



პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

N1, 2024



პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

№1, 2024

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის შესაბამე გამოცემა ეძღვნება
„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ამოქმედებას

მთავარი რედაქტორი:

ასოც. პროფ. დოქტ. დოქტ. ლელა ჯანაშვილი
(თსუ; ბარსელონის ავტონომიური უნივერსიტეტი)

სარედაქციო კოლეგია:

პროფ. დოქტ. გიორგი ხუბუა (თსუ; ქუთაისის საერთაშორისო უნივერსიტეტის რექტორი)

პროფ. დოქტ. პაატა ტურავა (თსუ)

დოქტ. ოთარ ჩახუნაშვილი (თსუ)

პროფ. დოქტ. ნორბერტ ბერნსდორფი (მარბურგის ფილიპეს სახელობის უნივერსიტეტი)

პროფ. დოქტ. ხუან რამონ ფერეირო გალგერა (ოვიედოს უნივერსიტეტი)

პროფ. დოქტ. როსერ მარტინეს (ბარსელონის ავტონომიური უნივერსიტეტი)

პროფ. დოქტ. ხოსე ხულიო ფერნანდეს როდრიგეს (სანტიაგო-დე-კომპოსტელას უნივერსიტეტი)

პროფ. დოქტ. ტანელ კერიკმეე (ტალინის ტექნოლოგიური უნივერსიტეტი)

პროფ. დოქტ. ტიჰომირ კატულიჩი (ზაგრების უნივერსიტეტი)

დოქტ. ენდრი გიოზო საბო (ევროსტატის იურიდიული და პოლიტიკის ოფიცერი, მონაცემთა დაცვის კოორდინატორი)

ემვინი კუმარი (გიოტინგენის უნივერსიტეტი (LL.M.); ბრიუსელის თავისუფალი უნივერსიტეტის მკვლევარი)

აღმასრულებელი რედაქტორი:

ანა თოხაძე (ასისტენტი, თსუ)

ტექნიკური რედაქტორები:

ნინო ხუბულია (დოქტორანტი, თსუ)

ირაკლი ლეონიძე (დოქტორანტი, თსუ)

თარგმანი:

თეო კვატაშიძე

© პერსონალურ მონაცემთა დაცვის სამსახური, 2024

P-ISSN 2720-8753

E-ISSN 2720-8761

სარჩევი

ლელა ჯანაშვილი

მთავარი რედაქტორისაგან..... 5

ნორბერტ ბერნსდორფი

პერსონალური მონაცემების გადაცემა მესამე სახელმწიფოებში - „უსაფრთხო ნავსადგომი“, „ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემა“ და „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩო“ 7

ალექსანდრე ბოდუინი, ანდრეა ფ. ფერარისი

სინთეზური მონაცემების, როგორც ანონიმიზაციის სტრატეგიის სამართლებრივი და მარეგულირებელი პერსპექტივები..... 18

ეკატერინე შენგელია, ირაკლი ლეონიძე

ელექტრონული სანოტარო რეესტრი და მონაცემთა უსაფრთხოება..... 37

მაკა ნუცუბიძე

პერსონალურ მონაცემთა დაცვა მოქმედებების აღრიცხვის ჟურნალებში (ე.წ. „ლოგებში“) 52

ნინო ხუბულია

არასრულწლოვნის პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული გამოწვევები..... 62

ნინო ცაგარეიშვილი

პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები)..... 73

დავით ქანთარია

კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობა და პერსონალური მონაცემების დაცვა..... 86

ლუკა ფავლენიშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობა და კონტროლი 103

მარიამ მაიშმელაშვილი

პერსონალურ მონაცემთა დაცვა სამომხმარებლო ურთიერთობებში (საერთაშორისო და ეროვნული სტანდარტების მიმოხილვა)..... 117

ნორბერტ ბერნსდორფი

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი საქართველოში - მოკლე მიმოხილვა 127

მთავარი რედაქტორისაგან

ძვირფასო მკითხველო,

წარმოგიდგენთ „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ მესამე გამოცემას, რომელიც ეძღვნება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ამოქმედებას.

პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უმნიშვნელოვანესი კონსტიტუციური უფლების განმტკიცების, მონაცემთა დაცვის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოების, საქართველოს მიერ ნაკისრი საერთაშორისო ვალდებულებების შესრულების, აგრეთვე, საერთაშორისოდ აღიარებული პრინციპებისა და საუკეთესო პრაქტიკის დამკვიდრების მიზნით, მონაცემთა დაცვის საზედამხედველო ორგანოებს განსაკუთრებული როლი აკისრიათ. კანონმდებლობის აღსრულების თვალსაზრისით, არსებითი მნიშვნელობისაა მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანოს საქმიანობა საზედამხედველო პასუხისმგებლობისა და უფლებამოსილების ეფექტიანად განსახორციელებლად. საერთაშორისო საუკეთესო სტანდარტების იმპლემენტაციის პროცესში საგულისხმოა მონაცემთა დაცვის საზედამხედველო ორგანოთა შორის საერთაშორისო თანამშრომლობა. ამ კუთხით აღსანიშნავია „მონაცემთა დაცვის ევროპულ საბჭოსთან“ („EDPB“), „ევროპის მონაცემთა დაცვის ზედამხედველთან“ („EDPS“) და ევროპის ქვეყნების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან ჩვენი სამსახურის ურთიერთობა, რომლის ფარგლებშიც განვითარებული თანამშრომლობა და გაზიარებული საუკეთესო პრაქტიკა პერსონალურ მონაცემთა დაცვის ახალი კანონის იმპლემენტაციის პროცესში, ჩვენთვის უაღრესად მნიშვნელოვანი და ღირებულია.

წინამდებარე სამეცნიერო პუბლიკაციაც პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის სამართლის ქართველ თუ უცხოელ მეცნიერთა, პრაქტიკოსთა თანამშრომლობის ერთგვარი პლატფორმაა. იგი მკითხველს დარგის აქტუალურ საკითხებსა და საერთაშორისოსამართლებრივ ტენდენციებზე არაერთ საინტერესო სამეცნიერო ნაშრომს სთავაზობს. ჟურნალის მთავარი მისიაა, კვლევითი კომპონენტის გამოყენებით, ინფორმაციის დაცვასთან დაკავშირებულ აქტუალურ საკითხებზე შედარებითსამართლებრივი დისკურსის წარმართვა, რასაც ეროვნული საზედამხედველო ორგანოს განვითარებისა და საზოგადოების ცნობიერების ამაღლების ერთ-ერთ ხელშემწყობ ფაქტორად მივიჩნევთ.

ჟურნალის წინამდებარე გამოცემაში განხილულია პერსონალურ მონაცემთა დაცვის ძირითადი ტენდენციები და აქტუალური საკითხები — მონაცემთა საერთაშორისო გადაცემა, სინთეზური მონაცემები და ანონიმიზაციის კონცეფცია, ელექტრონული სანოტარო რეესტრი და მონაცემთა უსაფრთხოების სტანდარტი, არასრულწლოვანთა მონაცემთა დაცვა და სხვა. თითოეული ეს ნაშრომი ღირებული სამეცნიერო კონტრიბუციაა „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონით გათვალისწინებული სამართლებრივი ინსტიტუტების განმარტებისთვის. მაღლობას ვუხდით თითოეული სტატიის ავტორს, ჟურნალის წინამდებარე გამოცემაში მათ მიერ განხორციელებული სამეცნიერო წვლილისთვის და უაღრესად საინტერესო კვლევების გამოქვეყნებისათვის.

მსურს განსაკუთრებული მადლიერებით აღვნიშნო გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლის, მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორის, „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ სარედაქციო კოლეგიის წევრის — **დოქტორ ნორბერტ ბერნსდორფის** წვლილი ჟურნალის სამეცნიერო მხარდაჭერაში.

ამასთანავე, მადლიერებას გამოვთქვამ პირადი ცხოვრების ხელშეუხებლობის დარგის მკვლევრის — **დოქტორ ალექსანდრე ბოდუინისა** და ბოლონიის უნივერსიტეტის მკვლევრის — **ანდრეა ფ. ფერარისის** მიმართ ინოვაციური, აქტუალური სამეცნიერო ნაშრომის წარმოდგენისათვის.

სწრაფი ტექნოლოგიური პროგრესის გათვალისწინებით, ვფიქრობ, რომ ჟურნალის წინამდებარე გამოცემას კვლავ ფართო აუდიტორია ეყოლება და მასში გამოქვეყნებული შრომებით სამართალმცოდნეთა გარდა, პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის სამართლის მომიჯნავე დარგის წარმომადგენლებიც დაინტერესდებიან.

ლელა ჯანაშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის
ასოცირებული პროფესორი

ბარსელონის ავტონომიური უნივერსიტეტის ასოცირებული პროფესორი

ნორბერტ ბერნსდორფი*

პერსონალური მონაცემების გადაცემა მესამე სახელმწიფოებში - „უსაფრთხო ნავსადგომი“, „ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემა“ და „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩო“

ახალი შეთანხმება - „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის დამცავი სისტემა“ („Trans-Atlantic Data Privacy Shield Framework“) წარმოადგენს „ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემის“ („EU-US Privacy Shield“) შეთანხმების სამართალმემკვიდრეს. ევროკომისიის შესაბამისობის გადაწყვეტილება, რომელიც ამ უკანასკნელს ეფუძნებოდა, ევროკავშირის მართლმსაჯულების სასამართლოს („CJEU“) სენსაციური გადაწყვეტილებით („Schrems II“), 2020 წლის ივლისში გამოცხადდა ძალადაკარგულად. აღნიშნულს წინ უძღოდა შესაბამისობის გადაწყვეტილების კრიტიკა ლუქსემბურგის მოსამართლეების მხრიდან, რაც „უსაფრთხო ნავსადგომის“ სახელით ცნობილი შეთანხმებიდან გამომდინარეობდა. ორივე შემთხვევა შეეხებოდა აშშ-ს უსაფრთხოების სამსახურების ფართო უფლებამოსილებას ევროკავშირის მოქალაქეების პერსონალურ მონაცემებთან მიმართებაში. „CJEU“-მ დაადგინა, რომ აშშ-ში მონაცემთა დაცვის დონე არ შეესაბამებოდა ევროკავშირის სტანდარტებს.

საკვანძო სიტყვები: მონაცემთა კონფიდენციალობა, მონაცემთა დაცვა, მესამე სახელმწიფოებისათვის გადაცემა, „უსაფრთხო ნავსადგომის“ შეთანხმება, „ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემა“, „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩო“ შეთანხმება, „Facebook“, ევროკავშირის მართლმსაჯულების სასამართლო, პრეცედენტული სამართალი, მონაცემთა დაცვის ძირითადი რეგულაცია („GDPR“).

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, წინამდებარე ჟურნალის სარედაქციო კოლეგიის წევრი.

