამისი სამართლებრივი საფუძველი მონაცემთა საერთაშორისო გადაცემისათვის.

აქვე უნდა აღინიშნოს, რომ აუცილებელია ღრუბლოვანი სისტემების და მონაცემთა დაცვის კანონმდებლობას შორის ურთიერთმიმართებაზე ცნობიერების ამაღლება, რათა დამუშავებისთვის პასუხისმგებელ პირებს ჰქონდეს მეტი ინფორმაცია ღრუბლოვანი სისტემების გამოწვევების და მათგან მომდინარე საკანონმდებლო ვალდებულებების თაობაზე, რადგან, პერსონალურ მონაცემთა დაცვა არამხოლოდ ტექნიკური საკანონმდებლო

[19] შეად. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 14-15, <https://ico.org.uk/> [10.03.2025].

მოთხოვნა, არამედ მონაცემთა ნებისმიერი დამუშავებისთვის პასუხისმგებელი პირის ფუნდამენტური პასუხისმგებლობაა.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანება.
3. CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012.
4. EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.
5. EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.
6. EU Data Protection Code of Conduct for Cloud Service Providers, 2020.
7. European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012.
8. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].
9. National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012.
10. Public cloud services end-user spending worldwide from 2017 to 2024 <https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].
11. The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.

გიორგი ხორბალაძე*

დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი

პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ძირითადი მიზანია. ვიდეომონიტორინგი მონაცემთა დამუშავების ერთ-ერთ ფორმას წარმოადგენს. დასაქმებული პირის, როგორც მონაცემთა სუბიექტის პირადი ავტონომიის პატივისცემის უფლების დასაცავად და მისი სამუშაო სივრცის/პროცესის ვიდეომონიტორინგის კანონიერად განსახორციელებლად, აუცილებელია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით დადგენილი არაერთი სამართლებრივი საკითხის გათვალისწინება.

წინამდებარე ნაშრომში განიხილება დასაქმებულის სამუშაო ადგილზე ვიდეომონიტორინგის განხორციელების საკანონმდებლო რეგულირება და პერსონალურ მონაცემთა დაცვის სამსახურის, ევროპის ქვეყნების საზედამხედველო ორგანოებისა და ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა, დასაქმებულის სამუშაო პროცესისა თუ სივრცის ვიდეომონიტორინგთან დაკავშირებული ცალკეული საკითხები და დამუშავებისთვის პასუხისმგებელი/უფლებამოსილი პირის ძირითადი ვალდებულებები.

საკვანძო სიტყვები: *პერსონალური მონაცემი, სამუშაო სივრცე/პროცესი, სამუშაო ადგილი, ვიდეომონიტორინგი, მონაცემთა უსაფრთხოება, ზეგავლენის შეფასება.*

1. შესავალი

პირადი და ოჯახური ცხოვრების პატივისცემის უფლება საქართველოს კონსტიტუციით აღიარებული ადამიანის ერთ-ერთი ფუნდამენტური უფლებაა. ფიზიკური პირის პერსონალური ავტონომია პირადი ცხოვრების უფლების ძირითად პრინციპად მოიაზრება[1]. აღნიშნულ პრინციპს კი, თავის მხრივ, უკავშირდება პერსონალური მონაცემების კონცეფცია, როგორც

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

[1] *Case of Pretty v. the United Kingdom,* [2002] ECHR App. No. 2346/02, §61.

პირადი ცხოვრების ხელშეუხებლობის უფლების უმნიშვნელოვანესი ასპექტი. რამდენადაც არსებობს ადამიანი, არსებობს პერსონალური მონაცემებიც. შესაბამისად, ნებისმიერ დემოკრატიულ სახელმწიფოში ადამიანის, როგორც უზენაესი ღირებულების, პირადი ცხოვრების დაცვა პრიორიტეტი უნდა იყოს.

პირადი ცხოვრების დაცვის განუზომელი მნიშვნელობის მიუხედავად, როგორც ეროვნული, ასევე საერთაშორისო კანონმდებლობის მიხედვით, აღნიშნული უფლება დაცვის აბსოლუტური სტანდარტით არ ხასიათდება, რაც იმას ნიშნავს, რომ გარკვეულ შემთხვევებში, უფლების შეზღუდვა დასაშვებია. ადამიანის უფლებათა ერთმანეთთან კონკურირებადი ხასიათის გათვალისწინებით, აუცილებელია მათ შორის სამართლიანი ბალანსის დაცვა, რაც გულისხმობს საქმის განმხილველი ორგანოს/პირის მიერ თითოეული შემთხვევის ინდივიდუალურ შეფასებასა და ანალიზს. პერსონალური მონაცემების დაცვის უფლებას, ხშირად, მეორე მხარის სიტყვისა და გამოხატვის თავისუფლების უფლება უპირისპირდება. ამ უფლებათა შორის სამართლიანი ბალანსის დაცვის მიზნით, საქმის განმხილველი ორგანოს/პირის მიერ გარემოებათა სრულყოფილი შესწავლა და თანაზომიერების პრინციპის შესაბამისად განხილვაა აუცილებელი. სახელმწიფოს მიერ უფლების შეზღუდვა მართლზომიერია, თუ შეზღუდვის შესაძლებლობა დადგენილია კანონით, იგი ემსახურება ლეგიტიმურ მიზანს და აუცილებელია დემოკრატიულ საზოგადოებაში.

ადამიანის ძირითადი უფლებებისა და თავისუფლებების, განსაკუთრებით კი პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვის ერთ-ერთი ძირითადი ეროვნული საკანონმდებლო აქტია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომლის რეგულირების საგანი, სხვა საკითხებთან ერთად, სხვადასხვა კერძო თუ საჯარო სივრცეში ვიდეომონიტორინგის განხორციელების გზით პერსონალურ მონაცემთა დამუშავებაა. პირადი ცხოვრების დაცულობის ამ მნიშვნელოვანი სპექტრის მოცულობიდან გამომდინარე, წინამდებარე კვლევის მიზანია ვიდეომონიტორინგის განხორციელების ერთ-ერთი მიმართულების - დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგთან დაკავშირებული არსებითი საკითხების წარმოჩენა. შესაბამისად, ნაშრომის ფარგლებში განხილული იქნება აღნიშნული თემატიკის საკანონმდებლო რეგულირება, განიმარტება დასაქმებულის სამუშაო სივრცისა თუ პროცესის არსი, ასევე, პირადი ცხოვრების დაცულობის გონივრული მოლოდინის სტანდარტი. ამასთან, კვლევის ძირითად ნაწილში მოცემული იქნება პერსონალურ მონაცემთა დაცვის სამსახურის, ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოებისა და ადამიანის უფლებათა ევროპული სასამართლოს რელევანტური, საუკეთესო პრაქტიკა.

2. ვიდეომონიტორინგის განხორციელების საკანონმდებლო რეგულირება

ვიდეომონიტორინგი არის საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ვიზუალური გამოსახულების მონაცემთა დამუშავება, კერძოდ, ვიდეოკონტროლი ან/და ვიდეოჩაწერა (გარდა ფარული საგამოძიებო მოქმედებისა).[2] განსხვავებით 2024 წლის პირველი მარტიდან ამოქმედებული კანონისა, „პერსონალურ მონაცემთა დაცვის შესახებ“ 2011 წლის 28 დეკემბრის კანონი ვიდეომონიტორინგის ცნებას არ ითვალისწინებდა, თუმცა ვიდეოჩაწერას მონაცემთა დამუშავების ერთ-ერთ ფორმად მიიჩნევდა. ევროპული კანონმდებლობის იმპლემენტაციისა და მასთან ჰარმონიზაციის მიზნის გათვალისწინებით, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონით სრულყოფილად მოწესრიგდა ვიდეომონიტორინგთან დაკავშირებული საკითხები. განისაზღვრა დასაქმებულის სამუშაო პროცესისა თუ სივრცის ვიდეომონიტორინგის განხორციელების საფუძვლები.

ვიდეომონიტორინგი პერსონალურ მონაცემთა დამუშავების დასაშვები ფორმაა, თუ იგი მიმდინარეობს დანაშაულის თავიდან აცილების, მისი გამოვლენის, საზოგადოებრივი უსაფრთხოების, პირის უსაფრთხოებისა და საკუთრების დაცვის, არასრულწლოვანის დაცვის (მათ შორის, მავნე ზეგავლენისგან დაცვის), საიდუმლო ინფორმაციის დაცვის, გამოცდის/ტესტირების მიზნებისთვის, აგრეთვე სხვა საჯარო ან/და სხვა ლეგიტიმური ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესასრულებლად, თუ ვიდეომონიტორინგის განხორციელება მონაცემთა დამუშავების მიზნის ადეკვატური და პროპორციული საშუალებაა[3].

დასაქმებული პირის სამუშაო ადგილზე ვიდეომონიტორინგის განხორციელების მიზანი შესაძლოა განსხვავდებოდეს იმისდა მიხედვით, თუ რა სახის სამუშაო პროცესი მიმდინარეობს, როგორია სამუშაო სივრცის სპეციფიკა და ა.შ[4]. სწორედ შესასრულებელი სამუშაოს სპეციფიკიდან გამომდინარე, ზოგიერთ შემთხვევაში დამსაქმებელი ვალდებულიც[5] კია განახორციელოს ვიდეომონიტორინგი[6]. შრომითი ურთიერთობების მრავალფეროვანი ხასიათიდან გამომდინარე, მოქმედი კანონმდებლობა იძლევა შესაძლებლობას, პერსონალურ მონაცემთა დაცვის საზედამხედველო

[2] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 3, ქვეპუნქტი „ღ“.

[3] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 10, პუნქტი 1.

[4] მაგალითად, „ზოგადი განათლების შესახებ“ საქართველოს კანონის მე-20 მუხლის მე-17 პუნქტით განსაზღვრულია, რომ პირის უსაფრთხოების დაცვისა და მავნე ზეგავლენისაგან არასრულწლოვნის დაცვის მიზნით უნდა განხორციელდეს ვიდეოთვალთვალი სკოლის გარე და შიდა პერიმეტრებზე.

[5] იხ., მაგალითად, „აზარტული და სხვა მომგებიანი თამაშობების (გარდა წამახალისებელი გათამაშებისა) ადგილებზე და გარე პერიმეტრზე ვიდეომეთვალყურეობის სისტემებისა და მათი დამონტაჟება-ექსპლუატაციის წესის დამტკიცების შესახებ“ საქართველოს შინაგან საქმეთა მინისტრის 2007 წლის 29 აგვისტოს №1143 ბრძანება.

[6] *ტაკაშვილი ს.*, პერსონალური მონაცემების დამუშავების სტანდარტი დასაქმებულის სამუშაო სივრცის ვიდეომონიტორინგისას, სამართლის მეთოდები, №8, 2024, 129.

ორგანომ თითოეულ, კონკრეტულ შემთხვევაში შეაფასოს დამსაქმებლის ის ლეგიტიმური ინტერესი, რაც უშუალოდ არ არის მითითებული კანონში, თუმცა მიეკუთვნება „სხვა ლეგიტიმური ინტერესის სფეროს“. ამისგან განსხვავებით, 2024 წლის პირველ მარტამდე მოქმედი კანონის რეგულაცია 7 სამუშაო ადგილზე ვიდეოთვალთვალის სისტემის განთავსების კანონისმიერ მიზნად ადგენდა მხოლოდ პირის უსაფრთხოებისა და საკუთრების, საიდუმლო ინფორმაციის დაცვისა და გამოცდის/ტესტირების მიზნებს. ამდენად, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოქმედი რეგულაცია შეფასების მეტ სივრცეს ტოვებს, რათა კომპლექსური საკითხები კანონიერად და სამართლიანად გადაწყდეს.

პერსონალურ მონაცემთა დაცვის სამართალში მნიშვნელოვანი ადგილი უკავია ევროპის საბჭოს პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ 1981 წლის 28 იანვრის 108-ე კონვენციას და ასევე, მოდერნიზებულ 108-ე კონვენციას. პერსონალური მონაცემების დამუშავების უმთავრეს საერთაშორისო აქტად კი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (შემდგომში - “GDPR”) გვევლინება. საგულისხმოა, რომ როგორც აღნიშნული კონვენციები, ისე “GDPR”-ი ვიდეომონიტორინგის მეშვეობით პერსონალურ მონაცემთა დამუშავების წესებს არ ითვალისწინებს, თუმცა ერთმნიშვნელოვნად ადგენს, რომ დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირები ამ გზით მონაცემთა დამუშავებისას უნდა მოქმედებდნენ მონაცემთა სუბიექტის ღირსების, კანონიერი ინტერესებისა და ფუნდამენტური უფლებების დაცვის ვალდებულებიდან გამომდინარე.

ამდენად, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოები (DPAs) ვიდეომონიტორინგის გზით დასაქმებულის პერსონალური მონაცემების დამუშავების კანონიერების შესწავლის პროცესში ხელმძღვანელობენ ეროვნული კანონმდებლობით, ევროკონვენციებით და GDPR-ის იმ რელევანტური ნორმებით, რომლებითაც გათვალისწინებულია პერსონალური მონაცემების დამუშავებასთან დაკავშირებული პრინციპები თუ მონაცემთა დამუშავების ზოგადი წესები.

3. დასაქმებული პირის სამუშაო სივრცე/პროცესი

დასაქმებული პირი, ისევე როგორც დამსაქმებელი, შრომითი ურთიერთობის სუბიექტია. დასაქმებული არის ფიზიკური პირი, რომელიც შრომითი ხელშეკრულების საფუძველზე, დამსაქმებლისათვის ასრულებს გარკვეულ სამუშაოს. იგი, ასევე, შესაძლებელია იყოს „საჯარო სამსახურის შესახებ“ საქართველოს კანონით გათვალისწინებული საჯარო მოსამსახურე.[8]

[7] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011, მუხლი 12, პუნქტი 3.

[8] საქართველოს ორგანული კანონი „საქართველოს შრომის კოდექსი“, 4113-რს, 17/12/2010, მუხლი 3, პუნქტი 3. ასევე, „საჯარო სამსახურის შესახებ“ საქართველოს კანონის მე-3 მუხლის „დ“ ქვეპუნქტის თანახმად, საჯარო მოსამსახურე არის პროფესიული საჯარო მოხელე/საჯარო მოხელე/მოხელე,

„შრომის ინსპექციის შესახებ“ საქართველოს კანონში მოცემულია დასაქმებული პირისა და მისი სამუშაო სივრცის/ადგილის განმარტება, რომლის მე-3 მუხლის „კ“ და „ლ“ ქვეპუნქტების თანახმად, კონკრეტული ადგილი, სადაც დასაქმებული უშუალოდ ახორციელებს შრომით საქმიანობას სამუშაო ადგილად მიიჩნევა, ხოლო სამუშაო სივრცე არის ყველა სამუშაო ადგილისა და იმ ტერიტორიის ერთობლიობა, სადაც დასაქმებული ან სხვა პირი სამსახურებრივი დანიშნულებით იმყოფება/გადაადგილდება და რომელსაც დამსაქმებელი პირდაპირ ან არაპირდაპირ აკონტროლებს.[9] იდენტურ განმარტებას ვხვდებით, მაგალითად, „სამუშაო სივრცეში უსაფრთხოებისა და ჯანმრთელობის დაცვის მინიმალური მოთხოვნების შესახებ ტექნიკური რეგლამენტის დამტკიცების თაობაზე“ საქართველოს მთავრობის 2022 წლის 1 ივლისის №341 დადგენილებაშიც. ამავე დადგენილებით გამიჯნულია ღია და დახურული სამუშაო სივრცეებიც. თუმცა, სამუშაო ადგილისა და სივრცის შესაძლო სპეციფიკური ხასიათიდან გამომდინარე, კანონქვემდებარე ნორმატიულ აქტებში მსგავსი ტერმინების განსხვავებულ განმარტებასაც ვხვდებით.[10]

რაც შეეხება სამუშაო პროცესს, იგი დაკავშირებულია დასაქმებული პირის უშუალო საქმიანობასთან, აღნიშნული შრომითი პროცესი კი შესაძლოა განსხვავდებოდეს მისი ხანგრძლივობით, შესასრულებელი სამუშაოს თავისებურებით და სხვა. სამუშაო პროცესი შესაძლოა გულისხმობდეს არა მხოლოდ მის დახურულ, არამედ ღია ცის ქვეშ წარმოებასაც, რაც გამოიკვეთა პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ერთ-ერთ კომპანიაში დასაქმებული პირების მონაცემთა დამუშავების კანონიერების შესწავლისას[11]. საქმის გარემოებების მიხედვით, კომპანია მონაცემთა დამუშავებაზე უფლებამოსილი პირის მეშვეობით, სამხრე კამერების გზით, ახორციელებდა გარე სივრცეებში მომუშავე დასაქმებულების ვიდეომონიტორინგს, ვინაიდან არსებობდა თანამშრომლების ჯანმრთელობის დაზიანების მაღალი რისკი. შესწავლის პროცესში დადგინდა, რომ აღნიშნული გარე სივრცეები კომპანიის თანამშრომლების ძირითადი სამსახურებრივი ფუნქცია-მოვალეობების შესასრულებლად განკუთვნილ ადგილს წარმოადგენდა. ამდენად, სამუშაო ადგილზე ვიდეომონიტორინგის წესების დარღვევიდან გამომდინარე (კომპანიას არ ჰქონდა შემუშავებული წერილობითი დოკუმენტი ვიდეომონიტორინგის განხორციელების თაობაზე), იგი ცნობილ იქნა სამართალდამრღვევად „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის 69-ე მუხლის საფუძველზე. შესაბამისად, სამუშაო პროცესების

ადმინისტრაციული ხელშეკრულებით დასაქმებული პირი, შრომითი ხელშეკრულებით დასაქმებული პირი.

[9] შეად. რეკომენდაციები ვიდეომონიტორინის და აუდიომონიტორინგის განხორციელების თაობაზე, 2024, 8.

[10] მაგალითად, საქართველოს განათლებისა და მეცნიერების მინისტრის 2021 წლის 29 დეკემბრის №104/ნ ბრძანება, მუხლი 3, ქვეპუნქტი „დ“.

[11] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 20 ნოემბრის №გ-1/340/2024 გადაწყვეტილება.

განსხვავებულობის მიუხედავად, კანონი დასაქმებული პირების პერსონალურ მონაცემებს თანაბრად იცავს.

4. პირადი ცხოვრების დაცულობის გონივრული მოლოდინის სტანდარტი

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი ვიდეომონიტორინგის განხორციელებას გამორიცხავს ისეთ სივრცეში, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს.[12]

პირადი ცხოვრების დაცულობის გონივრული მოლოდინი განისაზღვრება არა ფიზიკური პირის სუბიექტური შეხედულებით, არამედ ობიექტური დამკვირვებლის, მესამე მხარის თვალთახედვიდან[13]. დასაქმებული პირის სამუშაო ადგილზე პირადი ცხოვრების დაცულობის გონივრული მოლოდინი ობიექტურად არსებობს ისეთ სივრცეებში, როგორიცაა, მაგალითად, ჰიგიენისთვის განკუთვნილი ადგილები. ასევე, თუ შესასრულებელი სამუშაო განსაკუთრებული სპეციფიკით ხასიათდება და საჭიროებს გამოსაცვლელი ოთახების არსებობას, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით, ყოველგვარი გამონაკლისის გარეშე, არ დაიშვება ასეთი სივრცის ვიდეომონიტორინგი. ამ და მსგავს სივრცეებში ვიდეომონიტორინგის განხორციელება საყოველთაოდ აღიარებულ ზნეობრივ ნორმებს ეწინააღმდეგება. თუმცა, იქიდან გამომდინარე, რომ თითოეული სივრცის *Numerus Clausus* პრინციპით გათვალისწინება შეუძლებელია, კანონმდებელმა დაამკვიდრა ტერმინი - პირადი ცხოვრების დაცულობის გონივრული მოლოდინი.

გარდა ზემოთ ჩამოთვლილი შემთხვევებისა, დასაქმებულს სამუშაო ადგილზე პირადი ცხოვრების დაცულობის გონივრული მოლოდინი შესაძლოა გაუჩნდეს სამუშაო ადგილზე განთავსებულ სამზარეულოში, სადაც იგი, ძირითადად, იმყოფება შესვენებისთვის განკუთვნილ დროს. მსგავსი მოლოდინის არსებობა გონივრულია ასევე ისეთ სამუშაო ადგილზე, სადაც არსებობს დღისა და ღამის ცვლა (მაგალითად, სამედიცინო დაწესებულებები, ობიექტის დაცვის კომპანიები) და როდესაც ამგვარ დაწესებულებებში ვხვდებით მოსასვენებელ სივრცეებს[14].

„გარკვეულ გარემოში ადამიანს პირადი ცხოვრების დაცულობისა და პატივისცემის ლეგიტიმური მოლოდინი აქვს“[15]. ამდენად, პირადი ცხოვრების დაცულობის მომეტებული საჭიროებიდან გამომდინარე, კანონმდებელი

[12] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 10, პუნქტი 4.

[13] *European Data Protection Board (EDPB),* Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §36.

[14] მაგალითად, „ზოგადსაგანმანათლებლო დაწესებულებაში უსაფრთხოებისა და საზოგადოებრივი წესრიგის დაცვის წესისა და პირობების დამტკიცების შესახებ“ საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის მინისტრის 2019 წლის 29 იანვრის №06/ნ ბრძანებით დადგენილია, რომ დაუშვებელია ვიდეოთვალთვალის განხორციელება სკოლის საპირფარეშოში, გამოსაცვლელ ოთახებში, საკლასო ოთახში და სამასწავლებლოში.

[15] *Case of Von Hannover v. Germany,* [2004] ECHR App. No. 59320/00, §51.

ყოველგვარი გამონაკლისის გარეშე კრძალავს მსგავსი სივრცეების ვიდეომონიტორინგს და შესაბამისად, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის 69-ე მუხლიც ჯარიმის სახით უფრო მეტად მაღალ სანქციას ითვალისწინებს იმ შემთხვევისთვის, როდესაც დამუშავებისთვის პასუხისმგებელი პირი ვიდეომონიტორინგს ახორციელებს სივრცეში, სადაც მონაცემთა სუბიექტის პირადი ცხოვრების დაცულობის გონივრული მოლოდინი არსებობს.

5. “Ultima Ratio”-ს პრინციპის მნიშვნელობა დასაქმებულის სამუშაო სივრცის/პროცესის ვიდეომონიტორინგისას

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-10 მუხლის მე-3 პუნქტის მიხედვით, დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი დასაშვებია მხოლოდ გამონაკლის შემთხვევაში, თუ კანონით განსაზღვრული მიზნების მიღწევა სხვა საშუალებით შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. ვიდეომონიტორინგის განხორციელების სამართლებრივი, ლეგიტიმური საფუძვლები განსაზღვრულია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-10 მუხლის პირველი პუნქტით (პირის უსაფრთხოებისა და საკუთრების დაცვა, საზოგადოებრივი უსაფრთხოება და ა.შ.). მიუხედავად ამისა, დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგის განხორციელების კანონიერად მიჩნევისთვის კანონმდებელი აწესებს უფრო მაღალ სტანდარტებს და განსაზღვრავს, რომ კანონისმიერი მიზნის არსებობასთან ერთად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დაამტკიცოს, რომ დასახული მიზანი სხვა საშუალების გამოყენებით ვერ მიიღწევა ან ალტერნატიული მეთოდის გამოყენება არაპროპორციულად დიდ ძალისხმევას საჭიროებს. შესაბამისად, სამუშაო სივრცის/პროცესის ვიდეომონიტორინგი, როგორც *Ultima Ratio*, განსაკუთრებულ შემთხვევებშია დასაშვები, როდესაც არ არსებობს სხვა ლოგიკური და ნაკლებად მზღუდავი ალტერნატივა, რაც პირადი ცხოვრების უფლებაში ჩარევას გაამართლებს.

საკითხის პრაქტიკული მიმოხილვისთვის საინტერესოა პერსონალურ მონაცემთა დაცვის სამსახურის მიერ გეგმური ინსპექტირების ფარგლებში ერთ-ერთი კერძო სკოლის მიერ ვიდეომონიტორინგის განხორციელების კანონიერების შესწავლის საკითხი[16]. საქმის გარემოებების მიხედვით, სკოლის ინფორმატიკის საკლასო ოთახში ხორციელდებოდა ვიდეომონიტორინგი. სკოლის წარმომადგენლის განმარტებით, ვიდეომონიტორინგის მიზანს წარმოადგენდა საკუთრების დაცვა, უსაფრთხოების პრევენცია და ზარალის მიმყენებელი პირის იდენტიფიცირება. გარდა ამისა, ვიდეომონიტორინგი ხორციელდებოდა ტესტირების მიზნით, პერიოდულად განსახორციელებელი

[16] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 22 ნოემბრის №გ-1/342/2024 გადაწყვეტილება.

საგანმანათლებლო პროექტების ფარგლებში. შემოწმებისას გამოიკვეთა, რომ სკოლას განათლების სამინისტროსთან შეთანხმებული ჰქონდა „უსაფრთხოების წესი“, რომლითაც სხვა სივრცეებთან ერთად საკლასო ოთახებში ვიდეომონიტორინგი დაუშვებლად იყო მიჩნეული. ამდენად, გარდა იმისა, რომ ინფორმატიკის საკლასო ოთახში ვიდეომონიტორინგის მიმდინარეობა აღნიშნულ წესს არღვევდა, სამსახურის შეფასებით, იგი არ იყო დასახელებული მიზნების მიღწევის ადეკვატური და პროპორციული საშუალება, ვინაიდან საკუთრების დაცვა, უსაფრთხოების პრევენცია და ზარალის მიმყენებელი პირის იდენტიფიცირება სხვა ალტერნატიული საშუალებებითაც შეიძლებოდა, ასეთად კი დასახელდა მასწავლებლებთან დადებულ ხელშეკრულებებში, მატერიალური ფასეულობის დაცვის მიზნით, შესაბამისი ვალდებულებების გაწერა, ასევე, ნივთებზე პასუხისმგებელი/მეთვალყურე პირის გამოყოფა. რაც შეეხება ტესტირების მიზანს, მიუხედავად იმისა, რომ აღნიშნული მიზანი შესაძლოა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-10 მუხლის პირველ პუნქტში პირდაპირ სახელდება, დადგინდა, რომ საკლასო ოთახში ტესტირების მონიტორინგის მიზნის მიღწევა შესაძლებელი იყო მხოლოდ და მხოლოდ უშუალოდ ამ პროცესის ვიდეომონიტორინგით, ხოლო ტესტირების დაწყებამდე და დასრულების შემდგომ ვიდეომონიტორინგის განხორციელება დასახელებულ მიზანს სცდებოდა. ამდენად, კანონის 69-ე მუხლის (ვიდეომონიტორინგის განხორციელების წესების დარღვევა) შესაბამისად, სკოლა ცნობილ იქნა სამართალდამრღვევად.

საგანმანათლებლო დაწესებულება წარმოადგენს სივრცეს, სადაც სასწავლო პროცესში ჩაბმული არიან როგორც მოსწავლეები/სტუდენტები, ისე დასაქმებული პირები (მაგალითად, მასწავლებლები, ლექტორები). შესაბამისად, ასეთ დაწესებულებებში არსებული სივრცეები იმავდროულად წარმოადგენს დასაქმებულების სამუშაო სივრცეს. შესაბამისად, ვიდეომონიტორინგის განხორციელების მიზანი უნდა ამართლებდეს პირად ცხოვრებაში ჩარევას. ადამიანის უფლებათა ევროპულმა სასამართლომ, საქმეზე „ანტოვიჩი და მირკოვიჩი მონტენეგროს წინააღმდეგ“, განმარტა, რომ აუდიტორია წარმოადგენს ლექტორების სამუშაო ადგილს, სადაც ისინი არა მხოლოდ ასწავლიან სტუდენტებს, არამედ ურთიერთობენ მათთან და თავიანთ სოციალურ იდენტობას ავითარებენ. რამდენადაც სასწავლო პროცესზე ზედამხედველობის განხორციელებას, როგორც ვიდეომონიტორინგის მიზანს, ეროვნული კანონმდებლობა არ ითვალისწინებდა, ხოლო პირთა უსაფრთხოების დაცვის რეალური აუცილებლობა არ გამოვლინდა, სასამართლომ აუდიტორიების ვიდეომონიტორინგი ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევად მიიჩნია[17].

[17] *Case of Antović and mirković v. Montenegro*, [2017] ECHR App. No. 70838/13, §44, §55-§60.

Ultima Ratio-ს პრინციპის მნიშვნელობა ნათლად იკვეთება პერსონალურ მონაცემთა დაცვის სამსახურის კიდევ ერთ გადაწყვეტილებაში[18], რომლის მიხედვით, დამუშავებისთვის პასუხისმგებელი პირი (კოლეჯი) რამდენიმე აუდიტორიაში (მათ შორის, სახელოსნო, სამკერვალო, ინტეგრირებული ლაბორატორია) განთავსებული ვიდეოკამერების მეშვეობით ახორციელებდა ვიდეომონიტორინგს. დამუშავებისთვის პასუხისმგებელი პირი აღნიშნული სივრცეების მონიტორინგის მიზნად ასახელებდა აუდიტორიებში განთავსებული, ძვირადღირებული მოწყობილობებისა და ინვენტარის დაცვას. გადაწყვეტილებაში აღინიშნა, რომ აუდიტორია, თავისი არსით, წარმოადგენს სტუდენტებისათვის სასწავლო და პედაგოგებისთვის სამუშაო სივრცეს, სადაც ერთმანეთს შორის კომუნიკაციის საგანს განეკუთვნება არა მხოლოდ სასწავლო თემატიკა, არამედ პირადი და ზოგადი ხასიათის საკითხებიც. მიუხედავად იმისა, რომ საკუთრების დაცვა ლეგიტიმურ მიზნად მიიჩნევა, არსებობდა აღნიშნული მიზნის მიღწევის სხვა, ალტერნატიული საშუალებები, კერძოდ, კოლეჯში ყოველწლიურად ტარდებოდა ინვენტარიზაცია, ასევე, პედაგოგებთან დადებული ხელშეკრულება ითვალისწინებდა მათ პასუხისმგებლობას კოლეჯის მატერიალურ ქონებაზე. დასახული მიზნის მიღწევა შეიძლებოდა, ასევე, ნივთებზე პასუხისმგებელი პირის გამოყოფით, ძვირადღირებული ინვენტარის დაცულ სივრცეში შენახვით, მათი გამოყენებისა და დაბრუნების ფაქტების აღრიცხვით. ასე რომ, აღნიშნულ სივრცეებში ვიდეომონიტორინგის განხორციელება კოლეჯის მიერ დასახელებული მიზნის მიღწევის აუცილებელი, ადეკვატური საშუალება არ იყო. ამდენად, ვინაიდან ვიდეომონიტორინგის განხორციელება არ წარმოადგენდა დასახული მიზნის მიღწევის ერთადერთ საშუალებას, ვიდეომონიტორინგის სისტემის განთავსების სამართლებრივი საფუძველი არ არსებობდა, შესაბამისად, კოლეჯს დაევალა სასწავლო აუდიტორიებში ვიდეომონიტორინგის შეწყვეტა.

დასაქმებულის სამუშაო სივრცის/პროცესის ვიდეომონიტორინგის დასაშვებობის ზემოაღნიშნული, განსაკუთრებული რეგულირება გამომდინარეობს როგორც პირადი ცხოვრების უფლების დაცვის აუცილებლობიდან, ასევე სხვა ფუნდამენტურ უფლებებზე (მაგალითად, შეკრების თავისუფლება) ე. წ. „მსუსხავი ეფექტის“[19] მოხდენის მაღალი ალბათობიდან. მაშასადამე, ლეგიტიმური ინტერესის არსებობასთან ერთად, ვიდეომონიტორინგი დასაქმებულის მონაცემთა დამუშავების მიზნის ადეკვატურ და პროპორციულ საშუალებას უნდა წარმოადგენდეს.

[18] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 26 ნოემბრის №გ-1/346/2024 გადაწყვეტილება.

[19] პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების თაობაზე, 2024, 8.

6. დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების ძირითადი ვალდებულებები

6.1. ინფორმირების ვალდებულება

მას შემდეგ, რაც დამსაქმებელს სამუშაო ადგილზე „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით გათვალისწინებული ვიდეომონიტორინგის განხორციელების საფუძველი ექნება, მას, როგორც დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირს, წარმოეშობა არაერთი ვალდებულება. მაგალითად, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-10 მუხლის მე-8 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშანი[20] თვალსაჩინოდ განათავსოს, ხოლო ამ მუხლის მე-3 პუნქტით განსაზღვრულ შემთხვევაში – დამატებით, დასაქმებული პირი წერილობით გააფრთხილოს ვიდეომონიტორინგის კონკრეტული მიზნის (მიზნების) შესახებ. აღნიშნული მოთხოვნების დაცვის შემთხვევაში მონაცემთა სუბიექტი მის შესახებ მონაცემთა დამუშავების თაობაზე ინფორმირებულად მიიჩნევა.

ამდენად, კანონი ერთმნიშვნელოვნად განსაზღვრავს, რომ ვიდეომონიტორინგის მეშვეობით დასაქმებული პირის პერსონალური მონაცემის (ვიზუალური გამოსახულების) დამუშავება დაუშვებელია იმგვარად, რომ მონაცემთა სუბიექტისთვის აღქმადი არ იყოს ამ პროცესების შესახებ. გამჭვირვალობის პრინციპის დაცვის მნიშვნელობიდან გამომდინარე, კანონმდებლობა დასაქმებული პირის სამუშაო სივრცის/პროცესის ვიდეომონიტორინგის შემთხვევაში აწესებს ინფორმირების კიდევ უფრო მაღალ სტანდარტს და გარდა გამაფრთხილებელი ნიშნის განთავსებისა, დამსაქმებელს, როგორც დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირს, აკისრებს ვალდებულებას, დასაქმებული პირები წერილობით გააფრთხილოს ვიდეომონიტორინგის კონკრეტული მიზნ(ებ)ის შესახებ. აქედან გამომდინარე, თუ მონაცემთა დამუშავება გამჭვირვალობის პრინციპის დაცვით არ განხორციელდება, იარსებებს რისკი იმისა, რომ დამსაქმებლის ინტერესი (მაგალითად, უზრუნველყოს მისი საკუთრების უსაფრთხოება) გაუმართლებელ, არალეგიტიმურ მიზნად გარდაიქმნას[21].

დამსაქმებლის მიერ დასაქმებული პირის ინფორმირების ვალდებულების შეუსრულებლობის კუთხით მნიშვნელოვანია ადამიანის

[20] ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშანი უნდა შეიცავდეს შესაბამის წარწერას, მარტივად აღქმად გამოსახულებას ვიდეომონიტორინგის მიმდინარეობის თაობაზე და დამუშავებისთვის პასუხისმგებელი პირის სახელწოდებასა და მის საკონტაქტო მონაცემებს.

[21] *Article 29 Data Protection Working Party*, Opinion 2/2017 on Data Processing at Work, Adopted on 8 June 2017, 9.

უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ლოპეზ რიბალდა და სხვები ესპანეთის წინააღმდეგ“[22]. საქმის ფაქტობრივი გარემოებების მიხედვით, მომჩივნები ბარსელონაში მდებარე ერთ-ერთ სუპერმარკეტში მოლარეებად და კონსულტანტებად მუშაობდნენ. სუპერმარკეტის ადმინისტრაციამ 2009 წლის მარტში შეიტყო კომპანიის ფინანსური დანაკარგების შესახებ. აღნიშნულის მიზეზის გამოსააშკარავებლად გადაწყდა ვიდეოკამერების მონტაჟი. განთავსებული ვიდეოკამერებიდან ზოგიერთი იყო ფარული, რომელთა ხედვის არეალში სალაროები ექცეოდა. კომპანიამ ხილული ვიდეოკამერების განთავსების თაობაზე დასაქმებულებს აცნობა და გამაფრთხილებელი ნიშანიც განათავსა. რამდენიმე თვეში კომპანიის 14 თანამშრომელთან, მათ შორის მოსარჩელეებთან, კომპანიის კუთვნილი ნივთების/პროდუქტების ქურდობის გამო შრომითსამართლებრივი ურთიერთობა შეწყდა. ადამიანის უფლებათა ევროპული სასამართლოს პალატის გადაწყვეტილებით დადგინდა კონვენციის მე-8 მუხლის დარღვევა, რადგან დასაქმებული პირები არ ყოფილან სრულად ინფორმირებული ვიდეომონიტორინგის შესახებ და არ იქნა დაცული სამართლიანი ბალანსი პირადი ცხოვრების პატივისცემის უფლებისა და მეორე მხარის ინტერესებს შორის. გადაწყვეტილება მოპასუხე მხარემ დიდ პალატაში გაასაჩივრა. დიდი პალატის შეფასებით, სუპერმარკეტი ღია სივრცეს წარმოადგენდა და სალაროში თანხის გადახდა პირადი სახის არ ყოფილა, თუმცა, ვიდეომონიტორინგი იმავდროულად ხორციელდებოდა სამუშაო ადგილზე. გადაწყვეტილებაში ხაზი გაესვა დასაქმებულის პირადი ცხოვრების დაცულობის გონივრული მოლოდინის საკითხს და აღინიშნა, რომ ამგვარი მოლოდინი ნაკლებად არსებობს სივრცეში, სადაც სამსახურებრივი ფუნქციები საჯაროდ, მომხმარებლებთან ვერბალური კონტაქტით გამოიხატება. ამასთან, იმის გათვალისწინებით, რომ თვალთვალი მხოლოდ 10 დღის განმავლობაში გაგრძელდა და ჩანაწერებზე წვდომა პირთა შეზღუდულ წრეს ჰქონდა, პირად ცხოვრებაში ჩარევის სიმძიმე მაღალი ხარისხის არ იყო, ხოლო იმ შემთხვევაში, თუ დასაქმებულები ვიდეომონიტორინგის შესახებ ინფორმირებული იქნებოდნენ, დამსაქმებლის მიზანი - დაედგინა სუპერმარკეტში ქურდობის მიზეზები, მიღწეული ვერ იქნებოდა. ევროსასამართლომ ხაზი გაუსვა დასაქმებულის ინფორმირების განსაკუთრებულ მნიშვნელობას და აღნიშნა, რომ გაუმართლებელია მცირედი ეჭვის დროს დასაქმებულების უკანონო ქმედებათა გამოვლენის მიზნით ვიდეომონიტორინგის ფარულად განხორციელება. თუმცა, მიუხედავად ამისა, სასამართლომ განმარტა, რომ დასაქმებულთა უკანონო ქმედებების შესახებ გონივრული ეჭვის არსებობისას, რასაც თან ახლავს ზარალის დიდი მოცულობაც, ინფორმირების ვალდებულების არსებობის მიუხედავად, გამართლებული იყო კომპანიის მენეჯმენტის მიერ ზემოაღნიშნული ზომების მიღება, რათა თანამშრომელთა ქმედებებს კომპანიის საქმიანობის პარალიზება არ გამოეწვია. ამდენად, პირადი ცხოვრების უფლებაში ჩარევა მართლზომიერი აღმოჩნდა.

[22] *Case of López Ribalda and others v. Spain*, [2019] ECHR App. No. 1874/13; 8567/13.

პირადი ცხოვრების უფლების დარღვევა არ დაადგინა ადამიანის უფლებათა ევროპულმა სასამართლომ კიდევ ერთ-ერთ საქმეში, რომელიც ზემოაღნიშნულ გადაწყვეტილებაში მითითებული გარემოებების მსგავსია. საქმე ეხებოდა დამსაქმებლის მიერ დასაქმებული პირის (მოლარის) ფარულ ვიდეომონიტორინგს. სასამართლომ დამსაქმებლის მიზანი - დაეცვა საკუთარი ქონება და გამოევლინა ქურდობის შემთხვევები, მიიჩნია ღირებულ ლეგიტიმურ ინტერესად, რომლის მიღწევა სხვა თანაბრად ეფექტური საშუალებით შეუძლებელი იქნებოდა.[23]

გარდა ზემოაღნიშნულისა, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანოს ("ICO") მიერ შემუშავებულ, დასაქმებულ პირთა კანონიერი მონიტორინგის შესახებ სახელმძღვანელოში ვკითხულობთ, რომ იმ საგამონაკლისო შემთხვევებში, რაც გულისხმობს, მაგალითად, სისხლის სამართლის დანაშაულის პრევენციას/გამოვლენას, დასაშვებია სამუშაო ადგილზე ფარული ვიდეომონიტორინგის განხორციელება. ამასთან, სხვა საკითხებთან ერთად გათვალისწინებული უნდა იყოს, რომ ვიდეომონიტორინგი მხოლოდ უფლებამოსილმა პირებმა განახორციელონ მკაცრად შეზღუდული დროისა და ვიდეოკამერების ლიმიტირებული ხედვის არეალის გათვალისწინებით[24] და არსებობდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება.[25] თუმცა, დასახელებული მიზნის არსებობის მიუხედავად, დაუშვებელია ფარული ვიდეომონიტორინგი იმ სივრცეებში, სადაც დასაქმებულს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს[26] (მაგალითად, საპირფარეშო, გამოსაცვლელი ოთახები და ა.შ.).

„პერსონალურ მონაცემთა დაცვის შესახებ" კანონის მიხედვით, დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი შესაძლოა დანაშაულის გამოვლენის მიზნით ხორციელდებოდეს. კანონი უშუალოდ დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის მიერ დასაქმებული პირის სამუშაო პროცესის/სივრცის ფარული ვიდეომონიტორინგის შესაძლებლობას არ ითვალისწინებს, არამედ, ერთმნიშვნელოვნად განსაზღვრავს დასაქმებულების, როგორც მონაცემთა სუბიექტების წერილობითი გაფრთხილების ვალდებულებას. სამუშაო ადგილზე ფარული ვიდეომონიტორინგი, თავისი არსით, პირად ცხოვრებაში ჩარევის ძალიან მძიმე შემთხვევაა, აღნიშნული შესაძლებლობა კი დამსაქმებლის მიერ დასაქმებული პირების პირადი ცხოვრების ამსახველი სხვა სახის ინფორმაციის უკანონო მოპოვების რისკებს ქმნის[27]. აქედან გამომდინარე, რადგან ადამიანის უფლებათა ევროპული სასამართლოს მიერ

[23] *Case of Köpke v. Germany*, [2010] ECHR, App. No. 420/07.

[24] *EDPS*, Video-Surveillance Guidelines, Brussels, 17 March 2010, 31-32 <https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> [16.12.2024].

[25] მსოფლიო პრაქტიკა, პერსონალურ მონაცემთა დაცვის სამსახური, 2023, ოქტომბერი, 7-8.

[26] Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].

[27] რაც შესაძლოა სისხლის სამართლის კოდექსით გათვალისწინებულ პასუხისმგებლობას იწვევდეს (მაგალითად, პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა (სისხლის სამართლის კოდექსი, №2287, მუხლი 157).

ზემოაღნიშნულ გადაწყვეტილებებში მოცემული პრეცედენტული განმარტებების თანახმად, განსაკუთრებული გარემოებების არსებობის შემთხვევაში სამუშაო ადგილზე ფარული ვიდეომონიტორინგი დასაშვებია, მიზანშეწონილია მისი განხორციელება არა თავად დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირთა მიერ, არამედ სამართალდამცავი ორგანოების მხრიდან (მაგალითად, სისხლის სამართლის დანაშაულის გამოვლენის მიზნით).

მონაცემთა სუბიექტის სათანადო ინფორმირების მნიშვნელობა იკვეთება პერსონალურ მონაცემთა დაცვის სამსახურის მიერ დადგენილი ერთგვაროვანი პრაქტიკის[28] მიხედვითაც, რომლის თანახმად, დაუშვებელია სამუშაო ადგილზე ისეთი ვიდეოკამერების არსებობა, რომლებიც არ ფუნქციონირებს. კერძოდ, იმ შემთხვევაში თუ ვიდეოკამერა დამონტაჟებულია, მაგრამ არ მუშაობს, დამსაქმებელი ვალდებული იქნება მოახდინოს ასეთი ვიდეოკამერ(ებ)ის დემონტაჟი ან ვიდეომონიტორინგი განახორციელოს კანონით დადგენილი წესით, რაც ეფუძნება პირადი ცხოვრების დაცვისა და პატივისცემის მოთხოვნას. დასაქმებული პირი მსგავს შემთხვევაში არ არის ინფორმირებული, რომ არ მიმდინარეობს მისი ვიზუალური გამოსახულების, როგორც პერსონალური მონაცემის, დამუშავება. ამდენად, იგი შეიძლება უსაფუძვლოდ ვარაუდობდეს, რომ მუშავდება მისი პერსონალური მონაცემები, რამაც, დიდი ალბათობით, შესაძლოა მის მიერ საკუთარი ქცევის არაგონივრული კონტროლი გამოიწვიოს.

ინფორმირების ვალდებულების შესრულებით იმავდროულად რეალიზდება მონაცემთა დამუშავების გამჭვირვალობის პრინციპი, ხოლო პერსონალური მონაცემები დამუშავდება კანონიერად, თუ დასაქმებულ პირს ექნება სრულყოფილი ინფორმაცია, რომ სამუშაო სივრცე/პროცესი რეალურად ექვემდებარება ვიდეომონიტორინგს.

6.2. წერილობითი დოკუმენტის შემუშავების ვალდებულება

მონაცემთა სუბიექტის ინფორმირებასთან ერთად, მნიშვნელოვანია, დამუშავებისთვის პასუხისმგებელმა/დამუშავებაზე უფლებამოსილმა პირმა, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-4 მუხლით დადგენილი პრინციპების შესაბამისად, წერილობით განსაზღვროს ვიდეომონიტორინგის მიზანი და მოცულობა, ვიდეომონიტორინგის ხანგრძლივობა და ვიდეოჩანაწერის შენახვის ვადა, ვიდეოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესი და პირობები, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები.

ვიდეომონიტორინგის მეშვეობით მონაცემთა დამუშავების პროცესის გამჭვირვალობის უზრუნველყოფის გარდა, დამსაქმებელი ვალდებულია: პერსონალური მონაცემები შეაგროვოს/მოიპოვოს მხოლოდ კონკრეტული,

[28] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 22 ნოემბრის №გ-1/342/2024 გადაწყვეტილება, 18.

მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის[29]; დაამუშაოს მონაცემები მხოლოდ იმ ვადითა და მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად[30]. სწორედ ამ პრინციპებს ეფუძნება დამსაქმებლის ვალდებულება - წერილობით ჩამოაყალიბოს ის მნიშვნელოვანი საკითხები, რაც ვიდეომონიტორინგს შეეხება. მიუხედავად იმისა, რომ ამავე ვალდებულების მარეგულირებელ ნორმაში არ არის მითითებული აღნიშნული წერილობითი დოკუმენტის მონაცემთა სუბიექტისთვის გაცნობის თაობაზე, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის 24-ე და 25-ე მუხლებით მონაცემთა სუბიექტის ინფორმირების ვალდებულება მსგავსი საკითხების შესახებ მაინც დადგენილია იმის მიუხედავად, მონაცემების შეგროვება ხდება უშუალოდ მონაცემთა სუბიექტისგან თუ არა.