1. შესავალი

პერსონალური მონაცემები, შესაძლოა, გადაეცეს მესამე სახელმწიფოს მხოლოდ იმ შემთხვევაში, თუ გარანტირებულია „მონაცემთა დაცვის ძირითადი რეგულაციით“ („GDPR“)¹ დადგენილი სტანდარტი. მესამე სახელმწიფოებად იწოდებიან ქვეყნები, სადაც „GDPR“ არ გამოიყენება. იქიდან გამომდინარე, რომ „GDPR“ სავალდებულოა მხოლოდ ევროკავშირის („EU“) წევრი ქვეყნებისთვის, მესამე სახელმწიფოებად მოიხსენიება ევროკავშირის არაწევრი ქვეყნები. ევროპული ეკონომიკური ზონის („EEA“) ქვეყნები, მაგალითად, ისლანდია, ლიხტენშტეინი და ნორვეგია, ასევე, მიეკუთვნებიან მესამე სახელმწიფოების ჯგუფს, თუ ისინი თავად არ გადაწყვეტენ, შეუერთდნენ „GDPR“-ს. მონაცემთა გადაცემის სერიოზული პრობლემა არსებობს ამერიკის შეერთებულ შტატებში (აშშ), რადგან აშშ-ში მონაცემთა დაცვის ევროპის მსგავსი დონე არ არის უზრუნველყოფილი.

„ედვარდ სნოუდენის საქმისა“ და საიდუმლო სამსახურის მხრიდან მასობრივი თვალთვალის გამოვლენის გათვალისწინებით, აშშ-ში მონაცემთა დაცვის მიმართ ნდობა დაიკარგა. აშშ-ში შესაძლებელია, განხორციელდეს ევროკავშირის მოქალაქეების მონიტორინგი მაშინაც კი, როდესაც ისინი აგზავნიან შეტყობინებებს სოციალური ქსელის, „Facebook“-ის („Meta“) მეშვეობით.

მას შემდეგ, რაც მონაცემთა დაცვის შესახებ შეთანხმებები - „უსაფრთხო ნავსადგომი“ და „ევროკავშირი-აშშ-ის კონფიდენციალობის ჩარჩო“ - გააუქმა ევროკავშირის მართლმსაჯულების სასამართლომ, ევროკავშირი და აშშ უკვე მესამედ ცდილობენ მონაცემთა დაცვის ევროპული სტანდარტები შეუსაბამონ აშშ-ს სათვალთვალო პრაქტიკას.

2. ისტორია და მნიშვნელობა

მონაცემთა დაცვის ადრე მოქმედი დირექტივით (95/46/EC; DPD)² მართებულად იყო აღიარებული მონაცემთა ტრანსსასაზღვრო გადაადგილება, როგორც საერთაშორისო ვაჭრობის განვითარების აუცილებლობა. მონაცემთა ტრანსსასაზღვრო ნაკადი და, შესაბამისად, პერსონალური მონაცემების ტრანსსასაზღვრო გადაცემა, უდავოდ, ციფრული სამყაროს გამოწვევაა. თუმცა, მსოფლიოში არ არსებობს და არც შეიძლება არსებობდეს მონაცემთა დაცვის თანაბარი დონე ან თუნდაც მონაცემთა დაცვის თანაბარი კონცეფცია³.

მონაცემთა დაცვის დირექტივას ორი მთავარი დანიშნულება ჰქონდა: ერთი მხრივ, შეიქმნა მონაცემთა დაცვის ეროვნული კანონმდებლობის ჩარჩო ევროკავშირის მასშტაბით, რითაც განხორციელდა მონაცემთა დაცვის დონის ჰარმონიზაცია და ჩამოყალიბდა ერთგვარი ჩარჩო პირობები ევროკავშირის შიგნით პერსონალური მონაცემების შეუფერხებელი გადაცემისთვის, მეორე მხრივ კი, მონაცემთა დაცვის თვალსაზრისით, ევროკავშირი გაიმიჯნა სხვა ქვეყნებისაგან,

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, 1.

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31.

³ იხ.: Wuermeling U., Handelshemmnis Datenschutz - Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.

რამდენადაც ითვალისწინებდა პირობებს, რომლებითაც მონაცემების გადაცემა ევროკავშირის წევრ ქვეყნებთან ერთად, შესაძლებელი გახდა სხვა ქვეყნებშიც.

ზემოაღნიშნული მიდგომა გაზიარებულია “GDPR”-ის 44-ე - 50-ე მუხლებშიც, თუმცა, აღსანიშნავია, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ საგრძნობლად გასცდა ღირეუქტივის დებულებების სიღრმეს. “GDPR”, 1995 წლიდან მოყოლებული, ეხმიანება მონაცემთა დაცვის სფეროში განვითარებულ მოვლენებს. მნიშვნელოვანია ისიც, რომ, მიუხედავად ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიზნისა, დაიცვას პერსონალური მონაცემები, მან არ უნდა შეაფერხოს ეკონომიკური ზრდა.⁴ მესამე სახელმწიფოებთან მონაცემთა ტრანსსასაზღვრო გადაცემას გადამწყვეტი მნიშვნელობა აქვს ბიზნესისა და ვაჭრობისთვის, თუმცა, ამასთანავე, წარმოქმნის მონაცემთა დაცვის რისკებს.

3. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ სისტემა

პერსონალური მონაცემების მესამე სახელმწიფოსთვის გადაცემა რეგულირდება “GDPR”-ის 44-ე - 50-ე მუხლებით, რაც ქმნის მონაცემთა დაცვის ერთიან სტანდარტს ევროკავშირის ფარგლებში. იმავდროულად, აღნიშნული მესამე სახელმწიფოებში პერსონალური მონაცემების დამუშავების შეზღუდვების დაწესებით, განასხვავებს ევროკავშირს სხვა ქვეყნებისგან.

“GDPR”-ის 44-ე მუხლი ადგენს პერსონალური მონაცემების მესამე სახელმწიფოსთვის გადაცემის ზოგად პრინციპებს. 45-ე - 49-ე მუხლები ასახავს ამგვარი გადაცემის ლეგიტიმაციის სხვადასხვა მექანიზმს და დასაშვებობის კრიტერიუმებს, რომლებიც იურიდიულად ერთმანეთთან დაკავშირებული არ არის. 45-ე მუხლის თანახმად, მონაცემთა გადაცემის საფუძველია მონაცემთა დაცვის შესაბამისობის გადაწყვეტილება. პერსონალური მონაცემების ინდივიდუალური კონკრეტული გადაცემა ნებადართულია “GDPR”-ის 48-ე და 49-ე მუხლების საფუძველზე; 50-ე მუხლი კი შეეხება საერთაშორისო თანამშრომლობას პერსონალურ მონაცემთა დაცვის სფეროში.

პერსონალური მონაცემების მესამე სახელმწიფოსათვის გადაცემის დასაშვებობის შეფასება მოითხოვს ორეტაპიან შემოწმებას.⁵ რეგულაციის 44-ე მუხლი განმარტავს, რომ გარდა მეხუთე თავით დადგენილი წესებისა, გადაცემა შესაბამისობაში უნდა იყოს “GDPR”-ის სხვა დებულებებთანაც, მათ შორის, მე-6, მე-9 და მე-10 მუხლებთან.⁶ საწყის ეტაპზე, “GDPR”-ის მე-6, მე-9 და მე-10 მუხლებში ასახული ზოგადი აკრძალვისა და გამონაკლისების შესაბამისად, აუცილებელია, დადგინდეს, არსებობს თუ არა კანონიერი საფუძველი მონაცემთა გადაცემისთვის. მეორე ეტაპზე კი, აუცილებელია იმის შემოწმება, არის თუ არა დაცული “GDPR”-ის 44-ე და მომდევნო მუხლებით დადგენილი მოთხოვნები. მხოლოდ ამ პირობების

⁴ For more information see: *Rüpke G., von Lewinski K., Eckardt J. (eds.), Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung*, München 2018, § 18. On the requirements of a "European internal data market" *Brink St., Oetjen St., Schwartmann R., Voss K.*, So war die DSGVO nicht gemeint, *Frankfurter Allgemeine Zeitung (FAZ)* v. 17 July 2022.

⁵ Likewise: *Albrecht J. Ph., Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017, Part 6.

⁶ *Schantz P., Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017, 239.

დაკმაყოფილების შემთხვევაში არის ნებადართული პერსონალური მონაცემების მესამე სახელმწიფოსათვის გადაცემა. აღნიშნული ორსაფეხურიანი სტრუქტურა გამომდინარეობს “GDPR”-ის მიზნიდან და სისტემიდან. ის ქმნის მონაცემთა დაცვის სამართლებრივ ჩარჩო სტანდარტს ევროკავშირში. შესაბამისად, ტრანსსასაზღვრო დამუშავება, როგორც ასეთი, არ წარმოადგენს რისკს მონაცემთა სუბიექტისთვის. რისკი წარმოიქმნება მაშინ, როდესაც პერსონალური მონაცემები გადაეცემა მონაცემთა დამუშავებაზე პასუხისმგებელი ერთი პირიდან მეორეს. სწორედ “GDPR”-ის მე-6, მე-9 და მე-10 მუხლები ითვალისწინებს ზემოხსენებულ რისკს,⁷ დამატებით რისკს კი წარმოადგენს მონაცემთა გადაცემა ჰარმონიზებული საკანონმდებლო ბაზის ფარგლებს მიღმა.

მონაცემთა გადაცემა მესამე სახელმწიფოებს შორის დასაშვებია მხოლოდ იმ შემთხვევაში, თუ დაცული იქნება “GDPR”-ის წესები, მათ შორის, 44-ე და შემდგომი მუხლები.

4. ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტული სამართალი

პერსონალური მონაცემების აშშ-ში გადაცემა არაერთხელ იქნა გაკრიტიკებული ევროკავშირის მართლმსაჯულების სასამართლოს მიერ. თავდაპირველად, მან ძალადაკარგულად გამოაცხადა ევროკავშირისა და აშშ-ს „უსაფრთხო ნავსადგომის“ შეთანხმება, შემდეგ კი, „ევროკავშირი-აშშ-ის კონფიდენციალობის ფარის“ შეთანხმება და მასთან დაკავშირებული ევროკომისიის შესაბამისობის გადაწყვეტილებები.

ა. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება საქმეზე C-362/14, Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd, 2015 წლის 6 ოქტომბერი ("Schrems I")⁸

„ევროკომისიის უსაფრთხო ნავსადგომის პრინციპების შესახებ“ ევროკავშირის მართლმსაჯულების სასამართლოს 2015 წლის 6 ოქტომბრის გადაწყვეტილებით, რომელსაც უდიდესი მნიშვნელობა ჰქონდა, დადგინდა მონაცემთა დაცვის ადრე მოქმედი დირექტივის (DPD) ფუნდამენტური პრინციპები. მან, ასევე, მნიშვნელოვანი გავლენა იქონია “GDPR”-ის 44-ე - 50-ე მუხლების შინაარსის ჩამოყალიბებაზე.

საქმის ფაქტობრივი გარემოებები: შრემსი იყო ავსტრიის მოქალაქე, რომელმაც საჩივარი შეიტანა ირლანდიის მონაცემთა დაცვის საზედამხებელო ორგანოში იმის გამო, რომ მისი პერსონალური მონაცემები “Facebook”-ის ადგილობრივმა შვილობილმა კომპანიამ გადასცა “Facebook Inc.”-ს და აშშ-ში მდებარე სერვერებს, სადაც მუშავდებოდა ასეთი მონაცემები. იმ დროს, ევროკავშირის ტერიტორიაზე მცხოვრებ “Facebook”-ის ყველა მომხმარებელს რეგისტრაციისას უნდა გაეფორმებინა ხელშეკრულება “Facebook Ireland”-თან, რის გამოც, ევროკავშირის ტერიტორიაზე მცხოვრები “Facebook”-ის მომხმარებლების პერსონალური მონაცემები სრულად ან ნაწილობრივ გადაეცემოდა აშშ-ში მდებარე “Facebook Inc.”-

⁷ იხ.: Rüpe G., von Lewinski K., Eckardt J. (eds.), Datenschutzrecht- Grundlagen und europarechtliche Umgestaltung, München, 2018, § 18, 266.

⁸ ECLI:EU:C:2015:650.

ის სერვერებს. ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ საჩივარი მიიჩნია უსაფუძვლოდ, არ მიიღო და განმარტა, რომ მონაცემთა აშშ-სთვის გადაცემა ეფუძნებოდა 2000 წელს მიღებულ შესაბამისობის კომისიის გადაწყვეტილებას 2000/520/EC⁹ და იძლეოდა მონაცემთა გადაცემის ნებართვას ამერიკულ კომპანიებზე, რომლებიც აცხადებდნენ, რომ დაიცავდნენ ევროკავშირიდან მიღებულ პერსონალურ მონაცემებს და შეასრულებდნენ ე.წ. „უსაფრთხო ნავსადგომის“ პრინციპებს.

ამდენად, ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ მიიჩნია, რომ ვალდებული იყო, საჩივრის განხილვის გარეშე სრულად გაეზიარებინა ევროკომისიის შესაბამისობის გადაწყვეტილება, რის შემდეგაც შრემსმა გადაწყვეტილება სასამართლოში გაასაჩივრა.

ირლანდიის უმაღლესმა სასამართლომ შემოთქმა გამოხატა აშშ-ში მონაცემთა გადაცემის დასაშვებობასთან დაკავშირებით და საკითხი მოსაკვლევეად და წინასწარი განჩინების გამოსატანად გადასცა ევროკავშირის მართლმსაჯულების სასამართლოს, კომისიის გადაწყვეტილების იურიდიული ძალის განსაზღვრისა და მისი ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის¹⁰ მე-8 მუხლთან შესაბამისობის დადგენის მიზნით.

ირლანდიის უმაღლესი სასამართლო ევროკომისიის 2000/520/EC გადაწყვეტილების კანონიერების საკითხის განხილვისას „უსაფრთხო ნავსადგომის“ პრინციპებს არ შეხებია, თუმცა, მიუხედავად ამისა, „CJEU“-მ საბოლოოდ მაინც იმსჯელა აღნიშნულ საკითხზე, რადგან შრემსის საჩივარი ფაქტობრივად ეჭვქვეშ აყენებდა გადაწყვეტილების კანონიერებასაც. შედეგად, „CJEU“-მ გააფართოვა გადაწყვეტის ფარგლები.

„CJEU“-მ დაადგინა, რომ მონაცემთა დაცვის საზედამხედველო ორგანოებს, დირექტივის (DPD) მიხედვით, ევროკომისიის გადაწყვეტილებების დამოუკიდებლად გადახედვის უფლებამოსილება გააჩნიათ, მიუხედავად იმისა, რომ მხოლოდ „CJEU“-ს შეუძლია ევროკომისიის გადაწყვეტილებების ბათილად გამოცხადება. შესაბამისად, იმ შემთხვევაშიც კი, როდესაც პერსონალურ მონაცემთა გადაცემის საფუძველია კომისიის გადაწყვეტილება შესაბამისობაზე, ეროვნულ საზედამხედველო ორგანოში საჩივრის შეტანისას, უწყება ვალდებულია, გულმოდგინედ განიხილოს მოთხოვნა.

ევროკავშირის მართლმსაჯულების სასამართლომ სიტყვასიტყვით განაცხადა:

„კანონმდებლობა, რომელიც საჯარო ხელისუფლებას აძლევს ელექტრონულ კომუნიკაციებზე ფართო წვდომის საშუალებას, ძირს უთხრის პირადი ცხოვრების ხელშეუხებლობის ფუნდამენტურ უფლებას, რომელიც დაცულია ქარტიის მე-7 მუხლით (იხ.: გადაწყვეტილება *Digital Rights Ireland and Others*, C-293/12 და C-594/12, ECLI:EU:C:2014:238, § 39).

ანალოგიურად, კანონმდებლობა, რომელიც არ ითვალისწინებს ინდივიდის შესაძლებლობას, გამოიყენოს სამართლებრივი დაცვის საშუალებები, რათა ჰქონდეს წვდომის, შესწორების და წაშლის უფლება პირადად მასთან დაკავშირებულ პერსონალურ მონაცემებზე, არღვევს ქარტიის 47-ე მუხლის საფუძველზე ეფექტიანი სასამართლოს უფლების არსს. ქარტიის 47-ე მუხლის პირველი პუნქტით დადგენილია, რომ ევროკავშირის კანონმდებლობით გარანტირებული უფლებებისა და

⁹ Decision 2000/520/EC of the European Commission of 26 July 2000.

¹⁰ Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.

თავისუფლებების დარღვევის შემთხვევაში, პირს სამართლებრივი დაცვის ეფექტიანი საშუალების მოთხოვნის უფლება აქვს, ამ მუხლით გათვალისწინებული პირობების დაცვით. ეფექტიანი სასამართლო განხილვის შესაძლებლობა უზრუნველყოფს ევროკავშირის კანონმდებლობის დაცვას, რაც აუცილებელია კანონის უზენაესობისთვის. (...).“

მართლმსაჯულების ევროპულმა სასამართლომ, თავისი გადაწყვეტილებით, არამხოლოდ ძალადაკარგულად ცნო ევროკავშირისა და აშშ-ს შორის „უსაფრთხო ნავსადგომის“ შეთანხმება, არამედ დაადგინა მონაცემთა დაცვის დონის შესაბამისობის შეფასების კრიტერიუმები.¹¹ აღნიშნულმა გავლენა იქონია ძალადაკარგული შეთანხმების სამართალმემკვიდრეზეც - "ევროკავშირი-აშშ-ის კონფიდენციალობის ფარი"-ზე რომელიც მოექცა გაძლიერებული კონტროლის ქვეშ მონაცემთა დაცვის კანონმდებლობისა და შესაბამისი პოლიტიკის თვალსაზრისით.

ბ. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება საქმეზე C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, 16 July 2020 ("Schrems II")¹²

აშშ-ში მონაცემთა მიმოცვლის მნიშვნელობის ხაზგასასმელად, 2016 წლის 12 ივლისს "EU-US Privacy Shield" - შეთანხმება იქნა მიღწეული, რომელიც „უსაფრთხო ნავსადგომის“ სამართალმემკვიდრედ მიიჩნევა. შეთანხმება ევროკომისიის შესაბამისობის გადაწყვეტილებას 2016/1250 დაეფუძნა,¹³ რომლის მიხედვით, ორგანიზაციები, რომლებმაც ნებაყოფლობით აიღეს "EU-US Privacy Shield" მექანიზმის იმპლემენტაციის ვალდებულება, პასუხისმგებელნი არიან, უზრუნველყონ მონაცემთა დაცვის შესაბამისი დონე.

„ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარი“ აღრინდელი „უსაფრთხო ნავსადგომის“ შეთანხმების მსგავსი იყო. ამერიკულმა კომპანიებმა აშშ-ს ვაჭრობის დეპარტამენტის წინაშე ნებაყოფლობით აიღეს ვალდებულება, ევროკავშირიდან გადაცემული მონაცემები მხოლოდ დადგენილი პრინციპების შესაბამისად დაემუშავებინათ, რათა შენარჩუნებულიყო ევროკავშირის მონაცემთა დაცვის დონე. ფედერალური სავაჭრო კომისია და აშშ-ის სატრანსპორტო დეპარტამენტი ზედამხედველობას უწევდნენ ვალდებულებების შესრულებას „ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარის“ ფარგლებში. ვაჭრობის დეპარტამენტი უმთავრესად პასუხისმგებელი იყო ნებაყოფლობითი ვალდებულების შესრულების მონიტორინგზე, ხოლო ფედერალურ სავაჭრო კომისიას შეეძლო ორგანიზაციების დაჯარიმება. თუმცა, თავიდანვე არსებობდა ეჭვი იმის თაობაზე, თუ რამდენად ეფექტიანად შეძლებდა აშშ-ს ხელისუფლება მონაცემთა დაცვის ზედამხედველობასა და აღსრულებას.

საქმის ფაქტობრივი გარემოებები: „უსაფრთხო ნავსადგომის“ საქმეში, მოქალაქე შრემსმა საჩივარი შეიტანა ირლანდიის მონაცემთა დაცვის ორგანოში, იგი მიუთითებდა, რომ "Facebook Ireland" გადასცემდა მის პერსონალურ მონაცემებს აშშ-ს. ირლანდიის სასამართლომ ევროკავშირის მართლმსაჯულების სასამართლოს მიმართა ხელშეკრულების სტანდარტული პირობებისა და „ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარი“-ს შესაბამისობის დასადგენად ევროკავშირის

¹¹ Likewise *Kühling J., Heberlein J.*, EuGH "reloaded": "unsafe harbour" USA vs. "Datenfestung" EU, *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* 2016, 7,9.

¹² ECLI:EU:C:2020:559.

¹³ Decision (EU) 2016/1250 of the European Commission of 12 July 2016.

მონაცემთა დაცვის სტანდარტებთან. “CJEU“-მ დაადგინა, რომ „ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარი“ არ იყო დამაკმაყოფილებელი ევროკავშირის სტანდარტებთან მიმართებით. გარდა ამისა, ფიზიკური პირებისთვის ხელმისაწვდომი სამართლებრივი დაცვა, როგორიცაა ეფექტიანი სამართლებრივი დაცვის უფლება, არასაკმარისად იქნა მიჩნეული.

ამ მოვლენების შემდეგ მნიშვნელოვანი საკითხი იყო აშშ-ს ხელისუფლების შესაძლებლობა, მიეღო წვდომა ევროკავშირიდან გადაცემულ მონაცემებზე და შეზღუდული სამართლებრივი საშუალებები, რომლებიც ხელმისაწვდომი იყო ამგვარი წვდომის გასაჩივრების მიზნით. აღნიშნულის გამო “CJEU“-მ მიიღო გადაწყვეტილება „უსაფრთხო ნავსადგომის“ მექანიზმის ბათილად ცნობის შესახებ.

“CJEU“-მ განმარტა:

„აშშ-ს კანონმდებლობით პერსონალური მონაცემების დაცვის შეზღუდვები, განსაკუთრებით აშშ-ს საჯარო ხელისუფლების მიერ ევროკავშირის მიერ გადაცემული მონაცემების ხელმისაწვდომობასა და გამოყენებასთან დაკავშირებით, არ აკმაყოფილებს ევროკავშირის კანონმდებლობით დადგენილ მოთხოვნებს, როგორც მითითებულია ევროკავშირის ძირითად უფლებათა ქარტიის 52(1) მუხლის მეორე წინადადებაში. კანონმდებლობა, რომელიც ფიზიკურ პირს არ აძლევს სამართლებრივი დაცვის საშუალებათა გამოყენების შესაძლებლობას - ჰქონდეს ხელმისაწვდომობა მის შესახებ არსებულ პერსონალურ მონაცემებზე, ან მოითხოვოს ასეთი მონაცემების შესწორება ან წაშლა - არ შეესაბამება ეფექტიანი სამართლებრივი დაცვის ფუნდამენტურ უფლებას (ქარტიის 47-ე მუხლი).“ ამრიგად, „უსაფრთხო ნავსადგომის გადაწყვეტილებით“, აშშ ვერ დაიცავდა ფუნდამენტურ უფლებებს იმ დონეზე, რომელიც გარანტირებულია ევროკავშირის ღირებულებით, ქარტიასთან ერთობლიობაში. შესაბამისად, “CJEU“-მ გადაწყვეტილება გამოაცხადა ძალადაკარგულად“.