გარდა ზემოაღნიშნულისა, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანოს (“ICO”) მიერ შემუშავებულ ერთ-ერთ სახელმძღვანელოში აღნიშნულია, რომ დასაქმებულ პირთა მონიტორინგისას პერსონალურ მონაცემთა დაცვის მიზნით მნიშვნელოვანია, დამსაქმებელმა განსაზღვროს მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროება. ხოლო იმ შემთხვევაში, თუ ამ პროცესში არსებობს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების ალბათობა[31], დამსაქმებელს ექნება ზეგავლენის შეფასების ვალდებულება.

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ზეგავლენის შეფასებისას შექმნას წერილობითი დოკუმენტი პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №21 ბრძანებით დამტკიცებული წესის შესაბამისად. ამავე ბრძანების თანახმად, ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალების გამოყენებით მონაცემთა დამუშავების შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის შექმნის მაღალი ალბათობა დასაქმებულ პირთა მიმართ შესაძლოა არსებობდეს ორი კუმულატიური პირობის დაკმაყოფილებისას, კერძოდ, იმ შემთხვევაში თუ, მაგალითად, პროფაილინგის შედეგად ხდება დასაქმებულთა მიერ შესრულებული სამუშაოს ხარისხის შეფასება და მიმდინარეობს დასაქმებულთა ქცევის ან მდგომარეობის (მათ შორის, ფიზიკური/ჯანმრთელობის მდგომარეობის) სისტემატური და მასშტაბური მონიტორინგი[32]. ამდენად, დამსაქმებელმა მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროება უნდა შეაფასოს

[29] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 4, პუნქტი 1, ქვეპუნქტი „ბ“.

[30] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 4, პუნქტი 1, ქვეპუნქტები: „გ“; „ე“.

[31] *ICO*, Guideline on Monitoring of Workers by Employers, 2023, p. 20; 35 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf> [20.12.2024].

[32] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №21 ბრძანება, მუხლი 5, ქვეპუნქტი „ა“ და „ბ“.

ზემოაღნიშნული ბრძანებით დადგენილი წესის შესაბამისად, რომლითაც განსაზღვრული პირობების დაკმაყოფილების შემთხვევაში, მას ექნება ვალდებულება, შეიმუშაოს ზეგავლენის შეფასების დოკუმენტი.

6.3. მონაცემთა უსაფრთხოების დაცვის ვალდებულება

დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის კიდევ ერთ ძირითად ვალდებულებად მონაცემთა უსაფრთხოების დაცვა უნდა დავასახელოთ. მონაცემთა უსაფრთხოება, როგორც პრინციპი, გულისხმობს დამუშავებისთვის პასუხისმგებელი/უფლებამოსილი პირის მიერ მონაცემთა დამუშავებისას ისეთი ტექნიკური და ორგანიზაციული ზომების მიღებას, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან[33]. სწორედ აღნიშნულ პრინციპს ეფუძნება „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-10 მუხლის მე-5 პუნქტის მოთხოვნა, რომ ვიდეომონიტორინგის სისტემა და ვიდეოჩანაწერები იყოს დაცული არამართლზომიერი ხელყოფისა და გამოყენებისგან. დამუშავებისთვის პასუხისმგებელ პირს აქვს ვალდებულება, უზრუნველყოს ვიდეოჩანაწერებზე წვდომის თითოეული შემთხვევის აღრიცხვა (ე. წ. „ლოგირება“), მათ შორის, წვდომის დროისა და მომხმარებლის სახელის აღრიცხვა, რაც წვდომის განმახორციელებელი პირის იდენტიფიცირების შესაძლებლობას იძლევა.

უსაფრთხოების გარანტიების შექმნის ვალდებულების მნიშვნელობაზე იმსჯელა საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი გადაწყვეტილების ფარგლებში და განმარტა, რომ დასაქმებულის ვიდეომეთვალყურეობის სისტემა უნდა ყოფილიყო საკმარისად ძლიერი პაროლით დაცული და მასზე წვდომა პირთა შეზღუდულ წრეს უნდა ჰქონოდა.[34] დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირს აქვს ვალდებულება, ვიდეომონიტორინგის სისტემის გამართულობა ხშირად გადაამოწმოს და სისტემაზე არასანქცირებული წვდომის შემთხვევებზე სათანადო რეაგირება მოახდინოს.[35]

ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განიხილა საქმე, რომელიც შეეხებოდა სამუშაო ადგილზე დამონტაჟებული ე. წ. “CCTV” ვიდეოკამერების მეშვეობით დასაქმებულების სამუშაო სივრცის ვიდეომონიტორინგს. საქმის გარემოებების მიხედვით, კომპანიის თანამშრომელმა ვიდეოჩანაწერი მონაცემთა სუბიექტს სხვადასხვა საკომუნიკაციო პლატფორმის მეშვეობით გაუზიარა, თუმცა კომპანიის

[33] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 4, პუნქტი 1, ქვეპუნქტი „ვ“.

[34] *CNIL,* Employee monitoring: CNIL Fined AMAZON FRANCE LOGISTIQUE €32 Million, <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> [10.12.2024].

[35] იხ. <https://pdps.ge/ka/content/978/5263/ra-unda-vicodeT-videomonitoringis-Sesaxeb> [11.12.2024].

შინაგანაწესის თანახმად, თანამშრომლებს ვიდეოჩანაწერებზე წვდომისა და მისი გაზიარების უფლება არ ჰქონდათ. საზედამხედველო ორგანომ განმარტა, რომ კომპანიას მონაცემთა უსაფრთხოებისთვის შემუშავებული ჰქონდა ტექნიკური და ორგანიზაციული ზომები. ამდენად, კომპანია, როგორც დამუშავებისთვის პასუხისმგებელი პირი, ვერ იქნებოდა პასუხისმგებელი იმ თანამშრომლის ქმედებაზე, რომელმაც განზრახ არ დაიცვა კომპანიის მიერ დადგენილი მონაცემთა უსაფრთხოების წესები.[36]

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის 27-ე მუხლი კონკრეტულად არეგულირებს მონაცემთა უსაფრთხოების საკითხებს. კერძოდ, ამავე მუხლის პირველი და მე-2 პუნქტების თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა ამ კანონის შესაბამისად დამუშავების უზრუნველსაყოფად და შეძლოს მონაცემთა დამუშავების ამ კანონთან შესაბამისობის დადასტურება. ამასთან, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან მიიღონ მონაცემთა დამუშავების შესაძლო და თანამდევი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას მონაცემთა დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან. მონაცემთა უსაფრთხოების დაცვის მნიშვნელობას ცხადყოფს პერსონალურ მონაცემთა დაცვის სამსახურის მიერ დადგენილი ერთგვაროვანი პრაქტიკაც, რომლის შესაბამისად, მონაცემთა უსაფრთხოების დაცვასთან დაკავშირებული მოთხოვნების შეუსრულებლობის დადასტურებისთვის არ არის აუცილებელი მონაცემთა უკანონო გამჟღავნების ფაქტის არსებობა, არამედ ისიც საკმარისია, რომ „მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა არ გაითვალისწინოს მონაცემთა დამუშავებასთან დაკავშირებული რისკები და თავისი ქმედებით ან უმოქმედობით შექმნას მონაცემთა უკანონო დამუშავების საფრთხე“[37].

საბოლოოდ, კანონით დადგენილ სხვა ვალდებულებებთან ერთად, მონაცემთა უსაფრთხოების დაცვა მნიშვნელოვანია იმდენად, რამდენადაც მის გარეშე არსებობს პერსონალური მონაცემების უკანონო წვდომის, გამჟღავნების, გასაჯაროების, გავრცელების რისკები, რაც მხოლოდ რისკის არსებობის შემთხვევაშიც კი, ქმნის ადმინისტრაციული პასუხისმგებლობის დაკისრების საფუძველს.

[36] მსოფლიო პრაქტიკა, პერსონალურ მონაცემთა დაცვის სამსახური, 2024, სექტემბერი, 4.

[37] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 20 ნოემბრის №გ-1/340/2024 გადაწყვეტილება.

7. დასკვნა

მონაცემთა სუბიექტის სამსახურებრივი, პროფესიული ხასიათის საქმიანობა მისი პირადი ცხოვრების განუყოფელი, შემადგენელი ნაწილია. „სამსახურებრივი ცხოვრების პროცესში ადამიანთა უმრავლესობას აქვს გამორჩეული შესაძლებლობა, განავითაროს თავიანთი ურთიერთობა გარესამყაროსთან[38]“. შესაბამისად, პერსონალურ მონაცემთა დაცვა, როგორც პირადი ცხოვრების უფლების მნიშვნელოვანი ასპექტი, გარანტირებული უნდა იყოს დასაქმებული პირის სამუშაო ადგილზე.

წინამდებარე ნაშრომში განხილულ იქნა დასაქმებული პირის სამუშაო სივრცის/პროცესის საკანონმდებლო მოწესრიგება, განიმარტა პირადი ცხოვრების დაცულობის გონივრული მოლოდინის სტანდარტი, *Ultima Ratio*-ს პრინციპი, გამოიკვეთა დამსაქმებლის, როგორც დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის ვალდებულებები. თეორიულ საკითხებთან ერთად, შეფასდა პერსონალურ მონაცემთა დაცვის სამსახურის, ევროპის ქვეყნების საზედამხედველო ორგანოებისა და ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა და მნიშვნელოვანი განმარტებები.

კვლევის შედეგად გამოიკვეთა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი დასაქმებული პირის, როგორც მონაცემთა სუბიექტის, უფლებების დაცვის მაღალ სტანდარტებს ადგენს და სამუშაო პროცესის/სივრცის ვიდეომონიტორინგს დასაშვებს ხდის მხოლოდ განსაკუთრებულ შემთხვევებში. გარდა ამისა, დადგინდა, რომ სამუშაო ადგილზე იმგვარი სივრცის არსებობისას, სადაც პირს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს, ვიდეომონიტორინგი დაუშვებელია იმისდა მიუხედავად, თუ რა ლეგიტიმური მიზანი შეიძლება გააჩნდეს დამსაქმებელს.

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი განსაკუთრებულად იცავს დასაქმებული პირის პერსონალურ მონაცემებს და ამ პროცესში, რომელიც მხოლოდ განსაზღვრული წინაპირობების არსებობისას დაიშვება, დამსაქმებელს, როგორც დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირს აკისრებს მთელ რიგ ვალდებულებებს. ზემოაღნიშნული ვალდებულებების განუხრელი შეუსრულებლობა, ხოლო მონაცემთა უსაფრთხოების დაცვის კუთხით მხოლოდ პერსონალურ მონაცემთა უსაფრთხოების დარღვევის რისკის არსებობა, წარმოადგენს ადმინისტრაციულ სამართალდარღვევას და ქმნის ადმინისტრაციული პასუხისმგებლობის დაკისრების საფუძველს.

[38] *Case of Bărbulescu v. Romania*, [2017] ECHR App. No. 61496/08, §61.

ბიბლიოგრაფია:

1. საქართველოს ორგანული კანონი „საქართველოს შრომის კოდექსი“, 4113-რს, 17/12/2010.
2. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023.
3. „საჯარო სამსახურის შესახებ“ საქართველოს კანონი, 4346-Iს, 27/10/2015.
4. „შრომის ინსპექციის შესახებ“ საქართველოს კანონი, 7178-Iს, 29/09/2020.
5. „ზოგადი განათლების შესახებ“ საქართველოს კანონი, სსმ, 1330, 08/04/2005.
6. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №21 ბრძანება.
7. განათლებისა და მეცნიერების მინისტრის 2021 წლის 29 დეკემბრის №104/ნ ბრძანება.
8. საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის მინისტრის 2019 წლის 29 იანვრის №06/ნ ბრძანება.
9. „აზარტული და სხვა მომგებიანი თამაშობების (გარდა წამახალისებელი გათამაშებისა) ადგილებზე და გარე პერიმეტრზე ვიდეომეთვალყურეობის სისტემებისა და მათი დამონტაჟება-ექსპლუატაციის წესის დამტკიცების შესახებ“ საქართველოს შინაგან საქმეთა მინისტრის 2007 წლის 29 აგვისტოს №1143 ბრძანება.
10. „სამუშაო სივრცეში უსაფრთხოებისა და ჯანმრთელობის დაცვის მინიმალური მოთხოვნების შესახებ ტექნიკური რეგლამენტის დამტკიცების თაობაზე“ საქართველოს მთავრობის 2022 წლის 1 ივლისის №341 დადგენილება.
11. *ტაკაშვილი ს.*, პერსონალური მონაცემების დამუშავების სტანდარტი დასაქმებულის სამუშაო სივრცის ვიდეომონიტორინგისას, სამართლის მეთოდები, №8, 2024, 129.
12. რეკომენდაციები ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების თაობაზე, პერსონალურ მონაცემთა დაცვის სამსახური, 2024, 8.
13. მსოფლიო პრაქტიკა, პერსონალურ მონაცემთა დაცვის სამსახური, 2023, ოქტომბერი, 7-8.
14. მსოფლიო პრაქტიკა, პერსონალურ მონაცემთა დაცვის სამსახური, 2024, სექტემბერი, 4.
15. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 26 ნოემბრის №გ-1/346/2024 გადაწყვეტილება.
16. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 22 ნოემბრის №გ-1/342/2024 გადაწყვეტილება.
17. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 20 ნოემბრის №გ-1/340/2024 გადაწყვეტილება.

18. 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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
19. EDPB, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, 2020, §36.
20. Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work, 2017, 9.
21. Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].
22. EDPS, Video-Surveillance Guidelines, Brussels, 17 March 2010, 31-32 <https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> [16.12.2024].
23. ICO, Guideline on the Monitoring of Workers by Employers, 20-35 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf> [20.12.2024].
24. CNIL, Employee Monitoring: Fined AMAZON FRANCE LOGISTIQUE €32 Million, <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> [10.12.2024].
25. López Ribalda and others v. Spain, [2019] ECHR, №1874/13; №8567/13.
26. Antović and Mirković v. Montenegro, [2017] ECHR, №70838/13, §44, §55-§60.
27. Bărbulescu v. Romania, [2017] ECHR, №61496/08, §61.
28. Köpke v. Germany, [2010] ECHR, №420/07.
29. Von Hannover v. Germany, [2004] ECHR, №59320/00, §51.
30. Pretty v. the United Kingdom, [2002] ECHR, №2346/02, §61.

მარიამი გიორგაძე*

ხელოვნური ინტელექტის სისტემების სამართლებრივი რეგულირება და პერსონალურ მონაცემთა დაცვასთან დაკავშირებული გამოწვევები

სტატიის მიზანია ხელოვნური ინტელექტის სამართლებრივ რეგულირებასთან დაკავშირებული მდგომარეობის, ასევე მისი მუშაობის/განვითარების პროცესში ადამიანის უფლებების, კერძოდ პირადი ცხოვრების ხელშეუხებლობის, პერსონალურ მონაცემთა დაცვის აქტუალური საკითხების ანალიზი. წინამდებარე სტატიის ფარგლებში განხილულია ხელოვნური ინტელექტის მიერ და მისი მეშვეობით პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული გამოწვევები და არსებული საერთაშორისო პრაქტიკა.

საკვანძო სიტყვები: *ხელოვნური ინტელექტი, ადამიანის ძირითადი უფლებები, პერსონალური მონაცემები, სამართლებრივი რეგულირება, მონაცემთა დაცვა.*

1. შესავალი

ტექნოლოგიების განვითარებას უდიდესი როლი გააჩნია კაცობრიობის ისტორიისა და ადამიანების ყოველდღიურობის შეცვლაში. აღნიშნულის თვალსაჩინო მაგალითია, ინდუსტრიული რევოლუციები, რასაც მე-18 საუკუნის ბოლოდან მოყოლებული არაერთი სოციალური და ეკონომიკური გარდატეხა მოჰყვა.[1] იგი სხვადასხვა ტექნოლოგიური პროცესების უწყვეტ ჯაჭვს წარმოადგენს და დღეს, მე-4 ინდუსტრიული რევოლუციის ეტაპზე, ხელოვნურ ინტელექტს ("AI"), როგორც მის ერთ-ერთ გამოვლინებას მეცნიერების სხვადასხვა დარგსა და ადამიანის ყოველდღიურობაში სისტემური ცვლილებების პოტენციალი აქვს.[2]

ხელოვნური ინტელექტის, როგორც ადამიანის მსგავსად მოაზროვნე მანქანის, შექმნის იდეას დასაბამი მე-20 საუკუნის მე-2 ნახევარში დაედო. 1950 წელს, ინგლისელმა მეცნიერმა, ალან ტურინგმა, თავის სტატიაში ადამიანის

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის აპარატის სპეციალისტი.

[1] *Stearns P. N.,* The Industrial Revolution in World History, 4th ed., Westview Press, 2013, 9-14.

[2] *Schwab K.,* The Fourth Industrial Revolution, *Encyclopedia Britannica,* 2023, <https://www.britannica.com> [10.01.2025].

დონეზე „მოაზროვნე“ მანქანის, სწავლების ალგორითმის მეშვეობით, შექმნის იდეა განავითარა და ჩამოაყალიბა „ტურინგის ტესტი“[3], რომელიც ადამიანის იდენტურად მოაზროვნე მანქანის შექმნის იდეას ეფუძნება[4]. ხელოვნური ინტელექტის განვითარებამ მას შემდეგ ბევრი ეტაპი (მათ შორის დაინტერესების კლების) განვლო, იმისათვის რომ დღევანდელ, პროგრესული შესაძლებლობების მქონე “AI”-იმდე მიეღწია.[5] ერთ-ერთ სამეცნიერო ლიტერატურაში განვითარებულია საინტერესო ჰიპოთეზა რომლის თანახმადაც თანამედროვე ხელოვნური ინტელექტის საწყისი სხვადასხვა, სრულიად განსხვავებული დარგებიდან მოდის, კერძოდ: *ფილოსოფოსების* მიერ ადამიანის გონების და მისთვის მიწოდებული ინფორმაციის ურთიერთქმედებასთან დაკავშირებული მოსაზრებებმა, *ეკონომისტების მიერ* გადაწყვეტილების მაქსიმალური სარგებლით მიღების პროცესის ფორმალიზებამ, *ნეირომეცნიერების* მიერ თავის ტვინის ფუნქციონირებისა და აგებულების გამოკვლევამ, მათემატიკოსებისა და კომპიუტერული ინჟინრების მიერ ხელსაწყოებსა და მოწყობილობებზე მუშაობამ ხელოვნური ინტელექტის არსებული მოდელების შექმნა გახადა შესაძლებელი.[6]

დღესდღეობით, ხელოვნურმა ინტელექტმა და მასზე დაფუძნებულმა ტექნოლოგიებმა მთლიანად მოიცვა საზოგადოების ცხოვრების სხვადასხვა სფერო, მეცნიერების სხვადასხვა დარგი - ის რაც თავის დროზე „მომავლის პროდუქტს“ წარმოადგენდა ახლა უკვე რეალობის ნაწილია. “AI” გამოიყენება როგორც სოციალურ მედიაში, ფინანსურ, განათლების, ისე სამედიცინო სექტორში.[7] მის მსოფლიო მასშტაბით პოპულარიზაციას ხელი განსაკუთრებით შეუწყო გენერაციული ხელოვნური ინტელექტის მოდელის, “ChatGPT”-ის ბაზარზე გამოჩენამ.[8]

ხელოვნური ინტელექტის სისტემების განვითარებას განსაკუთრებული როლი შეიძლება ჰქონდეს საზოგადოების ცხოვრების გაუმჯობესებაში, გამარტივებაში, მეცნიერების განვითარებაში, ამასთან მნიშვნელოვანია იმის გააზრება რომ, იგი არ არის სრულყოფილი, ხოლო ავტომატიზებული გადაწყვეტილებების მიღების პირობებში განსაკუთრებით იმატებს ადამიანის უფლებებისადმი საფრთხეები. ხელოვნური ინტელექტის მოდელები დიდი რაოდენობით ინფორმაციის დამუშავების საფუძველზე შემუშავდება,

[3] *Russell S. J., Norvig P.,* Artificial Intelligence: a Modern Approach, 4th ed., 2021, 35-36.

[4] გამომცდელმა, რომელიც წერილობით კომუნიკაციას ახორციელებს მანქანასთან და რეალურ ადამიანთან, უნდა დააიდენტიფიციროს ვინ არის კომუნიკაციის მეორე მხარეს - ადამიანი თუ მის მსგავსად მოაზროვნე მანქანა. დამატებით იხ. Geeks for Geeks, Turing Test in Artificial Intelligence, <https://www.geeksforgeeks.org/turing-test-artificial-intelligence/> [16.09.2024].

[5] *Kingsley O. A.,* Artificial Intelligence Research: a Review on Dominant Themes, Methods, Frameworks and Future Research Directions, Telematics and Informatics Reports, Volume 14, 2024.

[6] *Russell S. J., Norvig P.,* Artificial Intelligence: a Modern Approach, 4th ed., 2021, 35-36.

[7] *Gleeson B.,* How AI Is Reshaping The Future Of Work Across Industries, <https://www.forbes.com/sites/brentgleeson/2024/12/03/how-ai-is-reshaping-the-future-of-work-across-industries/> [03.12.2024].

[8] ChatGPT “OpenAI”-ის პროდუქტია, რომელმაც 2020-22 წლებიდან ხელოვნური ინტელექტის პროდუქტებისადმი განსაკუთრებული ყურადღება გამოიწვია მთელი მსოფლიო მასშტაბით. იგი არის ე.წ. „ჩატბოტი“ რომელსაც ადამიანის მსგავსი კომუნიკაციისა და ინფორმაციის გენერირების შესაძლებლობა აქვს.

ვითარდება, და მის მიერ გადაწყვეტილებების მიღება/პროგნოზირებაც სწორედ იმ ინფორმაციის დამუშავებას ეფუძნება, რომელთა ნაწილიც პერსონალურ მონაცემებს წარმოადგენს. შესაბამისად, მაშინ, როდესაც ხელოვნური ინტელექტი მსოფლიოს ტექნოლოგიური მომავლის ცენტრად იქცა, მხედველობიდან არ უნდა გამოგვრჩეს იმ პირთა უფლებების, განსაკუთრებით კი პირადი ცხოვრების ხელშეუხებლობის, პერსონალურ მონაცემთა დაცვის მნიშვნელობა, რომლებიც ამ საზოგადოების ნაწილნი არიან.

არამხოლოდ ხელოვნური ინტელექტის, არამედ ზოგადად ციფრული ტექნოლოგიების აქტუალობას თან ახლავს მნიშვნელოვანი გამოწვევები ადამიანის ფუნდამენტურ უფლებებთან მიმართებით, აღნიშნულთან დაკავშირებით კი განსაკუთრებით მნიშვნელოვანი შეიძლება იყოს საზედამხედველო ორგანოთა მიერ მათი კომპეტენციის ფარგლებში განხორციელებული ღონისძიებები. ამ მხრივ, ხაზგასასმელია რომ, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) გეგმის[9] ერთ-ერთ ძირითად მიმართულებას სწორედ თანამედროვე ტექნოლოგიების სფერო წარმოადგენს (მოიცავს როგორც კერძო, ისე საჯარო დაწესებულებებს)[10], რასაც განსაკუთრებული მნიშვნელობა და გავლენა შეიძლება ჰქონდეს ფიზიკურ პირთა მონაცემების დამუშავების ეროვნული სტანდარტების დამკვიდრებაზე და პრაქტიკის განვითარებაზე, თანამედროვე ტექნოლოგიების ეპოქაში პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვაზე.

დამატებით, აღსანიშნავია რომ მონაცემთა დაცვის ევროპულმა საბჭომ, 2025 წლის 11 თებერვალს, 102-ე პლენარულ სხდომაზე, ხელოვნური ინტელექტის შემსწავლელი მიზნობრივი ჯგუფის შექმნის გადაწყვეტილება მიიღო[11], რაც AI-ი სისტემების მიერ მონაცემთა დამუშავებისადმი მზარდ ინტერესზე მიანიშნებს.

წინამდებარე ნაშრომის ფარგლებში გაანალიზებულია ხელოვნურ ინტელექტის ცნება, მასთან დაკავშირებული სამართლებრივი რეგულირებების *status quo,* აღნიშნული ტექნოლოგიების პროგრესის პროცესში არსებული თუ მოსალოდნელი გამოწვევები, განსაკუთრებით კი პერსონალურ მონაცემთა დაცვის კონტექსტში, და ის საკითხები რაც ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავების დროს უნდა იქნეს გათვალისწინებული.

[9] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 31 დეკემბრის №ბ/1259 ბრძანება „პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) 2025 წლის გეგმის დამტკიცების შესახებ“.

[10] იქვე, დანართი №1 და №2.

[11] European Data Protection Board (EDPB), EDPB Adopts Statement on Age Assurance, Creates a Task Force on AI Enforcement and Gives Recommendations to WADA, <https://www.edpb.europa.eu/our-work-tools/plenary-meetings/102nd-plenary-meeting_en> [12.02.2025].

2. ხელოვნური ინტელექტის ცნება და სამართლებრივი რეგულირება

2.1. ხელოვნური ინტელექტის ცნება: სისტემები და მოდელები

ტერმინის „ხელოვნური ინტელექტი“ და მისი როგორც მეცნიერების ცალკეული დარგის წარმოშობა დარტმუთის კოლეჯის 1956 წლის კონფერენციას უკავშირდება. მეცნიერთა ჯგუფმა[12] მიზნად დაისახა გამოეკვლია გზა თუ როგორ შეიძლებოდა „მანქანებს ენა, კონცეფციებისა და აბსტრაქციების ფორმები გამოეყენებინა და გადაეწყვიტა სხვადასხვა პრობლემური საკითხები, რაც იმ ეტაპზე მხოლოდ ადამიანისთვის იყო დამახასიათებელი“.[13]

ხელოვნური ინტელექტის (“AI”) სისტემის თანამედროვე განმარტების თანახმად, იგი არის *„მანქანურ ტექნოლოგიებზე დაფუძნებული სისტემა რომელიც აშკარა ან ნაგულისხმევი მიზნებისთვის, მისთვის მიწოდებული ინფორმაციიდან გამომდინარე აანალიზებს როგორ მოახდინოს შედეგების, კერძოდ პროგნოზირების, შინაარსის (ე.წ. „კონტენტის“), რეკომენდაციის ან გადაწყვეტილებების გენერირება, რომლებსაც შესაძლოა გავლენა ჰქონდეთ ფიზიკურ ან ვირტუალურ გარემოზე“.*[14] ამასთან, სხვადასხვა ხელოვნური ინტელექტის სისტემები ექსპლუატაციის შემდეგ განსხვავებული ავტონომიურობისა და ადაპტაციის დონით ხასიათდება.[15] ხელოვნური ინტელექტის სისტემის:

- *ავტონომიურობა* - გულისხმობს მისთვის ავტონომიურობის მინიჭებისა და პროცესების ავტომატიზაციის შემდგომ, მის მიერ დამოუკიდებლად, ადამიანის ჩართულობის გარეშე სწავლების/მოქმედების ხარისხს;
- *ადაპტაცია* - მოიაზრებს თავდაპირველი შემუშავების შემდეგ სისტემის განგრძობად განვითარების უნარს, რაც, როგორც წესი, მანქანურ სწავლებაზე დაფუძნებულ ხელოვნური ინტელექტის სისტემებს ახასიათებს. ის მისთვის მიწოდებულ ინფორმაციასთან ურთიერთქმედებით იცვლის ქცევას, *მაგალითად,* ხმის ამომცნობი სისტემა რომელიც ინდივიდის ხმას ერგება.[16]

---

[12] *ჯონ მაკკარტი* (მათემატიკის ასისტენტ-პროფესორი, დარტმუთის კოლეჯი), *მარვინ მინსკი* (მათემატიკისა და ნევროლოგიის უმცროსი თანამშრომელი, ჰარვარდის უნივერსიტეტი), *ნატანიელ როჩესტერი* (ინფორმაციული კვლევის მენეჯერი, IBM Corporation), *კლოდ შენონი* (მათემატიკოსი, Bell Telephone Laboratories). იხ. History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence, <https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/> [30.09.2021].

[13] *McCarth J., Minsky M.L., Rochester N., Shannon C. E.,* A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, 2, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Article 3(1).

[15] *Organisation for Economic Co-operation and Development* (*OECD),* Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers, №8, OECD Publishing, Paris, 2024.

[16] იქვე, 6.

მანქანური სწავლება (“Machine Learning”) ხელოვნური ინტელექტის ერთ-ერთი მოდელია, რომელიც მონაცემებისა და ალგორითმების მეშვეობით ადამიანის სწავლების იმიტირებას ახდენს რათა ახალ, მსგავს, მონაცემებზე დაყრდნობით, თითოეული დავალებისთვის პირდაპირი პროგრამირების გარეშე, ხელოვნურმა ინტელექტმა პროგნოზირება და გადაწყვეტილების მიღება შეძლოს.[17] დღესდღეობით სხვადასხვა სახის მანქანური სწავლების მეთოდები თუ ალგორითმები გამოიყენება, *როგორიცაა წრფივი რეგრესია (“linear regression”), ლოგისტიკური რეგრესია (“logistic regression”), ხისებრი დიაგრამა (“decision tree”)* და სხვა. თითოეული მათგანი სხვადასხვა მონაცემებსა და პრობლემებზე არის მორგებული. აქედან ყველაზე მეტად გავრცელებული ხელოვნური ნეირონული ქსელია, რომელიც ადამიანის თავის ტვინის სტრუქტურასა და ფუნქციებთანაა მიმსგავსებული და შეუძლია დაამუშაოს, გაანალიზოს კომპლექსური მონაცემები.[18]

ღრმა სწავლება (“Deep Learning”) მანქანური სწავლების ქვეჯგუფია, რომელიც იყენებს ნეირონული ქსელების მრავალ შრეს (ღრმა ნეირონულ ქსელს) და ადამიანის ტვინთან მიმსგავსებული გადაწყვეტილების მიღების უნარი გააჩნია.[19] ხელოვნური ინტელექტის სხვადასხვა *სპეციალიზებული მოდელების* გამოყენებით (რომლებიც ეფუძნება ისეთ ფუნდამენტურ მოდელებს როგორიცაა, *დიდი ენობრივი მოდელები (“Large Language Models – LLM”)* გენერირებად ხელოვნურ ინტელექტს შეუძლია სხვადასხვა სახის გადაწყვეტილებები მიიღოს, შეასრულოს განსხვავებული ტიპის დავალებები, როგორიცაა ტექსტის, გამოსახულების ან აუდიოს გენერირება.[20] “ChatGPT“, “Gemini”, “Siri”, “DALL·E 3” და სხვა ცნობილი აპლიკაციები/ვებ-გვერდები, სწორედ ხელოვნური ინტელექტის აღნიშნულ სისტემას წარმოადგენენ.

ხაზგასასმელია რომ ხელოვნური ინტელექტის მოდელები, რომლებიც სისტემის აუცილებელი კომპონენტია, თავისთავად ხელოვნური ინტელექტის სისტემას არ წარმოადგენს. მოდელები საჭიროებენ დამატებით კომპონენტებს, როგორიცაა „მომხმარებლის ინტერფეისი“, ინტეგრირებულნი არიან ხელოვნური ინტელექტის სისტემაში და მის ნაწილს წარმოადგენენ.[21] ხელოვნური ინტელექტის მეტად განვითარებული, კომპლექსური მოდელების განვითარებისთვის განსაკუთრებით დიდი როლი აქვს სწავლების პროცესში გამოყენებული მონაცემების რაოდენობას, მრავალფეროვნებას, ხარისხს, რაც შემდგომში ხელოვნური ინტელექტის მუშაობაზე და მასთან დაკავშირებულ სხვადასხვა სახის გამოწვევებზე აისახება.

---

[17] *Keskpaik S.,* Machine Unlearning, TechSonar Reports, 2024, 19, <https://www.edps.europa.eu/system/files/2024-11/24-11-15_techsonar_2025_en.pdf>.

[18] IBM, What is Artificial Intelligence (AI), <https://www.ibm.com/think/topics/artificial-intelligence?> [09.08.2024].

[19] იქვე.

[2020] *European Data Protection Supervisor (EDPS),* Orientations for EUIs Using Generative AI, 2024, <https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf>.

[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Recital 97.

ხელოვნური ინტელექტი, გარდა იმ ბევრი დადებითი საკითხებისა, რომლებზეც აქამდე ყურადღება იქნა გამახვილებული, განსხვავებული სახის რისკებს შეიცავს. *მაგალითად,* ეს შეიძლება იყოს დეზინფორმაციის გავრცელების ხელის შეწყობა *(იმგვარი სიმულაციური „კონტენტის" შექმნა რაც ადამიანებისთვის აღქმადი იქნება როგორც რეალობა)*, ხელოვნური ინტელექტის მოდელების „ჰალუცინაციები" *(დამაჯერებელი ფორმით არასწორი ინფორმაციის გადმოცემა),* მიკერძოებული/დისკრიმინაციული გადაწყვეტილებები/პროგნოზები, მონაცემთა დაცვასთან დაკავშირებული რისკები *(როგორც სწავლების, მოდელის დონეზე, ისე ადამიანთან ურთიერთქმედებისას),* მის გამჭვირვალობასა და განმარტებასთან დაკავშირებული გამოწვევები *(ე.წ. „შავი ყუთის" მოდელები)*, მოდელების მიერ მიღებული შედეგების გასაჩივრების შეუძლებლობა, კონფიდენციალურობის დარღვევა *(მონაცემთა დაცვასთან დაკავშირებული ინციდენტების შემთხვევებში).*[22]

2.2. ხელოვნური ინტელექტის სამართლებრივი რეგულირება

ხელოვნური ინტელექტის შემუშავებასთან და ეთიკურ გამოყენებასთან დაკავშირებით არსებულმა გამოწვევებმა თანამედროვე მსოფლიოს ქვეყნების ნაწილი მისი სამართლებრივი რეგულირების საჭიროებაში დაარწმუნა.

2024 წლის 1 აგვისტოს ევროპის კავშირის „ხელოვნური ინტელექტის აქტი" შევიდა ძალაში. იგი აღნიშნული სისტემების პირველ სამართლებრივ მარეგულირებელ ჩარჩოს წარმოადგენს და ხელოვნური ინტელექტის განვითარების პროცესში უსაფრთხოების, ფუნდამენტური უფლებებისა და ეთიკის პრინციპების დაცვას ისახავს მიზნად.[23] დოკუმენტი აწესრიგებს ისეთ საკითხებს, როგორიცაა მაღალი რისკის შემცველი, ასევე ზოგადი დანიშნულების ხელოვნური ინტელექტი და მათი რეგულირება. ამასთან, იგი განსაზღვრავს ხელოვნური ინტელექტის გამოყენების აკრძალულ შემთხვევებს და სხვადასხვა დონეზე AI-ისთან დაკავშირებული ორგანოების შექმნას ითვალისწინებს. აქტი ეტაპობრივად ამოქმედდება, ხოლო მისი საბოლოო იმპლემენტაციის პროცესი 2030 წლამდეა განსაზღვრული.[24]

2024 წლის 5 სექტემბერს ხელმოსაწერად გაიხსნა ევროპის საბჭოს ჩარჩო კონვენცია „ხელოვნურ ინტელექტის და ადამიანის უფლებების, დემოკრატიასა და კანონის უზენაესობის შესახებ",[25] *რომლის ხელშემკვრელი*

[22] *OECD*, AI, Data Governance and Privacy: Synergies and Areas of International Cooperation, OECD Artificial Intelligence Papers, №22, OECD Publishing, Paris, 2024.

[23] *EDPS,* Artificial Intelligence Act, <https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en> [10.01.2025].

[24] <https://artificialintelligenceact.eu/implementation-timeline/> [01.06.2024].

[25] Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 05.09.2024.

მხარეც არის საქართველო.[26] აღნიშნული პირველი საერთაშორისო, სავალდებულო ძალის მქონე სამართლებრივი დოკუმენტია, რომელიც ხელოვნური ინტელექტის გამოყენებასა და ადამიანის უფლებებს შორის ბალანსს უზრუნველყოფს, ითვალისწინებს ხელოვნური ინტელექტის სისტემების მიერ მათი სასიცოცხლო ციკლის ფარგლებში უზრუნველსაყოფ პრინციპებს. ამასთან, ევროპის საბჭოს ხელოვნური ინტელექტის კომიტეტმა (CAI) 2024 წლის 28 ნოემბერს დაამტკიცა ინსტრუმენტი "HUDERIA", რაც როგორც საჯარო, ისე კერძო დაწესებულებებს ადამიანის უფლებების, დემოკრატიისა და კანონის უზენაესობის დაცვის მიზნით AI სისტემებთან დაკავშირებული რისკების შეფასებაში დაეხმარება.[27]

გარდა აღნიშნული სამართლებრივი აქტებისა, ხელოვნური ინტელექტის სამართლებრივი მოწესრიგების პროცესში უმნიშვნელოვანესი როლი სხვადასხვა საერთაშორისო ორგანიზაციის მიერ შემუშავებულ მოსაზრებებს, კვლევებს, „ინსტრუმენტებს" თუ სხვადასხვა სახელმძღვანელო რეკომენდაციებს გააჩნიათ. *მაგალითად,* აღნიშნული მიმართულებით გამოირჩევა ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია ("OECD"), რომლის მიერ შემუშავებულ განმარტებასაც ეფუძნება ევროკავშირის ხელოვნური ინტელექტის აქტში წარმოდგენილი ხელოვნური ინტელექტის სისტემის ცნება. ორგანიზაცია აწარმოებს ყოვლისმომცველ კვლევებს და ანალიტიკას, ხელოვნური ინტელექტის ტრანსფორმაციული ბუნებისა და სოციუმზე თუ ეკონომიკაზე მისი გავლენის სიღრმისეული შესწავლისთვის.[28]

გაერთიანებული ერების განათლების, მეცნიერებისა და კულტურის ორგანიზაცია ("UNESCO") ხელოვნური ინტელექტის საზოგადოებაზე „უსაზღვრო გავლენების და თანმდევი შედეგების გათვალისწინებით" მუშაობს ისეთ საკითხებზე როგორიცაა: *ხელოვნური ინტელექტის ეთიკა, სისტემების გამოყენება განათლების სფეროში, ხელოვნური ინტელექტი და გენდერული თანასწორობა და სხვა.*[29]

გაერთიანებული ერების ორგანიზაცია ("UN"), ასევე, აქტიურად აგრძელებს ხელოვნური ინტელექტის მიმართულებით მუშაობას, შეიქმნა *ხელოვნური ინტელექტის საკონსულტაციო ორგანო,*[30] ხოლო 2024 წლის მარტში შემუშავდა რეზოლუცია, რომელიც სახელმწიფოებს და სხვა დაინტერესებულ პირებს ადამიანის უფლებებისა და თავისუფლებების

[26] *Council of Europe (CoE),* The Council of Europe Framework Convention on Artificial Intelligence, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> [10.01.2025].

[27] *Council of Europe (CoE) Committee on Artificial Intelligence (CAI),* Methodology for the Risk and Impact Assessment of AI Systems from the Point of View of Human Rights, Democracy and the Rule of Law ("The HUDERIA"), 28.11.2024, <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f> [10.01.2025].

[28] *OECD*, OECD Artificial Intelligence Papers, <https://doi.org/10.1787/dee339a8-en> [10.01.2025].

[29] *United Nations Educational, Scientific and Cultural Organization (UNESCO),* Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence> [10.01.2025].

[30] High-Level Advisory Body on Artificial Intelligence, <https://www.un.org/digital-emerging-technologies/ai-advisory-body> [10.01.2025].

გარანტირებით, ხელოვნური ინტელექტის სისტემების ეთიკურად შემუშავების, განვითარების და ექსპლუატაციისკენ მოუწოდებს,.[31]

საქართველოში, აღნიშნულ ეტაპზე, კანონმდებლობაში გვხვდება მხოლოდ საქართველოს ეროვნული ბანკის პრეზიდენტის 2020 წლის ბრძანება „მონაცემებზე დაფუძნებული სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების მოდელების რისკების მართვის დებულების დამტკიცების თაობაზე“, რომელიც მონაცემებზე დაფუძნებული სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების მოდელების რისკების მართვის ჩარჩოს ჩამოყალიბებისა და მასთან დაკავშირებული რისკების ეფექტურად მართვის ხელშეწყობას ისახავს მიზნად და განსაზღვრავს მოდელების აგების, გამოყენების პროცესს, მის ძირითად კომპონენტებს საქართველოს ეროვნული ბანკის ზედამხედველობისადმი დაქვემდებარებული ზოგიერთი სუბიექტებისადმი.[32]

ასევე საყურადღებოა საქართველოს 2025 წლის სახელმწიფო ბიუჯეტის შესახებ კანონი, სადაც ხელოვნურ ინტელექტთან დაკავშირებით აღნიშნულია, რომ იგეგმება:

- ხელოვნური ინტელექტის სისტემების განვითარების მხარდაჭერა, რაც სარგებლისა და პროდუქტიულობის მომტანი იქნება საქართველოს მოქალაქეებისა და ეკონომიკის სხვადასხვა სექტორისთვის;
- ხელოვნური ინტელექტის საერთაშორისო კომპეტენციის ცენტრის შექმნა, რომელიც აღიჭურვება თანამედროვე ტექნოლოგიებითა და საერთაშორისო მასშტაბის ექსპერტიზით;
- ხელოვნური ინტელექტის სისტემების დანერგვა და გამოყენება საქართველოს იუსტიციის სამინისტროს ანალიტიკური და სამართალშემოქმედებითი საქმიანობის, სახელმწიფოს მიერ დასადები ხელშეკრულებების სამართლებრივი ექსპერტიზის, საერთაშორისო სასამართლოებსა და არბიტრაჟებში საქმისწარმოების წარმართვის ეფექტიანობის გაუმჯობესებისთვის, აგრეთვე საქართველოს საკანონმდებლო მაცნის მომხმარებელთათვის გამარტივებული სერვისების მიწოდების მიზნით;
- ხელოვნურ ინტელექტთან დაკავშირებული მსოფლიო ტენდენციების შესწავლის, ანალიზის, საქართველოს კანონმდებლობის ციფრულ სტანდარტებთან ადაპტირებისთვის საჭირო დასკვნებისა და რეკომენდაციების მომზადებისა და საზოგადოების ცნობიერების ამაღლების მიზნით, საქართველოს იუსტიციის სამინისტროს

[31] *United Nations (UN),* Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 11.03.2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf> [10.01.2025].

[32] საქართველოს ეროვნული ბანკის პრეზიდენტის 2020 წლის 17 აგვისტოს ბრძანება №151/04 „მონაცემებზე დაფუძნებული სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების მოდელების რისკების მართვის დებულების დამტკიცების თაობაზე“.

სასწავლო ცენტრის ბაზაზე ხელოვნური ინტელექტის სამართლებრივი კვლევის ცენტრის შექმნა.[33]

ზემოაღნიშნულიდან გამომდინარე შეგვიძლია დავასკვნათ რომ ხელოვნური ინტელექტი არამხოლოდ საერთაშორისო დონეზე თანამედროვე ტექნოლოგიების ყველაზე ტენდენციურ მიმართულებას წარმოადგენს, არამედ ეროვნულ დონეზეც დიდია სახელმწიფოს მზაობა ხელი შეუწყოს მის სხვადასხვა სფეროში ინტეგრირებას, რაც თავისთავად შესაძლოა მოიაზრებდეს რომ "AI"-სთან დაკავშირებული გამოწვევები არამხოლოდ აქტუალურ საკითხს წარმოადგენს, არამედ სხვადასხვა სფეროში მისი აქტიური ინტეგრაციის პირობებში, გაიზრდება მისი გავლენა ადამიანის ფუნდამენტურ უფლებებსა და თავისუფლებებზე.

3. ხელოვნური ინტელექტის მიერ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული გამოწვევები

3.1. ხელოვნური ინტელექტის მიერ/მეშვეობით მონაცემთა დამუშავება და მონაცემთა საზედამხედველო ორგანოების როლი სისტემების რეგულირებაში

როგორც ნაშრომის წინა თავებში არაერთხელ აღინიშნა, ხელოვნური ინტელექტის სისტემები, როგორც შექმნის, განვითარების ასევე სარგებლობაში მიღების პროცესში დიდი რაოდენობით მონაცემებს საჭიროებენ. აღნიშნული ხშირ შემთხვევებში შესაძლოა გულისხმობდეს სხვადასხვა პირთა პერსონალური მონაცემების[34] დამუშავებას. მონაცემთა დამუშავებაში პერსონალურ მონაცემთა დაცვის როგორც საერთაშორისო *(ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია" (GDPR)[35], ევროპის საბჭოს „კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ" (108-ე კონვენცია)),* ასევე ეროვნული კანონმდებლობის *(საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ")* მიზნებისთვის მოიაზრება ნებისმიერი ქმედება რომელიც მონაცემების მიმართ შეიძლება განხორციელდეს (შეგროვება, მოპოვება, ურთიერთდაკავშირება, დაჯგუფება და ა.შ.)[36].

ხელოვნური ინტელექტის მიერ მონაცემთა დამუშავება სხვადასხვა ეტაპზე შეიძლება გამოვლინდეს - მისი პროექტირების, ბაზარზე განთავსების, ფუნქციონირებისა და განვითარების პროცესებში.

[33] საქართველოს კანონი „საქართველოს 2025 წლის სახელმწიფო ბიუჯეტის შესახებ", 45-Iმს-XIმპ, 10.12.2024, მუხლი 15, §3 და §6.

[34] პერსონალური მონაცემია „ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება". იხ. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", 3144-XIმს-Xმპ, 14.06.2023, მუხლი 3, „ა" ქვეპუნქტი.

[35] 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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.

[36] იქვე, მუხლი 3, „ვ" ქვეპუნქტი.