რა როლს ასრულებენ ევროკომისია და მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანოები მესამე ქვეყნებისთვის მონაცემთა გადაცემისას?

ევროკომისიას არ მოეთხოვება მესამე ქვეყნებში მონაცემთა დაცვის დონის შეფასება, სტანდარტულ სახელმწიფოებო პუნქტების მიღებისას. ევროკავშირის მართლმსაჯულების სასამართლო ხაზს უსვამს, რომ მონაცემთა გამცემის (ექსპორტიორის) პასუხისმგებლობაა მესამე ქვეყანაში მონაცემთა დაცვის დონის შეფასება თითოეული გადაცემისთვის. მონაცემთა გამცემმა ასევე უნდა უზრუნველყოს ადეკვატური დაცვა შესაბამისი გარანტიებით, რომელიც შეიძლება მოიცავდეს დამატებით ზომებს ხელშეკრულების სტანდარტული პირობების მიღმა.

თუ მონაცემთა დაცვა ვერ იქნება უზრუნველყოფილი დამატებითი ზომებითაც კი, მონაცემთა გამცემმა უნდა შეაჩეროს ან შეწყვიტოს მონაცემთა გადაცემის პროცესი.

მონაცემთა დაცვის ეროვნულ საზედამხედველო ორგანოებს აქვთ ძალიან მნიშვნელოვანი როლი დაცვის გარანტიების ზედამხედველობის კუთხით, როგორიცაა ხელშეკრულების სტანდარტული პირობები. ორგანოებმა უნდა გადახედონ ამ გარანტიებს, განსაკუთრებით მაშინ, როდესაც საჩივარი ეჭვქვეშ აყენებს ევროკომისიის შესაბამისობის გადაწყვეტილების ეფექტიანობას მონაცემთა გადაცემასთან მიმართებით

“GDPR“-ის 58-ე მუხლის თანახმად, ეროვნულმა საზედამხედველო ორგანოებმა უნდა აკრძალონ ან შეაჩერონ მონაცემთა გადაცემა, თუ არ არსებობს ევროკომისიის

მოქმედი შესაბამისობის გადაწყვეტილება, ან ადეკვატური გარანტია ან/და დამატებითი ზომები საკმარისად არ უზრუნველყოფს მესამე ქვეყანაში გადაცემული მონაცემების დაცვას.

მესამე ქვეყნისთვის მონაცემთა გადაცემისას მონაცემთა დაცვის დონის შეფასების მიზნით საზედამხედველო ორგანოებმა უნდა იხელმძღვანელონ ევროკომისიის შესაბამისობის გადაწყვეტილებებით, როდესაც ეს უკანასკნელი ძალაშია.

5. ახალი „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩო“ შეთანხმება

ევროკავშირის მართლმსაჯულების სასამართლოს 2020 წლის 16 ივლისის გადაწყვეტილების შემდეგ („შრემს II“), ევროკავშირის კომისია და აშშ კვლავ ცდილობდნენ შეემუშავებინათ მონაცემთა დაცვის შესახებ ახალი შეთანხმება. ახალი შესაბამისობის გადაწყვეტილების მიზანია ამერიკულ ორგანიზაციებში პერსონალური მონაცემების უსაფრთხო გადაცემის უზრუნველყოფა.

ა. მომზადების პროცესი

2022 წლის 25 მარტს აშშ-ს პრეზიდენტმა ბაიდენმა და ევროკომისიის პრეზიდენტმა ფონ დერ ლაიენმა გამოაცხადეს შეთანხმება „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ფარის ჩარჩოზე“. ამ შეთანხმების დეტალები სხვა წყაროებთან ერთად გაზიარებული იყო აშშ-ს მთავრობის პრესრელიზში.¹⁴

აღნიშნული იწვევს შემდეგს:¹⁵

„ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარის“ - შეთანხმების ომბუდსმენის ნაცვლად, „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ფარი“ - შეთანხმება არის კვაზი-სასამართლო, ორსაფეხურიანი ორგანო, რომელიც ევროკავშირის მასშტაბით მონაცემთა სუბიექტების საჩივრებს განიხილავს. ორგანო უფლებამოსილია, შექმნას სამართლებრივი დაცვის საშუალებები. მიუხედავად იმისა, რომ ის არ უნდა იყოს სასამართლო სისტემის ნაწილი, უნდა იყოს დამოუკიდებელი და აშშ-ს მთავრობის წევრებით არ დაკომპლექტდეს.

გარდა ამისა, ახალი ზომები მტკიცდება აშშ-ს უსაფრთხოების ორგანოებში, რათა შემცირდეს თვალთვალი პროპორციულ დონეზე და განხორციელდეს კონსტიტუციური სტანდარტები, თუმცა დეტალები ჯერ კიდევ უცნობია. ცვლილებები არ განხორციელდება კონგრესის მიერ მიღებული კანონით, არამედ აშშ-ს პრეზიდენტის მიერ გამოცემული ახალი ადმინისტრაციული წესით (აღმასრულებელი ბრძანება).

¹⁴ For more information see: <<https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-shield-framework.pdf>> [10.05.2024]. Also *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html>> [10.05.2024].

¹⁵ *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission, <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html>> [10.05.2024] Also: *Glocker F.*, Politische Lösung für Datentransfer in die USA zeichnet sich ab <<https://www.cmshs-bloggt.de/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html>> [10.05.2024].

„Trans-Atlantic Data Privacy Shield Framework“ ეფუძნება წინა „EU-US Privacy Shield“ მექანიზმს. ამერიკული კომპანიებისთვის მოთხოვნები უცვლელი დარჩება და არსებული სერტიფიკატები კვლავ ძალაში დარჩება, ხოლო ტერმინი „კონფიდენციალურობის ფარი“ კვლავ იქნება გამოყენებული სერტიფიცირების მიზნებისთვის. აღსანიშნავია, რომ აშშ-ს მთავრობამ „კონფიდენციალურობის ფარის“ სერტიფიკატი 2020 წლის 16 ივლისის ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილების შემდეგაც კი შეინარჩუნა.¹⁶

„Trans-Atlantic Data Privacy Shield Framework“ - შეთანხმება შეიცავს გარკვეულ პრინციპებს ამერიკული კომპანიების თვითსერტიფიკაციისთვის, რომლებიც ეფუძნება მონაცემთა დაცვის ევროპულ კანონს. აღნიშნული პრინციპები განიხილება, როგორც „GDPR“-ის გამარტივებულ ვერსიას¹⁷. თვითსერტიფიკაცია გულისხმობს სარეგისტრაციო მოსაკრებლის გადახდის გზით ამერიკული კომპანიის დარეგისტრირებას კომერციის დეპარტამენტის ვებგვერდზე. აღნიშნული ვებგვერდი ხელმისაწვდომია 2023 წლის 17 ივლისიდან.¹⁸ აქედან მოყოლებული, დაახლოებით 2600 ამერიკული კომპანია, რომელიც ადრე იყო სერტიფიცირებული „კონფიდენციალურობის ფარის“ ფარგლებში, ავტომატურად იქნება აღიარებული სერტიფიცირებულად „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ჩარჩოს“ მიხედვით. მათ შორისაა: აშშ-ს ძირითადი „Cloud Provider“ - SaaS და IT სერვისის მიმწოდებლები.

ბ. ე.წ. ევროკომისიის აღმასრულებელი ბრძანება და შესაბამისობის გადაწყვეტილება

2023 წლის 10 ივლისს ევროკავშირის კომისიამ მიიღო „Trans-Atlantic Data Privacy Shield Framework“ - შეთანხმება და შესაბამისობის გადაწყვეტილება¹⁹. აშშ-ის მთავრობამ ასევე გამოაქვეყნა აშშ-ის პრეზიდენტის ე.წ. აღმასრულებელი ბრძანება. იმ შემთხვევაში თუ აშშ-ს კომპანიები გაივლიან თვითსერტიფიკაციას ახალი მექანიზმით, ივარაუდება, რომ უზრუნველყოფილია მონაცემთა დაცვის შესაბამისი სტანდარტი.²⁰

6. დასკვნა - "Schrems III"?

„Trans-Atlantic Data Privacy Shield Framework“- შეთანხმებას აქვს გადამწყვეტი უპირატესობა: ის სამართლებრივ უსაფრთხოებას უზრუნველყოფს. ევროკომისიის ახალი შესაბამისობის გადაწყვეტილება ავალდებულებს მონაცემთა დაცვის

¹⁶ For more information see: <<https://www.privacyshield.gov/article?id=EU-US-Privacy-Shield-Programm.html>> [10.05.2024].

¹⁷ Thus expressly *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html>> [10.05.2024].

¹⁸ The website can be found at <<https://www.dataprivacyframework.gov/s.html>> [10.05.2024].

¹⁹ Decision (EU) 2023/4745 of the European Commission of 10 July 2023.

²⁰ On this in detail *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <<https://www.cmshs-bloggt.de/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html>> [10.05.2024].

საზედამხედველო ორგანოებს, დაუშვან მონაცემთა გადაცემა თვითსერტიფიცირებულ ამერიკულ კომპანიებზე.

ასევე ეფექტურად გამარტივებულია გადაცემა არათვითსერტიფიცირებულ ამერიკულ კომპანიებზე. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა გააგრძელონ ხელშეკრულების სტანდარტული პირობების შეთანხმება არათვითსერტიფიცირებულ კომპანიებთან. ასეთ შემთხვევებში, მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანოები ფაქტობრივად ვალდებული იქნებიან, შეამოწმონ მესამე ქვეყნის კანონმდებლობის შესაბამისობა მონაცემთა დაცვის ევროპულ სტანდარტებთან (ე.წ. გადაცემის ზემოქმედების შეფასება). იმის ნაცვლად, რომ განახორციელონ შეფასება, მხარეებს შეუძლიათ დაეყრდნონ გადაწყვეტილებას, არსებულ შეფასებას.²¹

არსებობს ეჭვი, „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ჩარჩო“ შეთანხმება და ევროკომისიის შესაბამისობის გადაწყვეტილება რამდენად აკმაყოფილებს ევროკავშირის მართლმსაჯულების სასამართლოს მოთხოვნებს:

დამოუკიდებელი, კვაზი-სასამართლო ორგანოს შექმნა, რომელიც განიხილავს საჩივრებს მართლაც ეფექტიანი გამოსავალია და შესაძლოა აკმაყოფილებდეს სასამართლოს მოთხოვნებს სასამართლო დაცვის შესახებ. თუმცა, გაურკვეველია, დააკმაყოფილებს თუ არა აშშ-ს პრეზიდენტის აღმასრულებელი ბრძანების ფართო პირობები, რომელიც არეგულირებს აშშ-ს უსაფრთხოების სააგენტოების ფართო თვალთვალს, სასამართლოს მოთხოვნას მკაფიო და ზუსტი წესების შესახებ ასეთი ზომების მოცულობისა და გამოყენების შესახებ. გარდა ამისა, გამოქვეყნებული დოკუმენტები არ განმარტავს, თუ როგორ შემოიფარგლება აშშ-ს სააგენტოების თვალთვალის მხოლოდ იმით, რაც არის „აბსოლუტურად აუცილებელი“, როგორც ამას მოითხოვს „CJEU“.

„Trans-Atlantic Data Privacy Shield Framework“- შეთანხმების ბედი კიდევ ერთხელ შეიძლება გადაწყვიტოს „CJEU“-მ. სამოქალაქო უფლებების დამცველმა ორგანიზაციებმა, როგორიცაა „NOYB“²² - ციფრული უფლებების ევროპული ცენტრი, რომელსაც ხელმძღვანელობს მაქსიმილიან შრემსი, უკვე განაცხადეს თავიანთი პოზიცია ევროკომისიის ახალი შესაბამისობის გადაწყვეტილების წინააღმდეგ. მსგავსი ინიციატივა გამოთქვა ფრანგმა ევროპარლამენტარმა ლატომბემ. თუმცა, ნაკლებად სავარაუდოა, რომ „CJEU“ ამ საკითხზე მალე იმსჯელებს.²³

შენიშვნა: პერსონალური მონაცემების სხვა მესამე ქვეყნებში გადაცემისთვის, რომელთა შესახებაც არ არსებობს ევროკომისიის შესაბამისობის გადაწყვეტილება, მართლმსაჯულების სასამართლოს 2020 წლის 16 ივლისის გადაწყვეტილება რჩება ძალაში.²⁴

²¹ *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-dereu-kommission.html>> [10.05.2024].

²² „None Of Your Business“.

²³ See *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210, 213.

²⁴ *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210, 214; *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html>> [10.05.2024]; also *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html>> [10.05.2024].

ბიბლიოგრაფია:

1. Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.
2. 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, 1.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31.
4. Decision 2000/520/EC of the European Commission of 26 July 2000.
5. Decision (EU) 2016/1250 of the European Commission of 12 July 2016.
6. Decision (EU) 2023/4745 of the European Commission of 10 July 2023.
7. *Albrecht J. Ph., Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017.
8. *Bernsdorff N.*, „EU-US Data Privacy Shield Framework“ und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210.
9. *Eichenhofer E.*, „e-Privacy“ im europäischen Grundrechtsschutz: Das „Schrems“-Urteil des EuGH, Europarecht (EuR) 2016, 76.
10. *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <www.cmshs-bloggt.de> [10.05.2024].
11. *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <<https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html>> [10.05.2024].
12. *Kühling J., Heberlein J.*, EuGH „reloaded“: „unsafe harbor“ USA vs. „Datenfestung“ EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7.
13. *von Lewinski K.*, Privacy Shield – Notdeich nach dem Pearl Harbor für den transatlantischen Datenverkehr, Europarecht (EuR) 2016, 405.
14. *Rüpke G., von Lewinski K., Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, Munich, 2018.
15. *Schantz P., Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017.
16. *Schreiber G., Kohm W.*, Rechtssicherer Datenschutz unter dem EU-US Privacy Shield? – Der transatlantische Datenverkehr in der Unternehmenspraxis, Zeitschrift für Datenschutz (ZD) 2016, 255.
17. *Schwartmann R.*, Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2016, 864.
18. *Weichert Th.*, EU-US Privacy Shield – Ist der transatlantische Datenverkehr nun grundrechtskonform?, Zeitschrift für Datenschutz (ZD) 2016, 209.
19. *Wuermeling U.*, Handelshemmnis Datenschutz – Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.
20. CJEU, Case C-362/14, *Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd.* („Schrems I“; 2015).
21. CJEU, Case C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd., Maximillian Schrems* („Schrems II“; 2020).

ალექსანდრე ბოდუინი*

ანდრეა ფ. ფერარისი**

სინთეზური მონაცემების, როგორც ანონიმიზაციის სტრატეგიის სამართლებრივი და მარეგულირებელი პერსპექტივები

მზარდ ციფრულ სამყაროში პერსონალური მონაცემების დაცვა უმნიშვნელოვანესია, როგორც ფიზიკური და იურიდიული პირებისთვის, ისე მარეგულირებელი ორგანოებისთვის. მონაცემთა შეგროვების ტექნოლოგიების განვითარებასთან ერთად, ასევე, უნდა გაუმჯობესდეს მონაცემთა კონფიდენციალობის უზრუნველყოფის მეთოდები. წინამდებარე ნაშრომი იკვლევს სინთეზურ მონაცემებს, როგორც პერსპექტივას კონფიდენციალობის გამაძლიერებელი ტექნოლოგიის (“PET”) ანონიმიზაციის მიზნით. ნაშრომი ფოკუსირებულია იურიდიულ, თეორიულ და პრაქტიკულ ასპექტებზე, სადაც განხილულია მარეგულირებლის კონტექსტი, განსაკუთრებით “GDPR”-ის მიხედვით, და განსაზღვრულია კონფიდენციალობის რისკები და გამოწვევები, რომლებიც ანონიმიზაციით უნდა იყოს დაცული. ჩვენ ვამტკიცებთ, რომ სინთეზურ მონაცემებს, როდესაც ისინი სათანადოდ გენერირებულია, შეუძლიათ დააკმაყოფილონ ანონიმიზაციის სტანდარტები და უზრუნველყონ განლაგების რეკომენდაციები კონფიდენციალობის რისკების შესამცირებლად. ჩვენი დასკვნები ხელს უწყობს მონაცემთა სინთეზური კონფიდენციალობის უზრუნველყოფის სტანდარტიზებულ ჩარჩოს, რომელიც შეესაბამება მონაცემთა დაცვის მიმდინარე და მომავალ რეგულაციას.

საკვანძო სიტყვები: სინთეზური მონაცემი, ანონიმიზაცია, კონფიდენციალობის გამაძლიერებელი ტექნოლოგია, “GDPR”.

* სამართლის დოქტორი; “Aindo SpA”-ში პირადი ცხოვრების ხელშეუხებლობის დარგის მკვლევარი.

** ბოლონიის უნივერსიტეტის დოქტორანტი და “Data Valley Consulting srl”-ში სამართლის, მეცნიერებისა და ტექნოლოგიების მკვლევარ-სპეციალისტი.

1. შესავალი

მუდმივად განვითარებად ციფრულ სამყაროში პერსონალური მონაცემების დაცვა სულ უფრო და უფრო დიდ გამოწვევას წარმოადგენს, როგორც ინდივიდების, ისე ორგანიზაციებისა და მარეგულირებელი ორგანოებისთვის. მონაცემთა შეგროვების და დამუშავების ტექნოლოგიების მუდმივად განვითარების პირობებში, აუცილებელია, ასევე, გაუმჯობესდეს პერსონალური ინფორმაციის დაცვის საშუალებები.

ერთ-ერთი ასეთი საშუალებას წარმოადგენს ანონიმიზაცია, რომელიც მიზნად ისახავს მონაცემის იმგვარ გარდაქმნას, რომლის შედეგადაც შეუძლებელი გახდება მონაცემთა სუბიექტის იდენტიფიცირება. ანონიმიზაციის მექანიზმი აუცილებელია ევროკავშირის მონაცემთა დაცვის ძირითად რეგულაციასთან (“GDPR”) შესაბამისობის უზრუნველსაყოფად, იგი, ასევე, იცავს სუბიექტთა კონფიდენციალობას მათი მონაცემების ბოროტად გამოყენების შემთხვევაში.

წინამდებარე ნაშრომი იკვლევს სინთეზურ მონაცემს, როგორც კონფიდენციალობის გამაძლიერებელ ტექნოლოგიას (“PET”)¹, უფრო კონკრეტულად ნაშრომი განიხილავს ანონიმიზაციას იურიდიული და თეორიული თვალსაზრისით.

სინთეზური მონაცემები არ გროვდება ემპირიულად, არამედ გენერირდება ალგორითმების მეშვეობით. ამასთან, ისინი არ არის დაკავშირებული კონკრეტულ პირთან, მაგრამ, შესაძლოა, სასარგებლო იყოს მონაცემთა შესახებ მეცნიერებისა და ხელოვნური ინტელექტის (“AI”) განვითარებისთვის. ტექნოლოგიებთან და კონფიდენციალობის კონცეფციასთან დაკავშირებულ ნაშრომში მოცემული პერსპექტივები და ინტერპრეტაციები უზრუნველყოფს სინთეზური მონაცემების კონფიდენციალობის სტანდარტიზებული და მყარი ჩარჩოს შექმნას.

ნაშრომი სტრუქტურირებულია შემდეგნაირად: მეორე თავში განხილულია ანონიმიზაციის საკანონმდებლო განმარტება “GDPR”-ის შესაბამისად. უფრო კონკრეტულად, მოცემულია პერსონალური მონაცემის, ანონიმიზებული მონაცემის შესახებ ანალიზი, ასევე, განხილულია ანონიმიზაციის მოთხოვნები, მათ შორის, შესაძლო თავდასხმის ტიპები. მესამე თავში, განხილულია იურიდიული თეორია იმის საჩვენებლად, რომ შესაბამისი ტექნოლოგიების სწორი გამოყენების პირობებში, რეალური მონაცემებისაგან სინთეზური მონაცემების შექმნა გენერირებადი ხელოვნური ინტელექტის მეშვეობით შეიძლება იყოს ანონიმიზაციის ერთ-ერთი საშუალება. ნაშრომის მეოთხე თავში ჩვენ ვიყენებთ შემუშავებულ კონცეფციებს, რათა გავცეთ რეკომენდაციები სინთეზური მონაცემების სწორი გამოყენების შესახებ კონფიდენციალობასთან დაკავშირებულ პოტენციურ საფრთხეებსა და ღია კვლევებზე დაყრდნობით.

2. ანონიმიზაციის კონცეფცია

აღნიშნულ თავში მოცემულია ანონიმიზაციის კონცეფცია, როგორც ეს აღწერილია წინა ნაშრომში². ანონიმიზაცია არის პერსონალური მონაცემების

¹ OECD, “Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches,” OECD Digital Economy Papers (OECD, 2023).

² Panfilo D., Boudewijn A. T., Ferraris A. F., Cocca V., Zinutti S., De Schepper K., & Chauvenet C. R., Measuring Privacy Protection in Structured Synthetic Datasets: A Survey, in: Hideyuki Matsumi, Paul De Hert et al. (ed), Privacy and Data Protection: Ideas that Drive Our Digital World, 2024.

ტრანსფორმაციის პროცესი, რომლის შედეგადაც, მონაცემთა ბაზაში პირდაპირ თუ ირიბად შეუძლებელია ფიზიკური პირის იდენტიფიცირება. აღნიშნული ტექნიკა წარმოადგენს კონფიდენციალობის დაცვის აუცილებელ წინაპირობას მონაცემებზე ორიენტირებულ (“data-centric”) სამყაროში, ამასთან, იგი შესაბამისობაშია “GDPR”-თან. იდენტიფიცირებადი ელემენტების ეფექტურად წაშლით ან შეცვლით, ანონიმიზაცია პერსონალურ ინფორმაციას იცავს არაავტორიზებული წვდომისა და არასათანადო გამოყენებისგან, ამავე დროს იძლევა მონაცემთა ანალიზისა და შემდგომი გამოყენების საშუალებას. მონაცემთა ანონიმიზაციის სხვადასხვა მიდგომების შესწავლამდე, მნიშვნელოვანია, პირველ რიგში, გავანალიზოთ პერსონალური მონაცემების მახასიათებლები, “GDPR”-ის შესაბამისად.

2.1. პერსონალური მონაცემი

ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”)³ პერსონალურ მონაცემს განმარტავს, როგორც „ნებისმიერ ინფორმაციას, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს („მონაცემთა სუბიექტს“) უკავშირდება. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, ადგილმდებარეობით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით“.