მაგალითად, ხელოვნური ინტელექტის სისტემა შესაძლოა ავტომატიზებული სისტემის პროექტირებისა და განვითარების პროცესებისთვის გამოიყენებოდეს. იმ შემთხვევაში თუ აღნიშნული მოიაზრებს პერსონალური მონაცემების დამუშავების აუცილებლობას (მაგალითად, როგორიცაა მანქანური სწავლება), იგი პერსონალურ მონაცემთა დაცვის სამართლებრივი რეგულირების ქვეშ მოექცევა. გარდა ამისა, ხელოვნური ინტელექტის სისტემა შესაძლოა თავისთავად შეიცავდეს იდენტიფიცირებული ან იდენტიფიცირებადი პირის შესახებ მონაცემებს და ამგვარი სისტემების დისტრიბუცია მონაცემთა დამუშავებას წარმოადგენს, თუ პერსონალური მონაცემები სისტემით სარგებლობისას შესაძლებელია მესამე პირებზე გამჟღავნდეს. გარდა ამისა, ხელოვნური ინტელექტის სისტემა შესაძლოა პერსონალური მონაცემების ავტომატიზებული დამუშავებისთვის, ფიზიკურ პირებთან დაკავშირებით გადაწყვეტილებების მიღებისთვის ან პროფაილინგისთვის გამოიყენებოდეს. *მაგალითად,* ვაკანსიაზე წარმოდგენილი რეზიუმეების ფილტრაციისთვის, რაც გულისხმობს პერსონალური მონაცემების დამუშავებას ავტომატიზებული ფორმით, რამაც შესაძლოა სამართლებრივი ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგი წარმოშვას. [37]

ხელოვნური ინტელექტის სისტემების გამოყენებას განსაკუთრებით დიდი მნიშვნელობა შეიძლება ჰქონდეს მედიცინის დარგშიც, იმ მიზნით რომ დროის მცირე პერიოდში ზუსტი დიაგნოზის მიღება გახდეს შესაძლებელი. *აღნიშნულ შემთხვევაში* პერსონალური მონაცემები შესაძლოა სხვადასხვა მოწყობილობების, სენსორების, კლინიკური აღჭურვილობის მეშვეობით თუ სამედიცინო შემოწმებების ფარგლებში შეგროვდეს. პაციენტების მონაცემები ხელოვნური ინტელექტის სისტემების მეშვეობით შესაძლოა დამუშავდეს სისტემების სწავლების, შემოწმების, ფუნქციონირების განგრძობადი შეფასების პროცესში. აღნიშნულ შემთხვევაში როგორც წესი განსაკუთრებული კატეგორიის მონაცემების დამუშავების საჭიროება დგება, რაც ადამიანის უფლებებისა და თავისუფლებების მიმართ მეტი სენსიტიურობით ხასიათდება და შესაბამისად სპეციფიკურ რეგულაციებს ექვემდებარება, საჭიროებს დეპერსონალიზებას/ფსევდონიმიზირებას, კონკრეტული პაციენტის იდენტიფიცირების თავიდან არიდებისათვის.[38]

ყოველივე ზემოაღნიშნულიდან გამომდინარე აქტუალური გახდა მონაცემთა დაცვის საზედამხედველო ორგანოების ჩართულობა აღნიშნული სისტემების რეგულირების პროცესში და დღეს საზედამხედველო ორგანოების, მონაცემთა დაცვის საერთაშორისო ორგანიზაციების დიდი ნაწილის კვლევისა თუ მუშაობის მიმართულებას სწორედ ხელოვნური

[37] *Agencia Española de Protección de Datos (AEPD),* Legal Report 0059/2023 of the Legal Office of the AEPD Ruling on the Difference Between AI Systems and Processing of Personal Data and the Assessment of the Level of Risk of Processings, 2023, <https://www.aepd.es/documento/informe-juridico-0059-2023-en.pdf> [10.01.2025].

[38] *Council Of Europe (CoE) Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO),* Report on the Application of Artificial Intelligence in Healthcare and Its Impact on the "Patient–Doctor" Relationship, 2024, 7-8.

ინტელექტი წარმოადგენს. მაგალითად, *დიდი ბრიტანეთის მონაცემთა დაცვის საზედამხედველო ორგანოს (Information Commissioner's office – "ICO")* ხელოვნური ინტელექტი, ინდივიდებზე და მათ უფლებებზე მაღალი რისკის პოტენციალიდან გამომდინარე, პრიორიტეტულ მიმართულებად აქვს განსაზღვრული.[39] აღნიშნული ასევე მნიშვნელოვან მიმართულებას წარმოადგენს *ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანოსთვის (Agencia Española de Protección de Datos – "AEPD"),* რომელსაც შემუშავებული აქვს სხვადასხვა სახის სარეკომენდაციო დოკუმენტები ხელოვნური ინტელექტის განსხვავებულ კონტექსტებში *(მაგალითად, ბიომეტრიული მონაცემების დამუშავებისას)* გამოყენების თაობაზე.[40] გარდა აღნიშნულისა, ზოგიერთ შემთხვევაში საზედამხედველო ორგანოებს შეფასებული აქვთ ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავების შემთხვევებიც, რაც შემდგომ თავებში იქნება განხილული.

„პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეის" ("GPA") 2023 წლის გენერაციული ხელოვნური ინტელექტის სისტემების შესახებ რეზოლუციაში მითითებულია რომ სისტემების შემუშავებისა და ფუნქციონირების პროცესის ფუნდამენტური ელემენტებს მონაცემთა დაცვა და დამუშავების პრინციპები ქმნის, კერძოდ: *დამუშავების კანონიერება, მიზნის კონკრეტიზაციასა და შემდგომი სარგებლობის შეზღუდვა, მონაცემთა მინიმიზაცია, სიზუსტე, გამჭვირვალობა, უსაფრთხოება, ანგარიშვალდებულება, სუბიექტის უფლებების დაცვა, მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი.*[41]

3.2. ხელოვნური ინტელექტის სისტემების მიერ მონაცემთა დამუშავებასთან დაკავშირებული ძირითადი საკითხები

როგორც ხელოვნური ინტელექტის შემუშავებისა და განვითარების პროცესში სისტემების მიერ მონაცემების დამუშავებისას *(სწავლების პროცესში სხვადასხვა პირთა ჯგუფის შესახებ ინფორმაცია, მათ შორის მოპოვებული საჯარო წყაროებიდან, გამოყენების პროცესში მომხმარებლის მიერ მითითებული მონაცემები და სხვა)*, ასევე აღნიშნული ტექნოლოგიების მეშვეობით მოსარგებლე პირების მიერ მესამე პირთა პერსონალური მონაცემების დამუშავებისას (*მაგალითად, საბანკო სექტორში რისკების იდენტიფიცირებისთვის მომხმარებლის, ასევე დასაქმების კომპანიების მიერ პოტენციური კანდიდატების შესახებ ინფორმაციის დამუშავება, სამედიცინო*

[39] Information Commissioner's Office (ICO), Our Work on Artificial Intelligence, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> [10.01.2025].

[40] Agencia Española de Proteccion de Datos (AEPD), Innovation and Technology, <https://www.aepd.es/en/areas/innovation-and-technology> [10.01.2025].

[41] *Global Privacy Assembly(GPA),* Resolution on Generative Artificial Intelligence Systems, 45th Closed Session, 2023, 5-9, <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf> [10.01.2025].

სექტორში სხვადასხვა დაავადების დროული დიაგნოსტიკისთვის, სამართალდამცავ სექტორში დამნაშავეთა დროული იდენტიფიცირებისთვის მონაცემთა დამუშავება სხვა.) აუცილებელია უზრუნველყოფილი იყოს მონაცემთა დამუშავების პრინციპები და შეფასდეს თუ რა სამართლებრივი საფუძველი გააჩნიათ ორგანიზაციებს მონაცემთა ამ გზით დამუშავებისთვის.

3.2.1. ხელოვნური ინტელექტის მოდელების განვითარებისთვის პერსონალურ მონაცემთა დამუშავება

ევროკავშირის ხელოვნური ინტელექტის აქტი ხელოვნური ინტელექტის სისტემის მთლიანი სასიცოცხლო ციკლის ფარგლებში პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის უზრუნველყოფის ვალდებულებასა და დამატებით გარანტიებს ადგენს. იგი მიუთითებს რომ პერსონალურ მონაცემთა დამუშავებისას გათვალისწინებული უნდა იყოს მონაცემთა მინიმიზაციის პრინციპი და მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას. ამასთან, მიმწოდებლების მიერ პრინციპებთან შესაბამისობის უზრუნველსაყოფად იგი მიუთითებს როგორც მონაცემთა დეპერსონალიზაციაზე, დაშიფვრაზე, ასევე იმგვარი ტექნოლოგიების გამოყენებაზე რომელიც შესაძლებელს გახდის "AI" სისტემების სწავლებას „ნედლი" მონაცემების კოპირების ან მხარეებს შორის გადაცემის გარეშე.[42]

ხელოვნური ინტელექტის მიერ მონაცემთა დამუშავება შესაძლოა სხვადასხვა სახის გამოწვევებს უკავშირდებოდეს. *მაგალითად,* სხვადასხვა სახის გენერირებადი ხელოვნური ინტელექტის „ჩატბოტებისადმი" მოთხოვნის გაზრდამ წამოჭრა სათანადო ასაკობრივი ცენზის დაწესების აუცილებლობა. არასრულწლოვანი პირების შესაძლოა უფრო ნაკლებად იყვნენ ინფორმირებული აღნიშნული სისტემებისადმი მათი პერსონალური მონაცემების მიწოდების რისკების თაობაზე, და მოკლებულნი არიან თავიანთი უფლებების ეფექტიანი დაცვის შესაძლებლობას. "UNESCO"-ს რეკომენდაციის თანახმად აღნიშნული სისტემებით სარგებლობის მინიმალური ასაკობრივი ზღვარი 13 წელი უნდა იყოს. ამასთან სახელმწიფოებმა უნდა შეაფასონ სუბიექტის მიერ ასაკის თვითნებურად მითითება რამდენად არის საკმარისი ასაკის ვერიფიკაციისთვის და უზრუნველყონ ამ მიზნებისთვის გენერირებადი ინტელექტის მიმწოდებლების ანგარიშვალდებულება, განსაზღვრონ მშობლებისა და კანონიერი წარმომადგენლების 13 წელს ქვემოთ მყოფი პირების ხელოვნურ

[42] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Recital 69.

ინტელექტთან ინტერაქციის მონიტორინგის ვალდებულებები.[43] *ერთ-ერთ საქმეში,* რომელიც ხელოვნური ინტელექტის „ჩატბოტის“ მეშვეობით მონაცემთა დამუშავებას ეხებოდა (აპლიკაციას შეეძლო მომხმარებლების ემოციური მდგომარეობის იდენტიფიცირება და გაუმჯობესება, ეხმარებოდა მათ ხასიათის ცვლილებების აღრიცხვაში, შფოთვების, სტრესის მართვაში და სხვა), მონაცემთა საზედამხედველო ორგანომ მიიჩნია რომ არასრულწლოვანი პირების მონაცემების დამუშავების საფუძველი ვერ იქნებოდა სუბიექტთან დადებული ხელშეკრულების შესრულება, ამასთან იქიდან გამომდინარე რომ აღნიშნულ აპლიკაციას არ ჰქონდა ასაკის ვერიფიკაციის ეფექტიანი მექანიზმი, ხელოვნური ინტელექტის სისტემის მეშვეობით ამგვარი დამუშავების პროცესი ყველა მომხმარებლის მიმართ შეზღუდა, სანამ დამუშავებისთვის პასუხისმგებელი პირი ხარვეზებს არ გამოასწორებდა.[44]

ხელოვნური ინტელექტის სისტემები, შესაძლოა განუსაზღვრელი რაოდენობის პერსონალურ მონაცემებს ამუშავებდეს, რაშიც იგულისხმება როგორც სწავლების პროცესში, ასევე მომხმარებლების მიერ მიწოდებული ინფორმაცია, შესაბამისად მნიშვნელოვანია უზრუნველყოფილი იყოს მონაცემთა უსაფრთხოება ყველა სათანადო ღონისძიების გამოყენებით. *მაგალითად,* 2023 წელს “ChatGPT”-ის ტექნიკური ხარვეზიდან გამომდინარე, გარკვეული დროის ფარგლებში, მომხმარებლებისთვის ხელმისაწვდომი იყო სხვა მომხმარებლების კომუნიკაცია ხელოვნურ ინტელექტთან, რა დროსაც გამჟღავნდა ისეთ მონაცემები, როგორიცაა სახელი, ელ-ფოსტის მისამართები, საკრედიტო ინფორმაცია და სხვა. აღნიშნულ შემთხვევაში საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს ინციდენტის შეუტყობინებლობისთვის დააკისრა პასუხისმგებლობა, ამასთანავე მას არ ჰქონდა შეფასებული სწავლების პროცესში მონაცემთა დამუშავების სამართლებრივი საფუძველი, რაც წინააღმდეგობაში მოდიოდა ანგარიშვალდებულების ვალდებულებასთან, ასევე კონფიდენციალურობის პოლიტიკა მხოლოდ ინგლისურენოვანი იყო და არ ყოფილა მარტივად ხელმისაწვდომი მომხმარებლებისთვის, მიუხედავად იმისა რომ ხელოვნური ინტელექტის სისტემა ამუშავებდა არარეგისტრირებული მომხმარებლების პერსონალურ მონაცემებსაც აღნიშნულის თაობაზე კომპანიას არ ჰქონდა მითითებული პოლიტიკის დოკუმენტში, შესაბამისად დარღვეული იყო გამჭვირვალობის პრინციპიც.[45] ყოველივე ზემო აღნიშნული შესაძლოა, განსაკუთრებულად იყოს მნიშვნელოვანი ხელოვნური ინტელექტის სისტემების მიერ მონაცემთა დამუშავებისას, მითუმეტეს თუ

[43] *UNESCO,* Towards a human-centred approach to the use of generative AI, 2023, 21, <https://doi.org/10.54675/EWZM9535> [10.01.2025].

[44] *Garante per la Protezione dei Dati Personali (Garante)*, [2023], no. 9852214, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214> [10.01.2025].

[45] *Garante per la Protezione dei Dati Personali (Garante)*, [2014], no. 10085455, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10085455> [10.01.2025].

გავითვალისწინებთ იმას რომ სუბიექტების მიერ მათი პერსონალური მონაცემების დამუშავების თაობაზე ინფორმირებულობის არ არსებობა/ნაკლებობა მათ ასევე უზღუდავს სუბიექტის ისეთ მნიშვნელოვან უფლებასაც როგორიცაა გასაჩივრების უფლება, ინფორმაციის გამოთხოვის უფლება და სხვა.

მონაცემები ხელოვნური ინტელექტის ნებისმიერი სისტემის ფუნდამენტს წარმოადგენს, შესაბამისად მისი ხარისხი პირდაპირ იქონიებს გავლენას ამ სისტემების მიერ მიღებულ შედეგებზე. მონაცემების არასწორად/ტენდენციურად წარმოდგენის შემთხვევამ შესაძლოა მიკერძოებული ან უსამართლო შედეგები (გადაწყვეტილებები, პროგნოზები) გამოიწვიოს. ისტორიული მონაცემები რომლებიც ამ სისტემების სწავლების პროცესში გამოიყენება შესაძლოა საუკუნოვან სოციალურ სტიგმებთან იყოს კავშირში და ასახავდეს წარსულში არსებულ დისკრიმინაციულ პრაქტიკაც.[46] გარდა ისტორიული სტიგმების არსებობისა, ფიზიკური პირებისადმი დისკრიმინაციული მიდგომები შესაძლოა უკავშირდებოდეს ხელოვნური ინტელექტის სწავლების ეტაპზე სოციუმის ჯგუფების მახასიათებლების თუ სხვა ინფორმაციის არასათანადო ასახვასაც. საერთო ჯამში კი აღნიშნული პირების მონაცემების ამგვარი ხელოვნური ინტელექტის სისტემების მეშვეობით დამუშავება შესაძლოა ღირსების შემლახავი იყოს ან სხვაგვარად იქონიოს უარყოფითი გავლენა მონაცემთა სუბიექტის უფლებებზე, რომელთა მიმართაც სისტემა გამოიყენება.

ხელოვნური ინტელექტის მოდელების კონტექსტში საინტერესოა ხელოვნური ინტელექტის მოდელების „ანონიმურობის“ *(იგულისხმება რომ ხელოვნური ინტელექტი არ ამუშავებს იმგვარ მონაცემს რომელიც იდენტიფიცირებულ/იდენტიფიცირებად პირს უკავშირდება)* და მონაცემთა კანონიერი დამუშავების *(ლეგიტიმური ინტერესის საფუძველზე)* საკითხები:

„მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) შეფასებით, *ხელოვნური ინტელექტის სისტემის „ანონიმურობა”* ყოველ კონკრეტულ შემთხვევაში ინდივიდუალურად უნდა შეფასდეს, “EDPB”-ის მოსაზრებით ხელოვნური ინტელექტის სისტემები, რომელთა სწავლება პერსონალურ მონაცემებსაც მოიცავდა ვერ იქნება ანონიმური ყოველ შემთხვევაში. მისი მითითებით იმისათვის რომ ხელოვნური ინტელექტის სისტემა დეპერსონალიზებულად შეფასდეს აუცილებელია იმ პირთა პერსონალური მონაცემების მიღება (ასევე, ალბათობა), რომელთა პერსონალური მონაცემებიც ხელოვნური ინტელექტის მოდელის შემუშავების პროცესში გამოიყენებოდა და აღნიშნული მონაცემების სისტემებისადმი შეკითხვების მეშვეობით მოპოვების (განზრახ თუ უნებლიედ) ალბათობა უნდა იყოს უმნიშვნელო, დამუშავებისთვის პასუხისმგებელი თუ სხვა პირის მიერ მისი გონივრულად მოსალოდნელობის გათვალისწინებით.

[46] *The Europol Innovation Lab,* An Observatory Report on AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, 32,
<https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf> [10.01.2025].

მოსაზრებაში მითითებულია რომ მონაცემთა დაცვის საზედამხედველო ორგანოს შეფასება მოდელის ანონიმურობის დემონსტრირებისთვის შემუშავებული დოკუმენტაციის შეფასებით უნდა შეეძლოს. [47]

რაც შეეხება ხელოვნური ინტელექტის მოდელების შემუშავების და ექსპლუატაციაში მიღებისთვის *ლეგიტიმური ინტერესის საფუძველზე* მონაცემთა დამუშავებას, "EDPB"-ი ხაზს უსვამს რომ მონაცემთა დამუშავების საფუძვლებს შორის იერარქია არ არსებობს და უშუალოდ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა მოახდინონ მათი დამუშავების პროცესებში სათანადო საფუძვლის იდენტიფიცირება. ამასთან ლეგიტიმური ინტერესის შეფასების შემთხვევაში აუცილებლად უნდა იქნეს გათვალისწინებული სამეტაპიანი ტესტი, რაც მოიცავს (1) ლეგიტიმური ინტერესის არსებობის იდენტიფიცირებას (2) დამუშავების აუცილებლობას ამ მიზნის მიღწევისთვის (3) ლეგიტიმურ ინტერესსა და მონაცემთა სუბიექტების ინტერესებს თუ ფუნდამენტურ უფლებებსა და თავისუფლებებს შორის ინტერესთა ბალანსის შეფასებას. [48]

ამასთან აღსანიშნავია რომ ლეგიტიმური ინტერესი უნდა იყოს (1*) კანონიერი* (2) *მკაფიოდ და კონკრეტულად ფორმულირებული,* (3) *რეალური (და არა აბსტრაქტული).* ხელოვნური ინტელექტის მოდელების შემთხვევაში ასეთი ლეგიტიმური ინტერესი შეიძლება იყოს მაგალითად, ინფორმაციული სისტემის საფრთხეების იდენტიფიცირების მეთოდების გაუმჯობესება. აუცილებლობის ნაწილში უნდა შეფასდეს (1) *რამდენად გამოსადეგია მონაცემთა დამუშავება ლეგიტიმური ინტერესის მიზნებისთვის* და (2) *არსებობს თუ არა უფრო ნაკლებად შემზღუდავი საშუალება ამ ინტერესის მიღწევისთვის.* ხელოვნური ინტელექტის მეთოდების შემუშავების/განვითარებისას უმნიშვნელოვანესია მონაცემთა რაოდენობის პროპორციულობის - მინიმიზაციის პრინციპის გათვალისწინებით, შეფასება. ინტერესთა ბალანსის შეფასებისას, მხედველობაში უნდა იქნეს მიღებული პერსონალურ მონაცემთა კატეგორიები, დამუშავების კონტექსტი და სავარაუდო შემდგომი გავლენები სუბიექტების უფლებებზე. ამასთან აუცილებელია მათი მონაცემების გამოყენებასთან დაკავშირებით სუბიექტების გონივრული მოლოდინების გათვალისწინებაც.[49]

"EDPB"-ის მოსაზრებაში მითითებულია სუბიექტის *უფლებებზე უარყოფითი გავლენების შემცირების მიზნით სათანადო ღონისძიებების* გატარების საჭიროებაზეც, რაც განსხვავდება მონაცემთა დაცვის ძირითადი რეგულაციით გათვალისწინებული სავალდებულო ზომებისგან და უნდა იყოს

[47] *The European Data Protection Board ("EDPB"),* Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024, §43, <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> [10.01.2025].

[48] *EDPB,* Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(F) GDPR, Version 1.0 (for public consultation), 2024, §12, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> [10.01.2025].

[49] *EDPB*, Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024.

მორგებული ხელოვნური ინტელექტის მოდელის მახასიათებლებზე, მის დანიშნულებაზე და კონკრეტული შემთხვევის გარემოებებზე.[50]

3.2.2. ხელოვნური ინტელექტის მეშვეობით პერსონალურ მონაცემთა დამუშავება

ხელოვნური ინტელექტის დანიშნულებიდან გამომდინარე, მისი დასკვნები თუ პროგნოზები შესაძლოა კონკრეტული პირების პერსონალური მონაცემების დამუშავებას საჭიროებდეს. იმ შემთხვევებში თუ თანამედროვე ტექნოლოგიების გამოყენება, პირის პერსონალურ მონაცემთა დამუშავების საფუძველზე მის თაობაზე გადაწყვეტილების, მისთვის სამართლებრივი თუ სხვაგვარი შედეგების მომტანი შეიძლება იყოს - აღნიშნულს მონაცემთა სუბიექტის ფუნდამენტურ უფლებებსა და თავისუფლებებზე პოტენციური უარყოფითი გავლენები მოჰყვება. შესაბამისად, მსგავსი თანამედროვე ტექნოლოგიებით მოსარგებლე პირებს, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს განსაზღვრული ვალდებულებები ეკისრებათ, განსაკუთრებით კი პერსონალურ მონაცემთა დაცვის მიმართულებით. ამ მხრივ მნიშვნელოვანია ისეთი საკითხების გათვალისწინება, როგორიცაა დამუშავების პროცესის გამჭვირვალობა, ანგარიშვალდებულება, კანონიერება და სამართლიანობა, მონაცემთა უსაფრთხოება, მონაცემთა დაცვაზე ზეგავლენის შეფასება და სხვა.

ხელოვნური ინტელექტის გამოყენება სხვადასხვა სფეროში სხვადასხვაგვარ მიზანს შეიძლება ემსახურებოდეს, მაგალითად, *ბიზნეს სექტორში* - მომხმარებლების ქცევის ანალიზის გზით შეთავაზებებისა და მომსახურების მათზე მორგებას, *საგანმანათლებლო სექტორში* - პროცესის მარტივად წარმართვას, პერსონალიზებული სასწავლო გეგმის შედგენას, *ჯანმრთელობის დაცვის სფეროში* - დაავადებათა სიმპტომების დროულ აღმოჩენას, დიაგნოზირებას, დიაგნოსტიკის ანალიზს[51], *დასაქმების პროცესში* - კონკრეტული პოზიციისთვის თავის წარმატებით გართმევის შანსების პროგნოზირებას მის შესახებ ისეთი ინფორმაციის დამუშავების საფუძველზე როგორიცაა პროფესიული გამოცდილება, განათლება, ტესტირების პასუხები და სხვა.

აღნიშნულ შემთხვევებში, პირველ რიგში მნიშვნელოვანია შეფასდეს ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავებისთვის რა სამართლებრივი საფუძველი შეიძლება ჰქონდეს ორგანიზაციას. *მაგალითად,* შესაძლებელია მომხმარებლის შესახებ გარკვეული ინფორმაცია აუცილებელი იყოს შეკვეთის გაფორმებისთვის, მისთვის მომსახურების გაწევისთვის, თუმცა შემდგომში ამ ინფორმაციის ხელოვნური ინტელექტის მეშვეობით სუბიექტის პრეფერენციების გასაანალიზებლად

[50] იქვე.
[51] World Economic Forum, 5 Ways AI is Transforming Healthcare, <https://www.weforum.org/stories/2025/01/ai-transforming-global-health/> [22.01.2025].