აღნიშნული განმარტება მოიცავს ოთხ მნიშვნელოვან ელემენტს, როგორც ეს მოცემულია ლოპეზის და ელბის⁴ ანალიზში:

1. „ნებისმიერი ინფორმაცია“: ეს ტერმინი ყოვლისმომცველია, მოიცავს ყველა სახის ინფორმაციას პიროვნების შესახებ, განურჩევლად მისი ბუნებისა (ობიექტური თუ სუბიექტური) ან იმ კონტექსტისა, რომელშიც ადამიანი მოქმედებს (მაგ., როგორც მომხმარებელი, პაციენტი, თანამშრომელი). ის მოიცავს ფართო სპექტრს, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს, ასევე, ზოგად ინფორმაციას პირადი, ოჯახის ან პროფესიული ცხოვრების შესახებ.
2. „უკავშირდება“: ინფორმაცია პიროვნებას უკავშირდება სამ გზით: მისი შინაარსით (კონკრეტული მონაცემები ინდივიდის შესახებ, როგორიცაა: სამედიცინო ჩანაწერები), მიზნით (თუ გამოიყენება ინდივიდის სტატუსის ან ქცევის შესაფასებლად ან გავლენას ახდენს მასზე) და შედეგით (თუ მისი გამოყენება გავლენას ახდენს ინდივიდის უფლებებსა და ინტერესებზე).
3. „იდენტიფიცირებული ან იდენტიფიცირებადი“: აღნიშნული ფოკუსირდება ჯგუფში პიროვნების გარჩევის უნარზე სხვადასხვა იდენტიფიკატორის საშუალებით, რომლებიც შეიძლება იყოს პირდაპირი (მაგ.: სახელი) ან არაპირდაპირი (მაგ.: ინფორმაციის უნიკალური კომბინაცია). კანონმდებლობა ვრცელდება ნებისმიერ პერსონალურ მონაცემზე, იდენტიფიკაციის მეთოდის მიუხედავად.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), (GDPR) art. 4.1.

⁴ López C.A.F., Elbi A., On The Legal Nature of Synthetic Data, NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research, 2022.

4. „ფიზიკური პირი“: კანონმდებლობა ვრცელდება და იცავს მოიცავს ყველა ადამიანს, რომელთა იდენტიფიცირება შესაძლებელია.

აღნიშნული კომპონენტები ერთობლივად უზრუნველყოფენ მონაცემთა დაცვისათვის საჭირო თანმიმდევრულ და ყოვლისმომცველ მიდგომებს. ამასთან, ეს კომპონენტები აბალანსებს პერსონალური მონაცემების ფართო ასპექტს, მათ შორის, ინდივიდის იდენტიფიცირების ხარისხს.

2.2. ანონიმიზაცია და ანონიმიზებული მონაცემი

ანონიმიზებული მონაცემი გულისხმობს ინფორმაციას, რომელიც არ შეიცავს პირის იდენტიფიცირების ელემენტებს, რაც უზრუნველყოფს, რომ პიროვნების ამოცნობა შეუძლებელია პირდაპირ ან მესამე პირებისთვის ხელმისაწვდომი დამხმარე მონაცემების საშუალებით. ანონიმიზებულ მონაცემზე არ ვრცელდება „GDPR“, გამომდინარე იქიდან, რომ არ წარმოადგენს პერსონალურ მონაცემს. ამასთან, აღსანიშნავია, რომ ანონიმიზაცია იცავს ინდივიდების კონფიდენციალობას და მონაცემის უკანონო ან არაეთიკური გამოყენებისგან.⁵ „GDPR“-ის 26-ე მუხლი უფრო ღრმად იკვლევს პერსონალურ მონაცემებს, რაც თვალსაჩინო ხდის ანონიმიზაციის კონცეფციას. აღნიშნული მუხლის თანახმად, ანონიმიზებული მონაცემი არის მონაცემთა იმგვარი დამუშავების შედეგი, როდესაც შეუძლებელია იდენტიფიცირებულ ან იდენტიფიცირებად მონაცემთა სუბიექტთან მათი დაკავშირება.

ხელახალი იდენტიფიკაციის, ან ანონიმიზებული მონაცემების პერსონალურ მონაცემებად გადაქცევის ალბათობა ფასდება არსებული მონაცემთა ბაზის სპეციფიური მახასიათებლებიდან გამომდინარე. აღნიშნული, შესაძლოა, განხორციელდეს მონაცემთა დადარების ან სხვა მსგავსი მეთოდების გამოყენებით. „GDPR“-ის 26-ე მუხლის თანახმად, იმის დასადგენად, შესაძლებელია თუ არა პირის იდენტიფიცირება, მხედველობაში უნდა იქნას მიღებული ყველა ის მეთოდი, რომელიც შესაძლოა გამოიყენოს, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, ისე სხვა ნებისმიერმა მესამე პირმა.

„იმისათვის, რომ დადგინდეს არის თუ არა ფიზიკური პირი იდენტიფიცირებადი, მხედველობაში უნდა იქნას მიღებული ყველა ის საშუალება, რომელიც გონივრულად იქნება გამოყენებული ფიზიკური პირის პირდაპირ ან ირიბად იდენტიფიცირებისთვის, როგორც დამუშავებისთვის პასუხისმგებელი პირის, ისე სხვა ნებისმიერი მესამე პირის მიერ.

მოცემულ შემთხვევაში „გონივრული“ ცნება გადამწყვეტია, იგი გულისხმობს პიროვნების იდენტიფიცირებისთვის გამოყენებულ საშუალებებს, რაც შეიძლება მოიცავდეს მნიშვნელოვან ხარჯებს, დროსა და მოქმედებას. შეფასებისას მხედველობაში უნდა იქნას მიღებული, როგორც მონაცემთა დამუშავებისას არსებული და ხელმისაწვდომი, ისე შესაძლო სამომავლო ტექნოლოგიები.⁶

⁵ Foglia C., Il Dilemma (ancora aperto) dell'Anonimizzazione e il Ruolo della Pseudonimizzazione nel GDPR, in Circolazione e Protezione dei Dati Personali, tra Libertà e Regole del Mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al Novellato d.lgs. n. 196/2003 (Codice Privacy), 2019. Stalla-Bourdillon S., Knight A., Anonymous Data v. Personal Data-False Debate: an EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Journal, 2017.

⁶ Tempestini L., D'Acquisto G., Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dei dati sensibili, in Le nuove frontiere della privacy nelle tecnologie digitali, Aracne, 2016.

მონაცემთა დაცვის კანონმდებლობით აღიარებული პრინციპები არ ვრცელდება ანონიმიზებულ მონაცემებზე იმ შემთხვევაშიც თუკი მონაცემთა სუბიექტის ინდენტიფიცირება არაპროპორციულად დიდ ძალისხმევას ან/და ხარჯებს საჭიროებს. ამგვარად, ანონიმიზებული მონაცემიდან პირის იდენტიფიცირების მთავარ გამოწვევას იდენტიფიცირების პოტენციური ელემენტების არსებობა წარმოადგენს.⁷

29-ე მუხლის სამუშაო ჯგუფის (“WP29”) მოსაზრებაში 4/2007 (Opinion 4/2007), სიღრმისეულადაა განხილული პერსონალური მონაცემის კონცეფცია, მათ შორის, გაანალიზებულია „იდენტიფიცირებადობის“ მნიშვნელობები⁸, აღნიშნულის თანახმად, ანონიმიზაციის პროცესის მდგრადობა იზომება „გამოსაყენებელი საშუალების გონივრულობის“ (“means reasonably to be used”) ტესტით.

იმის დასადგენად, არის თუ არა გამოყენებული საშუალება „გონივრული“ ფიზიკური პირის იდენტიფიცირებისთვის, მხედველობაში უნდა იქნას მიღებული ყველა ობიექტური ფაქტორი, მათ შორის, იდენტიფიკაციისთვის საჭირო ხარჯები და დრო. ამასთან, უნდა შეფასდეს, როგორც მონაცემთა დამუშავებისას არსებული და ხელმისაწვდომი, ისე შესაძლო სამომავლო ტექნოლოგიები.

„მიზანშეწონილობის“ კრიტერიუმი განსაკუთრებით აქტუალურია სტატისტიკური მონაცემების კონტექსტში. თუკი შეჯამებული მონაცემი, მისი მცირე ზომის ან სხვა საიდენტიფიკაციო ინფორმაციის ხელმისაწვდომობის გამო, პოტენციურად იწვევს პირის იდენტიფიცირებას, რაც ხაზს უსვამს ანონიმიზაციის პროცესის არაადეკვატურობას.⁹

ეფექტიანი ანონიმიზაცია ხელს უშლის ნებისმიერ ორგანიზაციას, რომ მათ მიერ მონაცემთა ბაზაში მოხდეს ინდივიდის იზოლირება ან მოხდეს ორი ჩანაწერის დაკავშირება. ანონიმიზაციის უზრუნველსაყოფად მხოლოდ პირდაპირი იდენტიფიკატორების ამოღება არ კმარა.¹⁰ ხშირ შემთხვევაში საჭიროა დამატებითი ზომების მიღება, რომელთა ბუნება დამოკიდებულია მონაცემთა დამუშავების კონტექსტსა და მიზანზე. მნიშვნელოვანია, ასევე, ანონიმიზაციისათვის საჭირო ძალისხმევისა და ხარჯების შედარება ინდივიდების იდენტიფიცირების მზარდ ტექნიკურ შესაძლებლობებთან, მონაცემთა საჯარო ხელმისაწვდომობასა და არასრული ანონიმიზაციის შემთხვევებთან.¹¹

ტერმინი „იდენტიფიცირებადი“ მიემართება ნებისმიერ პირს, რომელიც ამუშავებს მონაცემებს და არა მხოლოდ დამუშავებისთვის პასუხისმგებელ თავდაპირველ პირს. თუ დამუშავებისთვის პასუხისმგებელი პირი ინახავს იდენტიფიცირებად ნედლ მონაცემებს და აზიარებს შეცვლილ ვერსიას, აღნიშნული მაინც კლასიფიცირდება, როგორც პერსონალური მონაცემი. ამის საწინააღმდეგოდ თუ დამუშავებისთვის პასუხისმგებელი პირი მონაცემს სრულად არაიდენტიფიცირებადს გახდის და მხოლოდ საერთო სტატისტიკისთვის გააზიარებს, აღნიშნული ანონიმიზებულ მონაცემად ჩაითვლება. ანონიმიზაციის

⁷ D’Acquisto G., Naldi M., Big Data e Privacy by Design, Anonimizzazione, Pseudonimizzazione, Sicurezza, Giappichelli, 2017.

⁸ Article 29 Data Protection Working Party (WP29), Opinion 4/2007 on the Concept of Personal Data, 2007.

⁹ Information Commissioner’s Office (ICO), Anonymisation: Managing Data Protection Risk Code of Practice, 2012.

¹⁰ Agencia Española de Protección de Datos (AEDP) and European Data Protection Supervisor (EDPS).

¹¹ Misunderstanding related to Anonymization, 2021, <https://www.edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en>[31.07.2024].

ტექნიკის გამოყენებისას დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს არჩეული მეთოდის სანდოობის დონე არსებულ ტექნოლოგიურ საშუალებებთან მიმართებით.

2.3. კონფიდენციალობის დარღვევის და თავდასხმების სახეები

29-ე მუხლის სამუშაო ჯგუფის (“WP29”) მიერ იდენტიფიცირებულია თავდასხმის სამი ძირითადი ტიპი ანონიმიზაციასთან მიმართებით: „გამორჩევა“ (Singling Out), „დაკავშირება“ (Linkability), „ვარაუდი“ (Inference)¹²:

- „გამორჩევა“ (Singling Out): გულისხმობს ზოგიერთი ან ყველა ჩანაწერის იზოლირების შესაძლებლობას, რომლითაც იდენტიფიცირდება ინდივიდი მონაცემთა ბაზაში. აღნიშნული მოიცავს ინდივიდის ჯგუფიდან გამორჩევის უნარს, რამაც შეიძლება გამოიწვიოს იდენტიფიკაცია, თუნდაც ინდივიდის ზუსტი ვინაობა უცნობი იყოს.
- Singling Out თავდასხმის ტიპი ყურადსაღები გახდა 1990-იან წლებში, როდესაც “MIT“-ის სტუდენტმა, ლატანია სვინიმ, მოიპოვა მასაჩუსეტისის გუბერნატორის უილიამ უელდის,¹³ სავარაუდოდ, ანონიმიზებული ჯანმრთელობის შესახებ ცნობები. მან შეადარა ეს ჩანაწერები ამომრჩეველთა საჯარო რეგისტრაციის მონაცემებთან, და აღნიშნა, რომ “ZIP” კოდი, დაბადების თარიღი და მხოლოდ სქესი აშშ-ს მოსახლეობის აბსოლუტურ უმრავლესობის იდენტიფიცირების შესაძლებლობას იძლევა.
- „დაკავშირება“ (Linkability) - აღნიშნული გულისხმობს ერთ მონაცემთა სუბიექტთან, ასევე ერთ ან ორ მონაცემთა ბაზაში არსებულ სუბიექტთა ჯგუფთან დაკავშირებული მინიმუმ ორი ჩანაწერის ერთმანეთთან დაკავშირების შესაძლებლობას. ეს ნიშნავს, რომ თუ ცალ-ცალკე შეგროვებული ინფორმაციის სხვადასხვა ნაწილის ერთმანეთთან დაკავშირებით შესაძლებელია პირის იდენტიფიცირება, ანონიმიზაციის პროცესი არაეფექტურია.
- „Linkability“-ის თავდასხმის ტიპი აქტუალური გახდა 2006 წელს „Netflix“-ში მომხდარი ინციდენტის დროს. კერძოდ, მკვლევრებმა ნარაიანამა და შმატიკოვმა „Netflix“-ის მონაცემთა ბაზაში არსებული მომხმარებლის ანონიმიზებული მონაცემები დაუკავშირეს „Internet Movie Database“ (“IMDb”)-ში არსებულ საჯაროდ ხელმისაწვდომ მონაცემებს. მათ შეძლეს იმ ანონიმიზებული მომხმარებლების იდენტიფიცირება, რომლებმაც “IMDb“-ზე თავიანთი სახელებით გამოაქვეყნეს ფილმების რეიტინგები. აღნიშნული ცხადყოფს, რომ ერთი შეხედვით ერთმანეთთან დაუკავშირებელმა ინფორმაციამ შეიძლება საფრთხე შეუქმნას მონაცემთა ანონიმიზაციას.
- „ვარაუდი“ (Inference) - სამართლებრივ კონტექსტში, ის ეხება ინდივიდის შესახებ უცნობი ინფორმაციის ცნობილი ინფორმაციიდან ამოღების შესაძლებლობას. “Inference” თავდასხმის ტიპი სარგებლობს მონაცემების

¹² Article 29 Data Protection Working Party (WP29). “Opinion 05/2014 on Anonymisation Techniques”, 2014

¹³ Barth-Jones D., The ‘Re-Identification’ of Governor William Weld’s Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now, 2012. Narayanan A., Shmatikov V., How to Break Anonymity of the Netflix Prize Dataset (arXiv preprint cs/0610105), 2006.

სტატისტიკური დამოკიდებულებებით, რათა გამოხშიროს განსაკუთრებული კატეგორიის მონაცემი ჩვეულებრივისგან.

- ამ თვალსაზრისით საინტერესოა 2014 წლის საქმე, რომელიც ეხება ნიუ-იორკის ტაქსისა და ლიმუზინის კომისიის მონაცემთა ბაზებს.¹⁴ კერძოდ, ანონიმიზებული მონაცემთა ბაზა შეიცავდა დეტალებს ქალაქში ტაქსით ყველა მგზავრობის შესახებ. მიუხედავად ამისა, მკვლევრებს შეეძლოთ აღნიშნული მონაცემთა ბაზიდან არა მხოლოდ კონკრეტული მძღოლების არამედ სხვა პირების, მათ შორის, ცნობილი ადამიანების აქტივობების და შემოსავლის იდენტიფიცირება და იმის დემონსტრირება, რომ სავარაუდო ანონიმური მონაცემებიც კი შეიძლება იყოს დაუცველი ამგვარი შეტევების მიმართ. აღნიშნული ცხადყოფს, რომ „Inference“-ის თავდასხმის დროს ანონიმიზებულად მიჩნეული მონაცემებიც შესაძლოა იყოს დაუცველი.

ამგვარად, ანონიმიზაციის მძლავრი მექანიზმი იცავს პირებს მონაცემთა ბაზაში „გამორჩევიდან“ („Singling out“), ასევე, ერთ ან რამდენიმე მონაცემთა ბაზაში არსებული ჩანაწერების მათთან ასოცირებისგან („Linkability“) და მონაცემთა ბაზაში შემავალი კონკრეტული პირების შესახებ ინფორმაციის გამოხშირვისგან („Inference“)¹⁵. შესაბამისად, შეიძლება ითქვას, რომ მაიდენტიფიცირებელი ელემენტების მხოლოდ ამორიცხვა შესაბამის მექანიზმს არ წარმოადგენს, რადგან რიგ შემთხვევებში მონაცემთა დამუშავების კონტექსტი, მიზანი და აუცილებლობა დამატებით ნაბიჯებს მოითხოვს. აქვე უნდა აღინიშნოს, რომ მონაცემთა დაცვის კანონმდებლობა ვრცელდება მხოლოდ იმ შემთხვევაში, თუკი პირის იდენტიფიცირება შესაძლებელია, განურჩევლად დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიზნებისა.

კონფიდენციალობასთან დაკავშირებული ბოლოდროინდელი შეხედულებები აღნიშნულს ყოფს ორ კატეგორიად: იდენტობის გამჟღავნება და პირის შესახებ უცნობი ინფორმაციის ცნობილი ინფორმაციიდან ამოღების შესაძლებლობა.¹⁶ აღნიშნული მოიცავს 29-ე სამუშაო ჯგუფის მიერ განმარტებულ „გამორჩევის“ („Singling Out“) და „ვარაუდის“ („Inference“) ტიპს. ორივე შემთხვევაში თავდასხმა წარმატებული იქნება, თუკი თავდამსხმელს შეეძლება პირის იდენტიფიცირება მონაცემთა ბაზაში („იდენტობის გამჟღავნება“) ან თავდამსხმელი მოიპოვებს ინფორმაციას კონკრეტული ინდივიდის შესახებ (ელემენტების გამოხშირვა). თავდასხმის წარმატებით განხორციელებისას, თავდამსხმელს ან სწორად უნდა შეეძლოს პირის იდენტიფიცირება მონაცემთა ბაზაში (იდენტიფიკაციის გამჟღავნება), ან უნდა ჰქონდეს გარკვეული ინფორმაცია კონკრეტული ინდივიდის შესახებ („პარამეტრის დასკვნა“). აღნიშნული განმარტებიდან გამომდინარე, „დაკავშირება“ („Linkability“) მიიჩნევა ზემოაღნიშნული მიზნებიდან ერთ-ერთის მიღების საშუალებად და არა თავდასხმის ტიპად, დღევანდელ ციფრულ სამყაროში არსებული ინფორმაციის სიმრავლის და პიროვნებებთან მის დასაკავშირებლად¹⁷ საჭირო შეზღუდული შესაძლებლობებიდან გამომდინარე.¹⁸

¹⁴ Hern A., New York Taxi Details Can Be Extracted from Anonymised Data, Researchers Say, The Guardian, 2014.

¹⁵ Article 29 Data Protection Working Party (WP29), „Opinion 05/2014 on Anonymisation Techniques“, 2014.

¹⁶ Hu J., Bowen C.M., Advancing Microdata Privacy Protection: A Review of Synthetic Data, 2023.

¹⁷ იხ.: De Montjoye Y. A., Hidalgo C. A., Verleysen M., & Blondel V. D., Unique in the Crowd: The Privacy Bounds of Human Mobility, Scientific Reports, 3(1), 2013, 1-5.

¹⁸ Beduschi A., Synthetic Data Protection: Towards a Paradigm Change in Data Regulation? *Big Data & Society*, 11(1), 2024.

3. სინთეზური მონაცემების გენერირება, როგორც ანონიმიზაციის მექანიზმი

სინთეზური მონაცემების კონცეფციას განვმარტავთ შემდეგნაირად¹⁹: „სინთეზური მონაცემი (“SD”) არის მონაცემი, რომელიც წარმოიქმნება მიზანმიმართული მათემატიკური მოდელის ან ალგორითმის („გენერატორის“) გამოყენებით, მონაცემთა მეცნიერების ამოცანების ამოსახსნელად.

ანალიზისას ჩვენ შემოვიფარგლებით მხოლოდ იმ სინთეზური მონაცემებით, რომლებიც გენერირებულია რეალურ მონაცემებზე დამყარებული მანქანური სწავლების ალგორითმის მეშვეობით (შემდგომ „სინთეზური მონაცემი“ ან “SD”). იურიდიულ საზოგადოებაში სინთეზური მონაცემების სწორედ ეს ფორმა წარმოადგენს ყველაზე განხილვად საკითხს.

აღნიშნულ თავში ყურადღება გამახვილდება, თუ რატომ წარმოადგენს სინთეზური მონაცემები მე-2 თავში აღნიშნულ ანონიმიზაციის ერთ-ერთ ტექნიკას. ამ მიზნით, პირველ რიგში, განხილულ იქნება კომპიუტერული მეცნიერების პერსპექტივები, ხოლო შემდგომ ტექნოლოგიებთან დაკავშირებული დინამიკური და განვითარებადი სამართლებრივი ლანდშაფტი. ბოლოს, განიხილება შესაბამისი ტექნოლოგიების სწორი გამოყენების გზები, რისკფაქტორების გათვალისწინებით, ამასთან, თავში მოცემულია კონკრეტული რეკომენდაციებიც. ყოველივე ეს ხაზს უსვამს, რომ სინთეზური მონაცემი წარმოადგენს ანონიმიზაციის ერთ-ერთ ტექნიკას.

3.1. მეცნიერული პერსპექტივები

სინთეზურ მონაცემთა გამოყენების მთავარი მიზანი ანონიმიზაცია და კონფიდენციალობის დაცვაა.²⁰ აღნიშნულის მთავარი მიზეზი სინთეზური მონაცემების კონცეფციაა, რომელიც პიროვნებასა და მონაცემებს ერთმანეთს ამორებს (ვერ ხერხდება იდენტიფიცირება). ანონიმიზაციის არსებული ტექნოლოგიები ეფუძნება რეალურ მონაცემებს, მათ შორის, შემთხვევითი განაწილებისა (“randomization”) და გენერაციის მეთოდებს.²¹ აღნიშნულის საპირისპიროდ, სინთეზური მონაცემი გენერირდება მონაცემთა ნაკრების სტატისტიკური მოდელის შექმნით. კერძოდ, მოდელი, განსაზღვრული ალბათობის საფუძველზე, აკვირდება რეალური მონაცემების შაბლონებს (“pattern”). შემდგომ ამ მოდელის ნიმუშის აღება შესაძლებელია ახალი, სრულად ხელოვნური ჩანაწერების შესაქმნელად.