დამუშავებისთვის განსხვავებული სამართლებრივი საფუძველი იყოს საჭირო. ძირითად შემთხვევებში ეს შეიძლება იყოს *თანხმობა ან ლეგიტიმური ინტერესი.* ამასთან მნიშვნელოვანია რომ თუ აღნიშნული ტექნოლოგიების მეშვეობით მონაცემთა დამუშავების საფუძველი იქნება უშუალოდ სუბიექტების თანხმობა, მონაცემთა სუბიექტმა იგი მხოლოდ სათანადოდ, მისთვის მარტივ გასაგებ ენაზე ინფორმაციის მიწოდების შემდეგ, ნებაყოფლობით უნდა განაცხადოს. რაც შეეხება ლეგიტიმურ ინტერესს, აღნიშნული საკითხი ყოველ კონკრეტულ შემთხვევაში ინდივიდუალურად უნდა შეფასდეს და მხედველობაში უნდა იქნეს მიღებული წინა თავში განხილული კრიტერიუმები. *მაგალითად, უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანოს ერთ-ერთ გადაწყვეტილებაში,* რომელიც ბანკის მიერ ხელოვნური ინტელექტის მეშვეობით მომხმარებლებთან საუბრის ჩანაწერის, კმაყოფილების შეფასების მიზნით ემოციურ ელემენტების გაანალიზებას ეხება, სუბიექტები ინფორმირებულები იყვნენ აუდიომონიტორინგის თაობაზე, თუმცა აღნიშნული ჩანაწერების შემდგომი დამუშავების თაობაზე ინფორმაციას არ ფლობდნენ. ბანკი თანამედროვე ტექნოლოგიების მეშვეობით მონაცემთა დამუშავების საფუძვლად ლეგიტიმურ ინტერესს - ხარისხის კონტროლს მიიჩნევდა. საზედამხედველო ორგანომ ხელოვნური ინტელექტის მეშვეობით მომხმარებლებისა და თანამშრომლების აუდიოჩანაწერების დამუშავება უკანონოდ მიიჩნია, რადგან ლეგიტიმური ინტერესის შეფასებისას მხედველობაში არ ყოფილა მიღებული დამუშავების პროპორციულობა, ამასთან მომხმარებლები არ ყოფილან ინფორმირებული მათი ხმის ანალიზის თაობაზე, შესაბამისად შეუძლებელი იქნებოდა მათ მიერ „უარის თქმის“ უფლების განხორციელება და არც ზეგავლენის შეფასება შეიცავდა რაიმე სახის შემამსუბუქებელ ღონისძიებებს მონაცემთა სუბიექტის უფლებებზე გავლენებისა და საფრთხეების შესამცირებლად. აღნიშნულიდან გამომდინარე საზედამხედველო ორგანომ ხელოვნური ინტელექტის მეშვეობით მომხმარებლებისა და დასაქმებული პირების პერსონალური მონაცემების დამუშავების პროცესი კანონთან შეუსაბამოდ მიიჩნია. [52]

ხელოვნური ინტელექტის სისტემების გამოყენებით მონაცემთა დამუშავებისას ასევე აუცილებელია *მონაცემთა მინიმიზაციის პრინციპის* გათვალისწინება. დიდი ბრიტანეთის საზედამხედველო ორგანოს (“ICO”) რეკომენდაციის თანახმად, დასაქმების აგენტებმა თავიანთის საქმიანობის პროცესში სისტემების გამოყენებისას *უნდა შეაფასონ ხელოვნური ინტელექტის მიერ შეგროვებული ინფორმაცია და დარწმუნდნენ რომ ეს მათი დამუშავების მიზნებისთვის მინიმალურად აუცილებელი ინფორმაცია იქნება, დარწმუნდნენ რომ აღნიშნული მონაცემები ხელოვნური ინტელექტის მიმწოდებლების მიერ არ დამუშავდება განსხვავებული მიზნებისთვის.*[53]

[52] *Nemzeti Adatvédelmi és Információszabadság Hatóság* (*NAIH),* [2024], NAIH-85-3/2022, <https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022> [10.01.2025].

[53] *ICO,* AI tools in recruitment, 2024, <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf> [10.01.2025].

აღნიშნული მიდგომა უნდა გავრცელდეს ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავების სხვა პროცესებზეც.

გამჭვირვალობა მონაცემთა დამუშავების ერთ-ერთ უმნიშვნელოვანეს პრინციპს წარმოადგენს და მოიაზრებს რომ მონაცემთა სუბიექტებს უნდა მიეწოდოთ ინფორმაცია პერსონალური მონაცემების დამუშავების თაობაზე, ლაკონურად, მათთვის გასაგებ ენაზე, ამასთან ინფორმაცია მარტივად უნდა იყოს ხელმისაწვდომი.[54] აღნიშნული პრინციპის დაცვა, ხელოვნური ინტელექტის მეშვეობით მონაცემების დამუშავებისას გარკვეულწილად შესაძლოა რთული იყოს, ვინაიდან მანქანური სწავლების ბევრი მოდელი „შავ ყუთს“ წარმოადგენს და იგი თავისივე პროგნოზების განმარტებას ადამიანისთვის გასაგებ ენაზე არ ახდენს.[55] შესაბამისად AI სისტემების მიერ მიღებული გადაწყვეტილებების ინტერპრეტირება, განმარტება შესაძლოა უშუალოდ მასზე მომუშავე პირებისთვისაც რთული იყოს, რაც დამუშავებისთვის პასუხისმგებელი პირის მიერ ვალდებულებების შესრულებისას გარკვეულ გამოწვევებს ქმნის.

მონაცემთა სამართლიანად, ღირსების შეულახავად დამუშავება ასევე უმნიშვნელოვანეს პრინციპს წარმოადგენს, რომელიც ყველა დამუშავების პროცესში უნდა იყოს დაცული. როგორც წინა თავში აღინიშნა, იქიდან გამომდინარე, რომ ხელოვნური ინტელექტის სისტემების მუშაობა მისი სწავლების პროცესში გამოყენებულ მონაცემებზეა დამოკიდებული, დიდია შანსი იმისა რომ აღნიშნული სათანადოდ არ ასახავდეს საზოგადოების ყველა ჯგუფის მახასიათებლებს, ან ეფუძნებოდეს ისტორიულ მონაცემებს, რაც სხვადასხვაგვარ სტიგმებს შეიცავს. აღნიშნული უკვე შემდგომ, დამუშავებისთვის პასუხისმგებელ პირს სისტემით სარგებლობის ეტაპზე მიკერძოებულ, დისკრიმინაციულ გადაწყვეტილებებამდე მიიყვანს. ხელოვნური ინტელექტის სისტემებისთვის დამახასიათებელია როგორც ისტორიული, სოციალური, ასევე ალგორითმული მიკერძოებები.[56] *მაგალითად,* დასაქმების სფეროში გამოყენებადი ხელოვნური ინტელექტის სისტემა, რომლის სწავლების პროცესი მამრობითი სქესის წარმომადგენლების რეზიუმეებს ეფუძნებოდა, გამოყენებისას, ახდენდა ყველა ქალი კანდიდატის ინფორმაციისგან გაფილტვრას და უპირატესობას მამაკაც კანდიდატებს ანიჭებდა.[57]

ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავების საკითხთან დაკავშირებით ასევე გასათვალისწინებელია, რომ მონაცემთა სუბიექტს უფლება აქვს, არ დაექვემდებაროს მხოლოდ ავტომატიზებულად,

[54] *Article 29 Working Party,* Guidelines on transparency under Regulation 2016/679, 2018.

[55] *Cynthia Rudin,* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions And Use Interpretable Models Instead, Nature Machine Intelligence, VOL 1, 2019, 206–215, <https://doi.org/10.1038/s42256-019-0048-x> [10.01.2025].

[56] *Shrishak K.,* AI-Complex Algorithms and effective Data Protection Supervision Bias evaluation, *EDPB,* Support Pool of Experts Programme, 2024, 5-6, <https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf> [10.01.2025].

[57] *Byrne A., Lee D., Le Q.,* Bias in AI: Tackling the Issues through Regulations and Standards, 2024, <https://publicpolicy.ie/wp-content/uploads/2024/10/Bias_in_AI.pdf> [10.01.2025].

მიღებულ გადაწყვეტილებას, რომელიც მისთვის წარმოშობს სამართლებრივ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს, გარდა იმ შემთხვევებისა თუ აღნიშნულის თაობაზე არსებობს სუბიექტის თანხმობა, ხელშეკრულების შესრულების/დადების მიზნითაა აუცილებელი ან კანონით თუ კანონქვემდებარე აქტითაა გათვალისწინებული.[58] შესაბამისად აღნიშნულ შემთხვევებში აუცილებელია მონაცემთა სუბიექტზე გავლენის მქონე გადაწყვეტილებების მიღება მხოლოდ სისტემის პროგნოზებს/დასკვნებს არ ეფუძნებოდეს და ადამიანური ზედამხედველობა ერთოდეს თან.

ზემოაღნიშნულ შემთხვევებში მონაცემთა სუბიექტის უფლებებისადმი მომეტებული რისკიდან, მათი შელახვის მაღალი საფრთხიდან გამომდინარე, ხელოვნური ინტელექტის სისტემების მეშვეობით მონაცემთა დამუშავებამდე შესაძლოა აუცილებელი იყოს მონაცემთა დაცვაზე ზეგავლენის შეფასება. აღნიშნული ერთი მხრივ სუბიექტის უფლებების დაცვის დამატებით გარანტიას ქმნის, ხოლო მეორე მხრივ დაეხმარება დამუშავებისთვის პასუხისმგებელ პირს ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავებისას ანგარიშვალდებულებისა და კანონიერი დამუშავების დემონსტრირებაში.[59] ორგანიზაცია რომელიც ხელოვნური ინტელექტის მეშვეობით სუბიექტების მონაცემთა დამუშავებას გადაწყვეტს უნდა დარწმუნდეს აღნიშნული სისტემების უსაფრთხოებაში, მათ შორის ტექნოლოგიის ტექნიკური თუ კონფიდენციალურობის დოკუმენტაციის მეშვეობით და განახორციელოს პერიოდული ზედამხედველობა, მისი კომპეტენციის ფარგლებში.

4. დასკვნა

ხელოვნური ინტელექტი, თანამედროვე ტექნოლოგიებში დღესდღეობით მოწინავე ადგილს იკავებს და სხვადასხვა სფეროების განვითარების დიდი პოტენციალი გააჩნია. აღნიშნული სისტემების გამოყენება ისეთ სექტორებში, როგორიცაა განათლება, ჯანმრთელობის დაცვა, სამართალდაცვითი საქმიანობა, ბიზნესი და საზოგადოების განვითარებისთვის სხვა მნიშვნელოვანი სფეროები, საქმიანობის სპეციფიკიდან გამომდინარე სხვადასხვა დანიშნულებით შეიძლება იქნეს გამოყენებული. იგი შეიძლება ემსახურებოდეს საქმიანობის გამარტივებას, ინფორმაციის ანალიტიკას, რისკების შეფასებას, გადაწყვეტილების მიღებას ან პროგნოზირებას/დიაგნოსტიკას უფრო მცირე დროში. მისი მზარდი პოტენციალიდან გამომდინარე, მსოფლიოში AI-ის სამართლებრივი რეგულირების აუცილებლობა დადგა, რასაც შედეგად ისეთი აქტების შემუშავება მოჰყვა როგორიცაა ევროკავშირის ხელოვნური ინტელექტის აქტი და ევროპის საბჭოს ხელოვნური ინტელექტის ჩარჩო კონვენცია. ამასთან

[58] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14.06.2023, მუხლი 19 (1).

[59] ICO, How to Use AI and Personal Data Appropriately and Lawfully, 2022, <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf> [10.01.2025].

აღნიშნული სისტემების ეთიკური, ადამიანის უფლებებთან მიმართებით დაბალანსებული გამოყენების მიზნებისთვის უმნიშვნელოვანესია სხვადასხვა საერთაშორისო ორგანიზაციების კვლევითი და სარეკომენდაციო საქმიანობა. აღნიშნული გარკვეულ საფუძვლებს ქმნის ტექნოლოგიების სამართლებრივი რეგულირებების შექმნის, სრულყოფისთვის, ასევე თავისი წვლილი შეაქვს მათი ეფექტიანი იმპლემენტაციის პროცესში.

ხელოვნური ინტელექტის სისტემების შექმნა დიდი რაოდენობით მონაცემებს, მათ შორის პერსონალურ მონაცემებს, საჭიროებს, ამასთან განსაკუთრებით მაღალია მონაცემებისადმი მოთხოვნები მეტად კომპლექსურ მოდელებში. ხელოვნური ინტელექტის მიერ ფიზიკური პირების შესახებ ინფორმაციის დამუშავება უკავშირდება როგორც მისი სწავლების, განვითარების ეტაპს, ასევე შესაძლოა მის მთლიან „სასიცოცხლო ციკლს“ მოიცავდეს. პერსონალური მონაცემების დამუშავება შესაძლოა განხორციელდეს როგორც უშუალოდ ხელოვნური ინტელექტის სისტემებზე მომუშავე ორგანიზაციების მიერ, ასევე უშუალოდ იმ დამუშავებისთვის პასუხისმგებელი პირების მიერ რომლებიც სხვადასხვა სექტორში საქმიანობის ფარგლებში სუბიექტების მონაცემებს ხელოვნური ინტელექტის მეშვეობით ამუშავებენ. ხშირ შემთხვევები ავტომატიზებული დამუშავების ამ ფორმას ფიზიკური პირების ფუნდამენტური უფლებებისადმი საფრთხეების შექმნის პოტენციალი გააჩნია.

ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავებისას აუცილებელია, როგორც აღნიშნულ ტექნოლოგიებზე მომუშავე პირების, ისე მოსარგებლე ორგანიზაციების მიერ გათვალისწინებულ იქნეს ისეთი საკითხები როგორიცაა მონაცემთა დამუშავების საფუძველი, მინიმიზაციის, გამჭვირვალობის, სამართლიანობის, მიზნით შეზღუდვის, უსაფრთხოების პრინციპები. ამასთანავე, მხედველობაში უნდა იქნეს მიღებული მონაცემთა ავტომატიზებული დამუშავებით გადაწყვეტილების მიღების შემთხვევებში მონაცემთა დაცვის წესები. განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება, განსაკუთრებით კი იმ შემთხვევებში როდესაც ხელოვნური ინტელექტი გამოიყენება ჯანდაცვის სექტორში ან ისეთი საქმიანობის განხორციელებისას რაც განსაკუთრებული კატეგორიის მონაცემების დამუშავებას ითვალისწინებს. ხელოვნური ინტელექტის მიერ/მეშვეობით მონაცემთა დამუშავებისას უნდა მოხდეს სუბიექტების სათანადო ინფორმირება, წინააღმდეგ შემთხვევაში აღნიშნული მათი როგორც სუბიექტის სხვა უფლებების დაუდევრობით შეზღუდვასაც გამოიწვევს.

ხელოვნური ინტელექტის სისტემების მიერ მონაცემთა დამუშავების უარყოფითი გავლენების პრევენციისთვის თუ ეფექტიანი რეაგირებისთვის მნიშვნელოვანი როლი შესაძლოა ჰქონდეთ მონაცემთა დაცვის საზედამხედველო ორგანოებს. ხაზგასასმელია აღნიშნულ ტექნოლოგიებთან დაკავშირებით სარეკომენდაციო სახის დოკუმენტების, პოლიტიკის დოკუმენტების საჭიროება. ამასთან, ხელოვნური ინტელექტის სისტემების გავლენების შემცირებისთვის და მისით ეფექტიანი სარგებლობისთვის *(უფლებების დაცვის მხედველობაში მიღებით)* მნიშვნელოვანია

საზოგადოების ინფორმირების მიზნით, ცნობიერების ამაღლების სხვადასხვა აქტივობების განხორციელება, რაც აღნიშნული ტექნოლოგიების უარყოფითი გავლენების შემცირებაში დიდ წვლილს შეიტანს.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023.
2. საქართველოს კანონი „საქართველოს 2025 წლის სახელმწიფო ბიუჯეტის შესახებ“, 10/12/2024.
3. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 31 დეკემბრის №ბ/1259 ბრძანება „პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) 2025 წლის გეგმის დამტკიცების შესახებ“.
4. საქართველოს ეროვნული ბანკის პრეზიდენტის 2020 წლის 17 აგვისტოს №151/04 ბრძანება „მონაცემებზე დაფუძნებული სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების მოდელების რისკების მართვის დებულების დამტკიცების თაობაზე“.
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12/07/2024.
6. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 05.09.2024.
7. 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, 04/05/2016.
8. Agencia Española de Proteccion de Datos (AEPD), Innovation and Technology, <https://www.aepd.es/en/areas/innovation-and-technology> [20.02.2025].
9. *Agencia Española de Protección de Datos (AEPD),* Legal Report 0059/2023 of the Legal Office of the AEPD Ruling on the Difference Between AI Systems and Processing of Personal Data and the Assessment of the Level of Risk of Processings, [2023], <https://www.aepd.es/documento/informe-juridico-0059-2023-en.pdf> [20.02.2025].
10. *Article 29 Working Party,* Guidelines on transparency under Regulation 2016/679, 2018.
11. *Byrne A., Lee D., Le Q.,* Bias in AI: Tackling the Issues through Regulations and Standards, 2024, <https://publicpolicy.ie/wp-content/uploads/2024/10/Bias_in_AI.pdf> [20.02.2025].
12. *Council Of Europe (CoE) Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO),* Report on the Application of Artificial Intelligence in Healthcare and Its Impact on the “Patient–Doctor” Relationship, September 2024.

13. *Council of Europe (CoE) Committee on Artificial Intelligence (CAI),* Methodology for the Risk and Impact Assessment of AI Systems from the Point of View of Human Rights, Democracy and the Rule of Law ("The HUDERIA"), 28/11/2024, <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f> [20.02.2025].
14. *EDPS*, Artificial intelligence Act, <https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en> [20.02.2025].
15. *EDPB,* Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(F) GDPR, 2024, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> [20.02.2025].
16. *Gleeson B.,* How AI Is Reshaping the Future of Work Across Industries, <https://www.forbes.com/sites/brentgleeson/2024/12/03/how-ai-is-reshaping-the-future-of-work-across-industries/> [03.12.2024].
17. Geeks for Geeks, Turing Test in Artificial Intelligence, <https://www.geeksforgeeks.org/turing-test-artificial-intelligence/> [16.09.2024].
18. History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence, <https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/> [30.09.2021].
19. Information Commissioner's Office (ICO), Our Work on Artificial Intelligence, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> [20.02.2025].
20. *Information Commissioner's Office (ICO),* How to Use AI and Personal Data Appropriately and Lawfully, 2022, <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf> [20.02.2025].
21. *Information Commissioner's Office (ICO),* AI Tools in Recruitment, 2024, <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf> [20.02.2025].
22. IBM, What is Artificial Intelligence (AI)?, <https://www.ibm.com/think/topics/artificial-intelligence> [09.08.2024].
23. *Keskpaik S.,* Machine Unlearning, TechSonar Reports, 2024, <https://www.edps.europa.eu/system/files/2024-11/24-11-15_techsonar_2025_en.pdf> [20.02.2025].
24. *Kingsley O.A.,* Artificial intelligence research: A review on dominant themes, methods, frameworks and future research directions, Telematics and Informatics Reports, Volume 14, 1.1, 2024, <https://doi.org/10.1016/j.teler.2024.100127> [20.02.2025].
25. *McCarth J., Minsky M.L., Rochester N., Shannon C.E.,* A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 31.08.1955, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> [20.02.2025].

26. OECD, Artificial Intelligence Papers, <https://doi.org/10.1787/dee339a8-en> [20.02.2025].

27. *Organisation for Economic Co-operation and Development* (*OECD),* Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers, №8, OECD Publishing, Paris, 2024.
28. *OECD*, AI, Data Governance and Privacy: Synergies and Areas of International Cooperation, OECD Artificial Intelligence Papers, №22, OECD Publishing, Paris, 2024.
29. *Russell S. J., Norvig P.,* Artificial Intelligence: A Modern Approach, 4th Global Edition, Pearson Education Limited, 2021.
30. *Rudin C.,* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions And Use Interpretable Models Instead, Nature Machine Intelligence, Vol. 1, 2019, 206-215.
31. *Shrishak K.,* AI-Complex Algorithms and effective Data Protection Supervision Bias evaluation, EDPB, Support Pool of Experts Programme, 2024, <https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf> [20.02.2025].
32. *Schwab K.,* The Fourth Industrial Revolution, Encyclopedia Britannica, 31.05. 2023, <https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734> [10.01.2025].
33. *Stearns P, N.,* The Industrial Revolution in World History, 4th ed., Westview Press, 2013.
34. The European Data Protection Board (EDPB), EDPB Adopts Statement on Age Assurance, Creates a Task Force on AI Enforcement and Gives Recommendations to WADA, <https://www.edpb.europa.eu/our-work-tools/plenary-meetings/102nd-plenary-meeting_en> [12.02.2025].
35. *The European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024,* <https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [20.02.2025].
36. *The European Data Protection Board ("EDPB"),* Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024, §43, <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> [20.02.2025].
37. *The Europol Innovation Lab,* An Observatory Report on AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, <https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf> [20.02.2025].
38. *The Global Privacy Assembly,* Resolution on Generative Artificial Intelligence Systems, 45th Closed Session, 2023, <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf>
39. UNESCO, Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence> [20.02.2025].

40. *UNESCO,* Towards a Human-Centred Approach to the Use of Generative AI, 2023, 21, <https://doi.org/10.54675/EWZM9535> [20.02.2025].

41. *United Nations (UN),* Seizing The Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 11.03.2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf> [20.02.2025].
42. World Economic Forum, 5 Ways AI is Transforming Healthcare, <https://www.weforum.org/stories/2025/01/ai-transforming-global-health/> [22.01.2025].
43. *Garante per la Protezione dei Dati Personali (Garante),* [2023], no. 9852214, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214> [20.02.2025].
44. *Garante per la Protezione dei Dati Personali (Garante),* [2014], no. 10085455, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10085455> [20.02.2025].
45. *Nemzeti Adatvédelmi és Információszabadság Hatóság* (*NAIH),* [2024], NAIH-85-3/2022, <https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022> [20.02.2025].
46. <https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed> [20.02.2025].
47. <https://artificialintelligenceact.eu/implementation-timeline/> [20.02.2025].

მარიკა აბაზაძე*

პერსონალურ მონაცემთა დაცვა სამეცნიერო და აკადემიური კვლევის პროცესში

საქართველოში „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის ამოქმედებით, განსაკუთრებული აქტუალობა შეიძინა მონაცემთა უსაფრთხოების დაცვის მაღალ სტანდარტსა და აკადემიური კვლევის მიზნით მონაცემთა დამუშავების ინტერესს შორის ბალანსის დაცვამ. წინამდებარე სტატია მიმოიხილავს სამეცნიერო და აკადემიური კვლევის პროცესში გასათვალისწინებელ პერსონალურ მონაცემთა დაცვის სამართლებრივ ასპექტებს.

სტატიაში განხილულია მკვლევრების მიერ ყოველდღიურ საქმიანობაში გასათვალისწინებელი საკითხები და შესაბამისი საუკეთესო პრაქტიკა.

***საკვანძო სიტყვები:** სამეცნიერო და აკადემიური კვლევა, მონაცემთა მეორეული დამუშავება, მონაცემთა სუბიექტის თანხმობის ნამდვილობა, პერსონალურ მონაცემთა უსაფრთხოების დაცვა, მონაცემთა სუბიექტის უფლებები.*

1. შესავალი

სამეცნიერო და აკადემიური კვლევის პროცესი, ხშირ შემთხვევაში, ინფორმაციის შეგროვებას და ციფრული ან მატერიალური ფორმით შენახვას ითვალისწინებს. ამ მიმართულებით მთავარი გამოწვევა პერსონალურ მონაცემთა შემცველი ინფორმაციის, მონაცემთა დაცვის კანონმდებლობის შესაბამისად გამოყენება და გაზიარებაა.

პერსონალურ მონაცემთა დაცვა მონაცემთა სუბიექტის ძირითადი უფლებაა და შესაბამისად, მისი დაცვის საკითხი აქტუალურია აკადემიური

* მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის სამართლის მაგისტრი, დუბლინის საქალაქო უნივერსიტეტი (Dublin City University (DCU)); საზოგადოებრივ საქმეთა ინსტიტუტის (GIPA) საერთაშორისო სამართლის მაგისტრი; პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის მკვლევარ-ანალიტიკოსი.

კვლევის დაგეგმვის ეტაპიდანვე, კვლევის მიზნის განსაზღვრისას.[1] საგულისხმოა, რომ მონაცემთა სუბიექტის „კონფიდენციალურობა“, როგორც ცნება, სხვადასხვა კულტურისა და კონტექსტის გათვალისწინებით სხვადასხვაგვარად შეიძლება განიმარტოს,[2] აღნიშნულიდან გამომდინარე, საჭიროა მონაცემთა დამუშავების საკითხი კვლევის კონტექსტის შესაბამისად განისაზღვროს.

მნიშვნელოვანია, რომ პერსონალურ მონაცემთა დაცვის პრიზმიდან შეფასდეს კვლევის ჩატარების მეთოდოლოგიაც. მაგალითად, მონაცემთა სუბიექტებზე ფარულად დაკვირვებისას საჭიროა ცნებების „საჯარო“ და „კერძო“ განმარტებების საკვლევ კონტექსტში გააზრება. ფარულად მიმდინარე დაკვირვების ჩატარება დასაშვებია მხოლოდ მაშინ, თუ მკვლევარს ნათლად შეუძლია აჩვენოს ამ მეთოდის დადებითი მხარეები, აგრეთვე დაასაბუთოს, რომ სხვა მეთოდის გამოყენებით სასურველი შედეგის მიღწევა ძალიან რთული ან შეუძლებელია. ამავდროულად, საჭიროა მკვლევრის მიერ დასაბუთდეს, რომ ფარული დაკვირვება მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებზე უარყოფით ზეგავლენას არ მოახდენს.

პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის ვალდებულება ვრცელდება კვლევის მიზნებისა და მეთოდოლოგიის განსაზღვრის შემდგომ, კვლევის პრაქტიკულად განხორციელების ეტაპებზეც: მონაცემთა შეგროვების; მონაცემებზე ხელმისაწვდომობის; რესპონდენტთან კომუნიკაციის და ინფორმაციის შენახვის ან/და წაშლის დროს. ზოგიერთი დაწესებულების და ორგანიზაციის მონაცემთა დაცვის სტრატეგიულ დოკუმენტში მონაცემთა სწორად შენახვის და სისწორის შენარჩუნების წესები დეტალურად არის გაწერილი. აღნიშნული დოკუმენტი აერთიანებს მონაცემთა დამუშავების წესებს მონაცემთა დამუშავების სრული ციკლის გათვალისწინებით.[3]

კვლევის პროცესი, შეიძლება, ითვალისწინებდეს მონაცემთა საერთაშორისო გადაცემას. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”) მიზნად ისახავს მონაცემთა დაცვის წესთა ჰარმონიზაციას ევროპის მასშტაბით. თუმცა, იმ შემთხვევაში, თუ მონაცემები სტატისტიკური ან აკადემიური კვლევის მიზნით მუშავდება, შესაძლებელია საკითხის მოწესრიგება დამატებითი, ეროვნული წესების შემუშავების გზით. წევრი ქვეყნების აღნიშნული დისკრეცია ევროკავშირის მასშტაბით საკითხის საკანონმდებლო რეგულირების განსხვავებებს წარმოშობს. მაგალითისთვის, სხვადასხვა წევრი ქვეყანა „სამეცნიერო კვლევას“ სხვადასხვაგვარად განმარტავს, რაც, შესაძლოა, რიგი სამართლებრივი პრობლემის საფუძველი

[1] *European University Institute*, Guide on Good Data Protection Practice in Research, 2022, 5.
[2] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 27 (2).
[3] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.

გახდეს, ხელი შეუშალოს მონაცემთა საერთაშორისო გადაცემის პროცესს ან საერთაშორისო კვლევით თანამშრომლობას.[4]

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ პერსონალურ მონაცემთა დამუშავებას კვლევითი მიზნებით დასაშვებად მიიჩნევს, თუ მონაცემთა სუბიექტის უფლებების დასაცავად მიღებულია უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომები. აგრეთვე, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ითვალისწინებს პერსონალურ მონაცემთა დამუშავების საკანონმდებლო მოთხოვნებს.[5]

2. პერსონალურ მონაცემთა დამუშავების პრინციპები და მოქმედებები

საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ პერსონალურ მონაცემებთან მიმართებით განხორციელებული ნებისმიერი მოქმედება მონაცემთა დამუშავებად მიიჩნევა. კვლევითი პროექტების კონტექსტში, მონაცემთა დამუშავებად ჩაითვლება: რესპონდენტთა ელექტრონული ფოსტის მისამართების ნუსხის შედგენა; მონაცემთა ბაზის შექმნა და მართვა; აგრეთვე, მონაცემთა გაზიარება მესამე მხარისათვის. კანონის თანახმად, „პერსონალურ მონაცემთა დამუშავება“ განიმარტება, როგორც, ნებისმიერი მოქმედება ან მოქმედებათა ერთობლიობა პერსონალურ მონაცემთა გამოყენებით, განუსაზღვრელად დამუშავების ფორმისა და საშუალებებისა. მონაცემები შეიძლება დამუშავდეს როგორც ავტომატური, ასევე არაავტომატური საშუალებებით და სხვადასხვა მეთოდით, როგორიცაა: მონაცემთა შეგროვება; ჩაწერა; ორგანიზება; შენახვა; ადაპტაცია ან შეცვლა; მოძიება; კონსულტაცია; გამოყენება; გამჟღავნება; გადაცემა; გავრცელება ან სხვაგვარად ხელმისაწვდომობა; გასწორება ან კომბინაცია; დაბლოკვა; წაშლა ან განადგურება და სხვა.[6]

მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავებაზე სხვადასხვა სფეროში განსხვავებულ ვალდებულებებს წარმოშობს. მაგალითად, სამეცნიერო ან კლინიკური კვლევის პროცესში, მონაცემთა შეგროვების ეტაპზე, შესაძლოა, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ვერ შეძლოს ზუსტად განსაზღვროს მონაცემთა დამუშავების მხოლოდ ერთი, კონკრეტული მიზანი.[7] რეგულაცია განმარტავს, რომ, დამუშავების სფეროსა და კონტექსტის გათვალისწინებით, მონაცემთა სუბიექტები უფლებამოსილნი არიან დაეთანხმონ პერსონალურ მონაცემთა დამუშავებას მეტად ზოგადი მიზნებისათვისაც.[8]

---

[4] *Ducato R.,* Data protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020,14.

[5] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 4(6).

[6] იქვე, 3 (ვ).

[7] *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016, pg 6.

[8] *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].

იმ შემთხვევაში, თუ საჭიროა მონაცემთა საერთაშორისო გადაცემა ან კვლევითი პროექტი ხორციელდება საერთაშორისო ორგანიზაციის ჩართულობით, რეკომენდებულია მკვლევრებმა გაითვალისწინონ და დაიცვან პერსონალურ მონაცემთა დაცვის შესაბამისი მოთხოვნები. კერძოდ, მონაცემთა დაცვის ადგილობრივი და საერთაშორისო კანონმდებლობა და სტანდარტები, საერთაშორისო ორგანიზაციის პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტით განსაზღვრული ვალდებულებები და სხვა შესაბამისი წესები. საჭიროა მკვლევრებმა მონაცემთა დამუშავების დაწყებამდე იზრუნონ სათანადო ნებართვის მიღებაზე, შესაბამისი მონაცემთა დაცვის საზედამხედველო ორგანოს ან კომიტეტის ინფორმირებაზე და შეასრულონ რიგი სხვა ვალდებულებები, რაც მათ შეიძლება ეკისრებოდეთ.[9]

მკვლევრის ვალდებულებაა უზრუნველყოს მონაცემთა სიზუსტე და ამ მიზნით პერიოდულად განაახლოს მონაცემები. აუცილებელია მონაცემთა უსაფრთხოების ზომებისა და მონაცემთა სუბიექტების უფლებების, მათ შორის მონაცემთა წაშლის - „დავიწყების უფლების დაცვა“. საჭიროა მონაცემები შენახული იქნას ისეთი ფორმით, რომელიც მონაცემთა სუბიექტების იდენტიფიცირების საშუალებას არ იძლევა და არაუმეტეს იმ დროით, რაც საჭიროა მონაცემთა შეგროვების მიზნის შესასრულებლად.[10] კვლევის დასრულების შემდგომ, შესაძლოა, საჭირო გახდეს მონაცემებზე წვდომა სათანადო ანგარიშის მოსამზადებლად, თუმცა, ამ უკანასკნელი მიზნითაც კი, მონაცემთა განუსაზღვრელი ვადით შენახვის პრაქტიკა დასაშვებად არ მიიჩნევა.[11]

კვლევის დაგეგმვის ეტაპიდანვე მნიშვნელოვანია მონაცემთა შენახვის ვადისა და წაშლის შესახებ გეგმის შემუშავება, ასევე, საჭიროებისამებრ, მონაცემთა ავტომატიზებული წაშლის ფუნქციის დამატება. სასურველია მონაცემთა შენახვის დეტალური გეგმის დასახვა, იმ ინფორმაციასთან მიმართებით, რომლის შენახვაც იგეგმება კვლევის დასრულების შემდგომ. პერსონალურ მონაცემთა შენახვის ვადა დამოკიდებულია იმ თავდაპირველ მიზანზე, რომლის მისაღწევადაც შეგროვდა მონაცემები, ან რა მიზეზითაც მონაცემები განმეორებით დამუშავდა. აქედან გამომდინარე, როდესაც პერსონალურ მონაცემთა შენახვა კვლევის მიზნებისათვის აუცილებელი აღარ არის, აუცილებელია მონაცემები წაიშალოს ან დეპერსონალიზებული ფორმით დაარქივდეს.[12]

შედარებისთვის, საერთაშორისო პრაქტიკის თანახმად, მონაცემთა დაცვის პრინციპებთან შესაბამისობის თაობაზე მტკიცების ტვირთი მკვლევრებს, კვლევით პროექტზე პასუხისმგებელ პირებს ან/და დაწესებულებებს ეკისრებათ. გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) პერსონალურ მონაცემთა უსაფრთხოების

[9] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები კონფიდენციალურობის პოლიტიკის დოკუმენტის შემუშავების თაობაზე, 2025, 11.
[10] EDPS, *Preliminary Opinion on Data Protection and Scientific Research,* 2020, 23.
[11] ICO, Guideilne on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
[12] European University Institute, Guide on Good Data Protection Practice in Research, 2022.

დარღვევის მიზეზით გრინვიჩის უნივერსიტეტს ადმინისტრაციული ჯარიმა დააკისრა. დარღვევის საფუძველი სტუდენტის მიერ წამოწყებული კვლევითი პროექტი გახდა.[13] კერძოდ, აღნიშნულმა სტუდენტმა ვერ უზრუნველყო კვლევასთან დაკავშირებული გვერდის გამართვა უსაფრთხოების სათანადო ზომებით. შედეგად, ჰაკერული თავდასხმის გზით 20 000 მონაცემთა სუბიექტის განსაკუთრებული კატეგორიის პერსონალური მონაცემები არაავტორიზებულ პირთათვის გახდა ხელმისაწვდომი. აღნიშნული საქმე ხაზს უსვამს რისკების საფუძვლიანი შეფასების, მონაცემთა უსაფრთხოების პოლიტიკის დანერგვისა და პერსონალურ მონაცემთა დამუშავების წესებთან შესაბამისობის მიმართებით კონტროლის განხორციელების აუცილებლობას.

აკადემიური კვლევის მიზნებისათვის განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საფუძველი, ძირითადად, მონაცემთა სუბიექტის აშკარად გამოხატული თანხმობაა. განსაკუთრებული კატეგორიის მონაცემია (მათ შორის): ინფორმაცია რასობრივი ან ეთნიკური წარმომავლობის; პოლიტიკური შეხედულებების; რელიგიური ან ფილოსოფიური მრწამსის; პროფკავშირის წევრობის; გენეტიკურ მონაცემების; ბიომეტრიულ მონაცემების; ჯანმრთელობის შესახებ მონაცემების და სექსუალური ორიენტაციის ან აქტივობის შესახებ.[14] განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავების შემთხვევაში, საჭიროა მონაცემთა დამუშავების სათანადო საფუძვლის წარდგენა შესაბამის ეთიკის კომიტეტთან. მნიშვნელოვანია, რომ კვლევითი პროექტის ფარგლებში განიმარტოს მონაცემთა შეგროვების საჭიროების შესახებ, ასევე ჩატარდეს მონაცემთა დამუშავების პროპორციულობის შეფასება. საყურადღებოა, რომ სხვადასხვა წყაროდან შეგროვებული პერსონალური მონაცემები მხოლოდ მაშინ შეიძლება გაერთიანდეს, როდესაც აღნიშნული კანონის მიერ დაშვებულია.

3. ინფორმირებული თანხმობის მიღება პერსონალურ მონაცემთა დამუშავებაზე

იმისათვის, რომ მონაცემთა დამუშავება კანონიერი იყოს, აუცილებელია მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავებაზე. პერსონალურ მონაცემთა თანხმობის გარეშე დამუშავება დასაშვებია მხოლოდ ცალკეულ შემთხვევებში: მაგალითად, როდესაც მონაცემთა დამუშავებას ინდივიდის ლეგიტიმურ ინტერესებზე უარყოფითი გავლენა არ აქვს; კვლევითი პროექტის განხორციელების საჯარო ინტერესი აღემატება მონაცემთა სუბიექტის ლეგიტიმურ ინტერესებს; კვლევის მიზანი სხვაგვარად ვერ მიიღწევა ან მისი მიღწევა შესაძლებელია მხოლოდ არაპროპორციული

[13] *Lallie H.S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.

[14] Article 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).

ძალისხმევით. თანხმობის გარეშე მონაცემთა დამუშავების კანონიერება ხშირად დამოკიდებულია კონფიდენციალურობის უფლებასა და კვლევის სარგებელს შორის ურთიერთბალანსზე.[15] საგულისხმოა, რომ ზოგიერთ სიტუაციაში, ძირითადი რეგულაციის თანახმად, დამუშავების ზუსტი მიზნების განსაზღვრის გარეშეც მონაცემთა დამუშავება შესაძლოა კანონიერი იყოს[16], მაგალითად, პანდემიის დროს, იმ პირობით, რომ დაცული იქნება კვლევის ეთიკური სტანდარტები.[17]

მონაცემთა სუბიექტს ნებისმიერ დროს აქვს თანხმობაზე უარის გაცხადების უფლება, შესაბამისი მიზეზის გაცხადების გარეშე. აგრეთვე, მისი უფლებაა დამუშავებული ინფორმაციის წაშლისა და დაბლოკვის მოთხოვნაც.[18] მკვლევარი, შეიძლება იურიდიული გამოწვევების ან პასუხისმგებლობის წინაშე აღმოჩნდეს, თუ მის მიერ მონაცემთა სუბიექტისგან მიღებული თანხმობა არ არის ნამდვილი. მონაცემთა სუბიექტის „ნამდვილი“ თანხმობა ნიშნავს ნებისმიერ თავისუფლად გაცემულ, კონკრეტულ, ინფორმირებულ და ცალსახა მითითებას პერსონალური მონაცემთა დამუშავებაზე თანხმობის შესახებ. [19]

თანხმობა ნამდვილია იმ შემთხვევაში, თუ მონაცემთა სუბიექტს გააჩნდა მონაცემთა შეგროვებასთან დაკავშირებით რეალური არჩევანის გაკეთების საშუალება. ნამდვილ თანხმობას გამორიცხავს ისეთი პრაქტიკები როგორიც არის მონაცემთა სუბიექტზე ნებისმიერი ფორმით ზემოქმედება, მათ შორის მისი შეცდომაში შეყვანა,[20] დაშინება ან იძულება. რესპონდენტის თანხმობა საჭიროა იყოს კონკრეტული, ნათლად გამოვლენილი, ზუსტად პასუხობდეს და ეთანხმებოდეს მონაცემთა დამუშავების მიზანს და შედეგებს.[21] მონაცემთა დამუშავებამდე, საჭიროა მონაცემთა სუბიექტის ინფორმირება იმის შესახებ, თუ რა ტიპის ინფორმაცია მუშავდება. სხვადასხვა დამუშავების მოქმედებათა განსახორციელებლად მონაცემთა სუბიექტისგან თანხმობის ერთხელ მიღება საკმარისია, თუ მონაცემთა სუბიექტს, გამომდინარე იმ ინფორმაციიდან რაც მან მიიღო, აქვს გონივრული მოლოდინი, რომ მისი მონაცემების გამოყენებით წინამდებარე ღონისძიებები განხორციელდება.[22]

---

[15] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021, 26.

[16] *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020, 3.

[17] Recital 33, 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).

[18] სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, 9.

[19] Recital 32, 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).

[20] EDPS, A Preliminary Opinion on Data Protection and Scientific Research, 2020, 19.

[21] სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, 21.

[22] WP29-ის სახელმძღვანელო პრინციპები ავტომატური ინდივიდუალური გადაწყვეტილების მიღების და პროფაილინგის შესახებ, 2016/679 (WP251) რეგულაციის მიზნებისთვის, პუნქტი IV.B, მე-20 და შემდგომი გვერდები.

საჭიროა კვლევის რესპონდენტებს მიეცეთ სრული და სწორი ინფორმაცია მონაცემთა დამუშავების მიზნების, დამუშავებულ მონაცემთა კატეგორიის, მეორეული დამუშავების, გადაცემის, შენახვის ვადის და მონაცემთა სუბიექტის თანამდევი უფლებების შესახებ, აგრეთვე, ინფორმაცია მონაცემთა დამუშავებაზე უარის თქმის უფლების შესახებ - მონაცემთა სუბიექტი თავისუფალია არჩევანში დაეთანხმოს ან უარი უთხრას შესაბამის პირს პერსონალურ მონაცემთა დამუშავებაზე.[23]

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა ამტკიცოს, რომ მონაცემთა სუბიექტი დაეთანხმა პერსონალურ მონაცემთა დამუშავებაზე და მისი პერსონალური მონაცემების გამოყენებაზე კონკრეტული კვლევასთან დაკავშირებული მიზნით.[24] ამ მიმართულებით გასათვალისწინებელი საკითხებია: სუბიექტთა ურთიერთმიმართება - როგორიცაა: ფაქტობრივი ან იურიდიული იერარქია; ეკონომიკური დამოკიდებულება მკვლევარსა და კვლევის მონაწილეს შორის; კვლევის მონაწილის მოწყვლადობა და კვლევის შედეგი პიროვნებაზე ან საზოგადოებაზე.

4. პერსონალურ მონაცემთა „მეორეული დამუშავება“

პერსონალურ მონაცემთა განმეორებით დამუშავებისას, პირველადი დამუშავების მიზნისაგან განსხვავებული მიზნით, სახეზეა მონაცემთა მეორეული დამუშავების შემთხვევა. მონაცემთა მეორეული დამუშავება უკანონოა თუ მონაცემები შეგროვდა ერთი კვლევითი პროექტისათვის და სხვა კვლევისათვის იქნა გამოყენებული, ისე, რომ მონაცემთა სუბიექტმა არ იცოდა ახალი კვლევის შესახებ და არ განუცხადებია შესაბამისი თანხმობა მონაცემთა დამუშავებაზე.[25]პერსონალურ მონაცემთა მეორეული დამუშავება კანონიერად ჩაითვლება იმ შემთხვევაში, თუ მონაცემთა პირველადი დამუშავებისას მიღებული მონაცემთა სუბიექტების თანხმობა მოიცავს ახალი კვლევის მიზნებისათვის პერსონალურ მონაცემთა დამუშავებაზე თანხმობასაც, ან ახალი კვლევის წარმოებისას მკვლევრები უზრუნველყოფენ თანხმობის მიღებას ახალი კვლევის მიზნებისათვის.[26]

მკვლევრის ვალდებულებაა მონაცემთა სუბიექტის სრულად ინფორმირება ინფორმაციის შეგროვებისას, მათ შორის, ინფორმირებული თანხმობის მნიშვნელობის შესახებ. აგრეთვე, თუ კვლევის პროცესში გამოიყენება საჯაროდ ხელმისაწვდომი ინფორმაცია, რეკომენდებულია

[23] ასევე, იხ. GDPR-ის პრეამბულა, 42-ე პუნქტი: „[...] იმისთვის, რომ თანხმობა ინფორმირებული იყოს, მონაცემთა სუბიექტისთვის, საჭიროა ცნობილი იყოს, სულ მცირე, დამუშავებისთვის პასუხისმგებელი პირის ვინაობა და მონაცემთა დამუშავების მიზანი. [...].“

[24] Article 7 and Recital 32, 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).

[25] იქვე, Recital 50.

[26] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 7.

მიეთითოს შესაბამისი წყაროს შესახებ. კვლევის პროცესში, საჭიროა პერსონალურ მონაცემთა კატეგორიის სწორად განსაზღვრა და მათი სათანადოდ დაცვა. პერსონალურ მონაცემთა კატეგორიას მიეკუთვნება: (მათ შორის) მონაცემთა სუბიექტის სახელი; სახლის მისამართი; ელექტრონული ფოსტის მისამართი, გეოგრაფიული მდებარეობის შესახებ ინფორმაცია. განსაკუთრებული კატეგორიის პერსონალური მონაცემების მაგალითად კი გამოდგება ინფორმაცია, რომელიც ეხება რელიგიურ, პოლიტიკურ შეხედულებებს ან სამედიცინო მონაცემებს. მათი დამუშავებისას მეტი სიფრთხილის გამოჩენაა საჭირო, ვინაიდან აღნიშნული ინფორმაციის გამჟღავნებით მონაცემთა სუბიექტების უფლებებს შესაძლოა მეტი ზიანი მიადგეს.[27]

პერსონალურ მონაცემთა დაცვის ტექნიკური და ორგანიზაციული ზომების განსაზღვრისას მნიშვნელოვანია გამოკითხულთა ვინაობის გათვალისწინება, რადგან, მონაცემთა სუბიექტების სხვადასხვა კატეგორიის გამოკითხვის შემთხვევაში შეიძლება საჭირო გახდეს პერსონალურ მონაცემთა დაცვის სხვადასხვა ზომის გამოყენება. მაგალითისთვის, კვლევითი პროექტის გამოკითხულთა კატეგორიებია: პაციენტი, მოხალისე (გამოკითხვისთვის, სამედიცინო კვლევისთვის და ა.შ.) თანამშრომელი (მაგალითად, კვლევითი ლაბორატორიის პერსონალი), კვლევაში ჩართული სხვა მკვლევარი, არასრულწლოვანი, ბავშვი ან მოზარდი და სხვა.[28]

როდესაც მონაცემთა მეორეული დამუშავება არ ეფუძნება მონაცემთა სუბიექტის თანხმობას ან კანონის მოთხოვნას, დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია დაამუშაოს პერსონალური მონაცემები დამუშავების პირველად მიზანთან „შესაბამისობის ტესტის“ საფუძველზე. წინამდებარე ტესტის საშუალებით, შესაძლოა, დადგინდეს, თუ რამდენად შეესაბამება მონაცემთა დამუშავების ახალი მიზანი მონაცემთა დამუშავების პირველად მიზანს.[29] აღნიშნულის დასადგენად კი დამუშავებისთვის პასუხისმგებელმა პირმა საჭიროა გაითვალისწინოს კავშირი მონაცემთა დამუშავების პირველად და ახალ მიზნებს შორის, მონაცემთა შეგროვების კონტექსტი, განსაკუთრებულ კატეგორიათა დამუშავების საკითხი, დამუშავების ზეგავლენა მონაცემთა სუბიექტების უფლებებზე, და მონაცემთა დაცვის გარანტიათა შესაბამისობა[30] მათი დამუშავების რისკებთან.[31]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლით განსაზღვრულია გამონაკლისი სფეროები, რომელთა

[27] პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დაცვის სახელმძღვანელო რეკომენდაციები მცირე და საშუალო ზომის მეწარმე სუბიექტებისათვის, 2024, 11.

[28] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, 2024, 17.

[29] *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018,4.

[30] მუხლი 89, 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).

[31] იქვე, მუხლი 5(1).

მიზნებისათვის მონაცემთა შემდგომი დამუშავება მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებლად არ მიიჩნევა. წინამდებარე გამონაკლისთა ჩამონათვალში ექცევა მონაცემთა შემდგომი დამუშავება საჯარო ინტერესების შესაბამისად არქივირების, სამეცნიერო, ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის.[32] საყურადღებოა, რომ ამ უკანასკნელი მიზნითაც პერსონალურ მონაცემთა მეორეული დამუშავებისას, პასუხისმგებელმა პირებმა საჭიროა შეაფასონ, მონაცემთა შემდგომი დამუშავების კანონიერების საკითხი. კერძოდ, რეკომენდებულია შეფასდეს მეორეული დამუშავების მიზნის შესაბამისობა დამუშავების პირველად მიზანთან.

5. კვლევის დაგეგმვისა და განხორციელების ეტაპზე გასათვალისწინებელი საკითხები

მონაცემთა დაცვის საკანონმდებლო მოთხოვნებთან შესაბამისობის მიზნებისათვის საჭიროა დეტალურად იყოს გააზრებული ის ინფორმაცია, რასაც მკვლევარი მიაწვდის კვლევაში ჩართულ რესპონდენტს. აუცილებელია ინფორმაციის მარტივი და ადვილად გასაგები ენით მიწოდება, რათა აღნიშნულმა ინფორმაციამ მონაცემთა სუბიექტს კვლევაში მონაწილეობის შესახებ თავისუფალი არჩევანის გაკეთების საშუალება მისცეს. რესპონდენტთა ინფორმირების ერთ-ერთი მეთოდია კვლევის შესახებ წინასწარ მომზადებული საინფორმაციო ფურცლის[33] გადაცემა კვლევის მონაწილისათვის, ისევე როგორც კითხვარზე ინფორმირებული თანხმობის პროტოკოლის დართვა.[34]

მონაცემთა დამუშავების შესახებ ინფორმირების მიმართულებით მნიშვნელოვანი საკითხია რესპონდენტების გაცნობა, და მათთან პირველი კომუნიკაციის დამყარება კვლევაში ჩართვის მოთხოვნით. იმ შემთხვევაშიც კი, როდესაც რესპონდენტი ოჯახის წევრი ან მეგობარია, მნიშვნელოვანია შესაბამისი ინფორმაციის გაზიარება და მათი თანხმობის მიღება პერსონალური მონაცემების დამუშავების თაობაზე. თუ პიროვნებას არ შეუძლია დაეთანხმოს მონაცემთა დამუშავებაზე, მაგალითად, არასრულწლოვანების გამო, აუცილებელია თანხმობის მიღება მათი მშობლების, მეურვის ან სხვა კანონიერი წარმომადგენლისაგან.

იმ შემთხვევაში, თუ კვლევა მოიცავს საველე სამუშაოს, ინფორმირებული თანხმობის მიღება შეიძლება არა ერთჯერადი, არამედ განგრძობითი პროცესი გახდეს, რომელიც, შესაძლოა განსხვავდებოდეს, კვლევის დაწყებამდე დაგეგმილ პროცესთან. დასაშვებია, მკვლევარს მოუხდეს თანხმობის შესახებ ხელახალი მოლაპარაკების წარმოება, იმ შემთხვევაში,

[32] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, 2024,17.

[33] *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, 1311-1316.

[34] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 15.

თუ აღმოჩნდა, რომ კვლევის პროცესში წინასწარ განუსაზღვრელი, ახალი საკითხები წარმოიშვა. ასევე, იმ შემთხვევაში, თუ ინტერვიუს ჩატარების ან კითხვარის შევსების დროს საჭირო გახდა დამატებითი ინფორმაციის გაცემა ან მიღება. საუბრის დასაწყისშივე, რეკომენდებულია რესპონდენტებს მიეწოდოთ ინფორმაცია იმ გამონაკლისების შესახებ, რასაც გულისხმობს ინფორმირებული თანხმობის მიღება. საჭიროა მონაცემთა სუბიექტებს ეცნობოთ, რომ შეიძლება საჭირო გახდეს თანხმობის შესახებ ხელახალი მოლაპარაკება, საუბრის მიმდინარეობიდან, ან განხილული თემატიკიდან წარმოშობილი საჭიროებებიდან გამომდინარე.

საჭიროა გამოსაკითხ საზოგადოებაში დამკვიდრებული კულტურული და ეთიკური ნორმების მხედველობაში მიღება. წერილობითი თანხმობა შეიძლება ეწინააღმდეგებოდეს რესპონდენტთა ეთიკურ ნორმებს, ან რესპონდენტთაგან თანხმობის მიღება შეუძლებელი აღმოჩნდეს სხვა მიზეზით. აღნიშნულ შემთხვევაში, რეკომენდებულია ალტერნატიული თანხმობის მექანიზმების შეთავაზება, როგორიცაა, მაგალითად, ვერბალური თანხმობის ჩანაწერის მომზადება ან მოწმის დასწრება. ნებისმიერი მეთოდის არჩევის შემთხვევაში, აუცილებელია გამოყენებული პროცედურის შესახებ შესაბამისი დოკუმენტების წარმოება. ისეთ შემთხვევაში, როდესაც რესპონდენტს არ შეუძლია საკუთარი სურვილის ნათლად გამოხატვა ან ინფორმაციის სათანადოდ გაგება, საჭიროა ინფორმირებული თანხმობა სხვა შესაბამისი საშუალებით ჩანაცვლდეს.

დაკვირვებითი კვლევის შემთხვევაში, კვლევის დაწყებამდე საჭიროა მიღებულ იქნას ინფორმირებული თანხმობა როგორც მონაცემთა სუბიექტთაგან, ასევე სხვა ზედამხედველი, მეურვე ან პასუხისმგებელი პირებისგან. საჯარო სივრცეში ადამიანებზე დაკვირვება, შესაძლოა, არ სჭირდებოდეს თანხმობის მიღებას. ამ მოცემულობაში, მკვლევრებს ევალებათ დაამტკიცონ, რომ მათ მიერ ჩატარებული კვლევა არ შეცვლის ან მოახდენს ნეგატიურ ზემოქმედებას ადამიანების ქცევაზე, და არ შელახავს მათი კონფიდენციალურობის უფლებას. აუცილებელია კვლევის ფარგლებში მონაცემთა დამუშავების შესახებ ბავშვთა ინფორმირების კუთხით შემუშავდეს სტრატეგია მათთვის მარტივად გასაგები მეთოდების გამოყენებით, მაგალითად, აუდიო ან ვიდეო მასალის გამოყენებით, ან ბავშვისთვის მარტივად აღსაქმელი საინფორმაციო ბროშურების მომზადების გზით.[35]

კიდევ ერთი საკვანძო საკითხია მკვლევრის უფლებამოსილება პერსონალურ მონაცემთა დამუშავების მიმართულებით. თუ მონაცემები განმეორებით მუშავდება, რომელიც პირველად სხვა კვლევისათვის დამუშავდა, საჭიროა პირველი კვლევის ჩატარებისას მიღებული თანხმობის მიღება განმეორებით, ახალი კვლევის მიზნებისათვის. როდესაც არსებობს სხვა კვლევითი პროექტისათვის შექმნილი მონაცემთა ბაზა, მნიშვნელოვანია გათვალისწინებულ იქნას სხვადასხვა საკითხი. მაგალითად, ვრცელდება თუ არა განმეორებით მონაცემთა დამუშავებაზე პირველად მიღებული

[35] იქვე.

მონაცემთა სუბიექტის ინფორმირებული თანხმობა. აღნიშნულ საკითხებზე კონსულტაციის გაწევა კომპანიის ან დაწესებულების ეთიკის კომისიის, მონაცემთა დაცვის ოფიცრის, ან პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს კომპეტენციაა.

6. მონაცემთა უსაფრთხოება

პერსონალურ მონაცემთა უსაფრთხოდ დამუშავების მიზნით, აუცილებელია სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება, რათა თავიდან იქნას არიდებული არაავტორიზებული წვდომა პერსონალურ მონაცემებზე. [36]აკადემიური და სამეცნიერო კვლევის პროცესში, მონაცემთა უსაფრთხოების დაცვის პრაქტიკული მეთოდი შეიძლება იყოს, მაგალითად, ჩანაწერების წარმოება წვდომის თაობაზე, რაც ცნობილია როგორც ინფორმაციის „ლოგირება“ და მიანიშნებს იმაზე თუ ვინ, როდის და რა ინფორმაციაზე განახორციელა წვდომა. ასევე, შესაძლოა კვლევის კონტექსტიდან გამომდინარე მონაცემების დასაცავად გამოყენებული იქნას სხვა შემდეგი მიდგომები: მომხმარებლის იდენტობის გადამოწმება ავტორიზაციის გზით; ელექტრონული ფაილების დაცვა პაროლებით (მაგალითად, პაროლით დაცული დოკუმენტის შენახვა); მონაცემთა ბაზის დაშიფვრა ანუ, მონაცემთა ისეთი ფორმით შენახვა, რომელიც გაუგებარს ხდის მას, და იგი გასაგები ხდება მხოლოდ ავტორიზებული პირისთვის, რომელსაც აქვს ე.წ. „გასაღები“ (პაროლი, რომლის საშუალებითაც ინფორმაცია კვლავ გახდება გასაგები).

მიუხედავად მონაცემთა შენახვის ადგილისა, კანონის მოთხოვნები მონაცემთა დაცვის მიმართულებით (იქნება ეს პერსონალური კომპიუტერი, მეხსიერების ბარათი, თუ „ქლაუდ“ ტექნოლოგია) თანაბრად ვრცელდება. საჭიროა პერსონალურ მონაცემებზე უსაფრთხო წვდომის წესი ნათლად ჩამოყალიბდეს და პერიოდულად განახლდეს და იყოს პროპორციული მოსალოდნელ უსაფრთხოების რისკებთან და დამუშავებულ მონაცემთა კატეგორიასთან. მაგალითად, განსაკუთრებული კატეგორიის მონაცემი, დაუცველი რესპონდენტი ან/და მკვლევარი შესაძლოა სხვა რესპონდენტებთან შედარებით მაღალი ხარისხის დაცვას საჭიროებდეს, მონაცემთა დამუშავების კონტექსტიდან და თანამდევი რისკებიდან გამომდინარე. რეკომენდებულია აღნიშნული დოკუმენტი, რომელშიც გაწერილი იქნება დამუშავებულ მონაცემებზე წვდომის წესი, მოიცავდეს ინფორმაციას გამოყენებულ დაცვის საშუალებებზე, მაგალითად, დაშიფვრა, დამცავი პაროლის გამოყენება და სხვა შესაბამისი საშუალებები.[37]

[36] *EDPS,* Preliminary Opinion on Data Protection and Scientific Research, 2020, 24.

[37]Article 4(13), (14) and (15) andArticle 9 and Recitals (51) to (56), 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).

არაავტორიზებული წვდომისაგან დაცვის მიზნით შესაძლოა საჭირო გახდეს მონაცემთა განცალკევება სხვა ინფორმაციისაგან. აღნიშნულის მაგალითია მონაცემთა ბაზების დაყოფა, რათა მონაცემთა სუბიექტების იდენტიფიცირება შეუძლებელი გახდეს არაავტორიზებულ პირთათვის. შეიძლება, განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა სხვა პერსონალური მონაცემებისაგან დამოუკიდებლად შენახვა მათი დაცვის მიზნით. ასევე, შესაძლებელია საჭირო გახდეს სამოქმედო გეგმის შემუშავება იმ მონაცემებთან დაკავშირებით, რომელთა შეგროვებაც წინასწარ არ იყო განსაზღვრული და მკვლევრისთვის ხელმისაწვდომი გახდა დაუგეგმავად, კვლევის პროცესში.

მონაცემთა გადაცემისას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია შეაფასოს მონაცემთა მიმღების პერსონალურ მონაცემთა დაცვის სისტემის ადეკვატურობა. მნიშვნელოვანია კვლევის მონაწილეებმა იცოდნენ იქნება თუ არა მათი მონაცემები გადაცემული მესამე ქვეყნებში. მონაცემთა დამუშავებაზე პასუხისმგებელმა პირმა შესაძლოა ვერბალურად აუხსნას მონაცემთა სუბიექტს მონაცემთა საერთაშორისო გადაცემის საკითხი. უკანასკნელ შემთხვევაში რთულდება მონაცემთა სუბიექტის მიერ გაცემული თანხმობის დოკუმენტებში ასახვა ან/და მტკიცებულების წარმოდგენა მიღებული თანხმობის თაობაზე. შესაძლებელია მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა შეიმუშაოს წერილობითი დოკუმენტი, რომელშიც ასახულია რესპონდენტთა თანხმობა პერსონალურ მონაცემთა დამუშავების შესახებ. საჭიროა მონაცემთა დაცვის ხარისხის შეფასება მესამე ქვეყანაში, სადაც იგეგმება ინფორმაციის გადაცემა, იმ მონაცემთა გადაცემის მეთოდების გათვალისწინებით, რა მეთოდებითაც იგეგმება ინფორმაციის გადაცემა. [38] სხვა სახელმწიფოში ან/და საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას აფასებს და მის შესახებ გადაწყვეტილებას იღებს პერსონალურ მონაცემთა დაცვის სამსახური მონაცემთა დამუშავების მომწესრიგებელი კანონმდებლობისა და პრაქტიკის ანალიზის საფუძველზე.[39]

პერსონალურ მონაცემთა უსაფრთხოების დაცვის კუთხით სასარგებლო ინსტრუმენტია მონაცემთა დეპერსონალიზაცია, ვინაიდან იგი იძლევა კვლევათა ჩატარების შესაძლებლობას, რომელთა განხორციელება შეუძლებელი იქნებოდა მათი კონფიდენციალურობის მიზეზით.[40] პერსონალურ მონაცემთა დეპერსონალიზაცია გულისხმობს პირდაპირი იდენტიფიცირების ისეთი საშუალებების ამოღებას ტექსტიდან, როგორიცაა მონაცემთა სუბიექტის სახელი, დაბადების თარიღი, ან მისამართი, თუმცა, ამ გზით სრულად ვერ გამოირიცხება მონაცემთა სუბიექტთა რეიდენტიფიცირების შესაძლებლობა. საყურადღებოა, რომ პირდაპირი იდენტიფიკატორების მოშორება ტექსტიდან, ავტომატურად არ ნიშნავს რომ

[38] *ცაგარეიშვილი ნ.,* პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები), პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, 1/2024, 84.

[39] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 42.

[40] რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ, 2024, 27.

მონაცემთა სუბიექტთა რეიდენტიფიცირება შეუძლებელია, ვინაიდან, არსებობს მათი რეიდენტიფიცირების შანსი სხვადასხვა ინფორმაციის გაერთიანების გზით.[41]

დეპერსონალიზაციის ხშირად გამოყენებული მეთოდია შემთხვევითი შერჩევის პრინციპი, რაც გულისხმობს მონაცემთა სუბიექტსა და ინფორმაციას შორის კავშირის წაშლას. თუ მონაცემები საკმარისად გაურკვევლად არის წარმოდგენილი, იგი ვეღარ დაუკავშირდება პიროვნებას.[42] დეპერსონალიზაციის ერთ-ერთი პრინციპია განზოგადება.[43] განზოგადების მიდგომის გამოყენებით ნაკლებია მონაცემთა იდენტიფიკაციის შანსი. მონაცემთა განზოგადების მაგალითად შესაძლოა მოვიყვანოთ მონაცემთა სუბიექტის საცხოვრებელი ქალაქის ან დაბის ნაცვლად, მიეთითოს რეგიონი, მეტად განზოგადებული გეოგრაფიული მდებარეობის ერთეული. ასევე, რესპონდენტის კონკრეტული ასაკის მითითების ნაცვლად, მინიშნება გაკეთდეს ასაკობრივ ჯგუფზე რომელშიც რესპონდენტი მოექცევა. საყურადღებოა, რომ მონაცემთა სუბიექტის ხელახალ იდენტიფიცირებასთან დაკავშირებული ყველა პრობლემის გადაწყვეტის საშუალებად არც ეს მეთოდი გამოდგება, ამიტომაც, სასურველია მონაცემთა დამუშავების კონკრეტულ კონტექსტზე მორგებული მონაცემთა დაცვის მეთოდის შერჩევა.

პერსონალურ მონაცემთა მინიმიზაციისა და უსაფრთხოების პრინციპების გათვალისწინება კვლევის ეთიკის მნიშვნელოვანი საკითხებია. მაგალითისთვის, შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ უმეას უნივერსიტეტის დაჯარიმების საქმე წარმოაჩენს პერსონალურ მონაცემთა უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომების გატარების მნიშვნელობას. უნივერსიტეტი განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა უსაფრთხოების წესების გათვალისწინების გარეშე ღრუბლოვან პლატფორმაზე შენახვის გამო დაჯარიმდა. აღნიშნულმა გადაწყვეტილებამ გამოკვეთა მკვლევრების ვალდებულება, განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავებისას უზრუნველყოს მონაცემთა დაცვის შესაბამისი მექანიზმების გამოყენება, როგორიცაა, მაგალითად, პერსონალურ მონაცემთა დაშიფვრა ან ანონიმიზაცია.[44]

კვლევის პროცესში დამუშავებული პერსონალური მონაცემების შემცველი ინფორმაციის დასაცავად კიდევ ერთი საშუალებაა პერსონალურ მონაცემთა ფსევდონიმიზაცია,[45] რომელიც გულისხმობს უნიკალური მახასიათებლების ჩანაცვლებას სხვა მახასიათებლით, მაგალითად, კოდით.[46] იმ შემთხვევაში, თუ ინფორმაციას მესამე პირი ინახავს ან ან იგი შენახულია

[41] იქვე, მუხლი 3(ც).
[42] AEPD, 10 Misunderstandings relating to Anonymisation, 2021, 5.
[43] Article 29 WP Opinion on Anonymisation Techniques, 2014.
[44] Decision of the DPA (Sweden), DI-2019-9432, 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].
[45] *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017, 344.
[46] EDPB Guidelines 01/2025 on Pseudonymisation, 2025, 36.

„ქლაუდ“ სისტემაში, საჭიროა გადამოწმდეს, რომ აღნიშნული მონაცემები უსაფრთხოდ წაიშალა. აგრეთვე, როდესაც, ინფორმაცია გადაიცა მესამე პირთან, რეკომენდებულია გადამოწმდეს, რომ მათ წინამდებარე ინფორმაცია დასახული მონაცემთა დამუშავების მიზნის შესრულების შემდგომ წაიშალა.

7. დასკვნა

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის ამოქმედებით მონაცემთა უსაფრთხოების მაღალი სტანდარტის დაცვისა და კვლევითი ინტერესების დაბალანსების საკითხმა განსაკუთრებული მნიშვნელობა შეიძინა. ამ მოცემულობაში, მკვლევრებს წარმოეშობათ მტკიცების ტვირთი იმის შესახებ, რომ იცავენ მონაცემთა დამუშავების კანონით განსაზღვრულ მოთხოვნებს როგორც კვლევის დაგეგმვის, ასევე მისი განხორციელების ყველა ეტაპზე.

მონაცემთა სუბიექტის კონფიდენციალურობის პატივისცემა და მისგან ინფორმირებული თანხმობის მიღება კვლევის პროცესის განუყოფელი ნაწილია. აკადემიურ და სამეცნიერო კვლევის პროცესში ხშირია მონაცემთა მეორეული დამუშავება, რაც გულისხმობს მონაცემთა გამოყენებას სხვა მიზნებისთვის, გარდა თავდაპირველად განსაზღვრულისა. ასეთ შემთხვევაში, საჭიროა მონაცემთა სუბიექტისაგან ახალი თანხმობის მიღება ან კანონით განსაზღვრული საფუძვლის არსებობა.

აუცილებელია პერსონალური მონაცემები დამუშავდეს მონაცემთა დამუშავების ძირითადი პრინციპების გათვალისწინებით; კანონიერად და გამჭვირვალედ; შეგროვდეს კონკრეტული, ნათელი და ლეგიტიმური მიზნების მისაღწევად, იყოს ზუსტი და საჭიროების შემთხვევაში განახლებული, ინახებოდეს იმ ფორმით, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას არაუმეტეს იმ დროისა, რაც საჭიროა დამუშავების მიზნებისთვის და იქნას მიღებული შესაბამისი ტექნიკური და ორგანიზაციული ზომები მონაცემთა უსაფრთხოების უზრუნველსაყოფად. განსაკუთრებული კატეგორიის მონაცემთა (მაგალითად, ჯანმრთელობის, ან/და რელიგიური შეხედულებების შესახებ ინფორმაციის) დამუშავებისას რეკომენდებულია დამატებითი სიფრთხილის გამოჩენა და მონაცემთა სუბიექტისაგან გამოხატული თანხმობის მიღება.

პერსონალურ მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელია ტექნიკური და ორგანიზაციული ზომების მიღება, როგორიცაა მონაცემების დაშიფვრა, პაროლებით დაცვა და წვდომის კონტროლი. ასევე, მნიშვნელოვანია მონაცემთა დეპერსონალიზაცია ან ფსევდონიმიზაცია, რათა შემცირდეს მონაცემთა სუბიექტის იდენტიფიცირების რისკი.

პერსონალურ მონაცემთა დამუშავების პრინციპების დაცვა სამეცნიერო და აკადემიურ კვლევათა წარმოების მიზნით არა მხოლოდ სამართლებრივი ვალდებულება, არამედ ეთიკური პასუხისმგებლობაც არის, რომელიც მონაცემთა სუბიექტების უფლებების პატივისცემას და კვლევის სანდოობას უზრუნველყოფს.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. 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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
3. პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ, 2024, 7.
4. პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დაცვის სახელმძღვანელო რეკომენდაციები მცირე და საშუალო ზომის მეწარმე სუბიექტებისათვის, 2024, 11.
5. პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები კონფიდენციალურობის პოლიტიკის დოკუმენტის შემუშავების თაობაზე, 2025.
6. სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით.
7. *ცაგარეიშვილი ნ.,* პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები), პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2024.
8. 29-ე სამუშაო ჯგუფის სახელმძღვანელო პრინციპები ავტომატური ინდივიდუალური გადაწყვეტილების მიღების და პროფაილინგის შესახებ, 2016/679 (WP251) რეგულაციის მიზნებისთვის.
9. *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].
10. *Ducato R.,* Data protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020.
11. EDPB Guidelines 01/2025 on Pseudonymisation, 2025.
12. EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020.
13. European University Institute, Guide on Good Data Protection Practice in Research, 2022.
14. ICO, Guideline on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
15. *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018.
16. *Lallie H.S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.

17. *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017.
18. *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020.
19. *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018.
20. *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.
21. *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016.
22. Decision of the DPA (Sweden), 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].

პერსონალურ მონაცემთა
დაცვის სამსახური

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