აღნიშნული პროცესის უკეთ აღქმა შესაძლებელია ექსპერიმენტის საფუძველზე.²² დავუშვათ, პირს სურს შექმნას მონაცემთა ხელოვნური ნაკრები, რომელიც ზუსტად ასახავს ადამიანთა რეალურ მახასიათებლებს. წინასწარ ჩატარებული კვლევის საშუალებით პირს აქვს ცოდნა ადამიანთა ზოგიერთი მახასიათებლის შესახებ. მაგალითად, ცნობილია, რომ დედამიწაზე ქალისა და

¹⁹ Jordon J., Szpruch L., Houssiau F., Bottarelli M., Cherubin G., Maple C., Weller A., Synthetic Data-What, Why and How? 2022.

²⁰ იქვე.

²¹ Article 29 Data Protection Working Party (WP29), “Opinion 05/2014 on Anonymisation Techniques”, 2014.

²² This thought experiment was previously described in a blog post, <<https://aindo.com/blog/is-synthetic-good/>> [30.07.2024].

მამაკაცის თანაფარდობა არის 1:1. გარდა ამისა, ცნობილია, რომ ყოველ ექვს ადამიანში მხოლოდ ერთს აქვს ცისფერი თვალები, დანარჩენს კი - ყავისფერი. „ხელოვნური ადამიანის“ მონაცემის შესაქმნელად მკვლევრები ატარებენ შემდეგ ექსპერიმენტს: მონეტის აგდებით და მიღებული შედეგით (ალბათობა $\frac{1}{2}$) ადგენენ „ხელოვნური ადამიანი“ იქნება ქალი თუ კაცი. შემდგომ მკვლევრები აგორებენ კამათელს, თუკი გაგორდა 6-იანი (ალბათობა $\frac{1}{6}$) „ხელოვნური ადამიანის“ თვალის ფერი იქნება ლურჯი, ხოლო სხვა ნებისმიერი შედეგის შემთხვევაში - ყავისფერი (ალბათობა $\frac{5}{6}$). ამ ექსპერიმენტის მრავალჯერ გამეორებით, მკვლევრები იღებენ მთლიანად სინთეზურ მოსახლეობას, რომელსაც აქვს რეალური მოსახლეობის ყველა სტატისტიკური და მათემატიკური თვისება.²³ მიუხედავად ამისა, ჩანაწერები წარმოიქმნება ალბათობაზე დაფუძნებული ექსპერიმენტებით და არა რეალური ინდივიდების მონაცემების გამოყენებით.

გენერირებად ხელოვნურ ინტელექტზე დაფუძნებული სინთეზური მონაცემიც ანალოგიურად იქმნება, თუმცა ავტომატიზებული და შედარებით უფრო დახვეწილი მეთოდით. ზემოაღნიშნული ექსპერიმენტი მოსახლეობის შესახებ წინასწარ ცოდნას და კვლევას მოითხოვს (კაცების და ქალების თანაფარდობა და თვალის ფერები). გენერირებადი ხელოვნური ინტელექტის გამოყენებისა კი ეს არ არის სავალდებულო. ხელოვნურ ინტელექტზე დაფუძნებული გენერატორები ზუსტად იმეორებენ სახასიათო ნიშნებს შორის თანაფარდობას. წინა აბზაცში მოცემულ ექსპერიმენტში, მაგალითად, ცისფერთვალებიანთა საერთო წილი შეიძლება იყოს $\frac{1}{6}$, მაგრამ, შესაძლოა, ცისფერი თვალები უფრო ხშირი იყოს ქალებში, ვიდრე მამაკაცებში. გენერირებად მოდელს შეუძლია ავტომატურად დაადგინოს და გაიმეოროს თანაფარდობა.²⁴

როგორც კონფიდენციალობის დაცვის, ისე სწორად გენერირებული სინთეზური მონაცემის ხარისხი ფართოდ არის აღიარებული. აშშ-ს სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (“NIST”) შეადარა დე-იდენტიფიკაციის (“de-identification”) მრავალი ალგორითმი²⁵. შედეგების ცხრილი გვიჩვენებს²⁶, რომ სინთეზური მონაცემის გენერატორები კონფიდენციალობის დაცვის ერთ-ერთ საუკეთესო საშუალებას წარმოადგენს. აღნიშნული ემპირიული მტკიცებულების საფუძველზე შეიძლება ითქვას, რომ სინთეზური მონაცემი ანონიმიზაციის სანდო საშუალებაა, აღნიშნული დასტურდება “NeurIPS 2020 Hide-and-Seek Privacy challenge”-ის²⁷ ფარგლებშიც.²⁸

²³ By a theorem called “The Law of Large Numbers”, see any introductory text on probability theory.

²⁴ Finocchiaro G., Landi A., Polifronei G., Ruffo D., Torlontano F., Il Futuro Regolatorio Dei Dati Sintetici. La Sintetizzazione dei Dati Come Risorsa per Ricerca Scientifica, Innovazione e Politiche Pubbliche nel Panorama Giuridico Europeo, 2024.

²⁵ See: Task C., Bhagat K., Howarth G., SDNist v2: DeidentifiedDataReport Tool, 2023, <<https://data.nist.gov/od/id/mds2-2943>> [30.07.2024].

²⁶ See NIST Collective Research Cycle (CRC), <https://pages.nist.gov/privacy_collaborative_research_cycle/pages/archive.html> [30.07.2024].

²⁷ Jordon J., Jarrett D., Saveliev E., Yoon J., Elbers P., Thorat P., van der Schaar M., Hide-and-Seek Privacy Challenge: Synthetic Data Generation vs. Patient Re-Identification.

²⁸ Competition and Demonstration Track, 2021.

3.2. პოლიტიკა და მარეგულირებელი პერსპექტივები

სინთეზური მონაცემის გენერირების პროცესი, როგორც ანონიმიზაციის საშუალება სამეცნიერო საზოგადოების მსგავსად, იურიდიულ საზოგადოებაშიც დიდი პოპულარობით სარგებლობს. თავის სასემინარო ნაშრომში, სტივენ ბელოვინი აღნიშნავს, რომ²⁹ „სინთეზური მონაცემი გვთავაზობს პროგრესს. მიუხედავად იმისა, რომ იგი არ არის უნაკლო, აღნიშნული მეთოდი იძლევა საშუალებას ბოლო მოეღოს იდენტიფიცირების პრობლემას და ფოკუსირება მოხდეს უფრო მნიშვნელოვან საკითხებზე - სასარგებლო პერსონალურ მონაცემებზე. აქედან გამომდინარე, კონფიდენციალობის დაცვის სფეროში ჩართულ საზოგადოებას ვურჩევთ დანერგონ სინთეზური მონაცემები შესაბამისი ბაზებში კონფიდენციალობის პრობლემის გადასაჭრელად.

აღნიშნული მოსაზრება ეხმიანება Finocchiaro-ს და სხვების უახლეს იურიდიულ ანალიზს, რომელიც თანახმადაც სინთეზური მონაცემის სწორი გენერირება წარმოადგენს „ანონიმიზაციის მოწინავე ტექნოლოგიას, რომელიც შეესაბამება მონაცემთა დაცვის მოქმედ და სამომავლო რეგულაციებს“.³⁰

სამეცნიერო საზოგადოების გარდა, სინთეზური მონაცემები, როგორც ანონიმიზაციის მეთოდი, უფრო და უფრო პოპულარული ხდება კანონმდებლებსა და სხვა სამთავრობო ორგანიზაციებს შორის.³¹ ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხებველო ორგანო („AEDP“) ცალსახად აღიარებს, რომ სინთეზური მონაცემი, გარკვეულ პირობებში, შესაძლოა გაუტოლდეს ანონიმურ მონაცემებს. „მონაცემთა მართვის აქტი“ („The Data Governance Act“)³² და „ხელოვნური ინტელექტის შესახებ აქტი“ („AI Act“)³³ აღიარებს სინთეზური მონაცემის გენერაციას, როგორც მონაცემთა დამუშავებისას კონფიდენციალობის შენარჩუნების მეთოდს, რომელიც გაიგივებულია ანონიმურ მონაცემებთან. ევროკავშირის ერთობლივი კვლევითი ცენტრი („JRC“) ასევე, მიიჩნევს, რომ სწორად შემუშავებულ სინთეზურ მონაცემი, ერთი მხრივ, ამცირებს კონფიდენციალობასთან დაკავშირებული რისკებს, ხოლო, მეორე მხრივ, ხელს უწყობს ხელოვნური ინტელექტის სფეროს სტრატეგიულ განვითარებას.³⁴

ბოლოს, საინტერესოა საფრანგეთში მოქმედი კანონი „Loi pour une République numérique“, რომელიც საფრანგეთის მონაცემთა დაცვის ორგანოს („CNIL“) უფლებას აძლევს დაამტკიცოს ანონიმიზაციის ტექნიკა. 2020 წელს „CNIL“-მა გამოიყენა აღნიშნული უფლებამოსილება და დაამტკიცა სინთეზური მონაცემების გენერირების მეთოდოლოგია, კერძოდ, დადასტურა მისი ანონიმური ბუნება, გადაწყვეტილების მიღების პროცესში კი დაეყრდნო ისეთ კრიტერიუმებს როგორიცაა

²⁹ Bellovin Steven M., Dutta, Preetam K., Reitinger N., Privacy and Synthetic Datasets. Stanford Technology Law Review, Vol. 22, 2018.

³⁰ Finocchiaro G., Landi A., Polifronei G., Ruffo D., Torlontano F., Il Futuro Regolatorio Dei Dati Sintetici. La Sintetizzazione dei Dati Come Risorsa per Ricerca Scientifica, Innovazione e Politiche Pubbliche nel Panorama Giuridico Europeo, 2024.

³¹ Agencia Española de Protección de Datos (AEDP), „Approach To Data Spaces From GDPR Perspective“, 2023.

³² See Recital 7 of the Regulation (EU) 2022/868.

³³ See art. 10.5.a and art. 59.1.b of the Regulation (EU) 2024/1689.

³⁴ See Hradec J., Craglia M., Di Leo M., De Nigris S., Ostlaender N., Nicholson N., Multipurpose Synthetic Population for Policy Applications, JRC Technical Report, 2022, 58-60.

ინდივიდუალიზაციის, დაკავშირებისა ("Linkability") და ვარაუდის ("Inference") შესაძლებლობა.³⁵

"CNIL"-მა დაიწყო ემპირიული შეფასების სისტემასთან დაკავშირებით საკანონმდებლო რეგულაციაზე მუშაობა, რომლის მიზანია დაადგინოს თუ რამდენად იცავს კონკრეტული სინთეზური მონაცემთა ნაკრები კონფიდენციალობას.³⁶ აღნიშნულის მეშვეობით, რაოდენობრივ და უფრო ობიექტური ანალიზის საფუძველზე იქნება შესაძლებელი სინთეზური მონაცემების გენერირების სხვადასხვა ტექნიკის ვალიდაცია.

4. სინთეზური მონაცემების გამოყენების რეკომენდაციები

მესამე თავში განხილულია სინთეზური მონაცემების, როგორც ანონიმიზაციის ტექნოლოგიის, მეცნიერული და საკანონმდებლო პერსპექტივები. ნაშრომში არაერთხელ აღინიშნა, რომ სწორი გამოყენების პირობებში, სინთეზური მონაცემი წარმოადგენს ანონიმიზაციის მიღწევის მეტად ძლიერ საშუალებას. კონფიდენციალობის პოტენციური რისკების, ასევე, სინთეზური მონაცემების გენერაციის თეორიული შედეგების საფუძველზე გაანალიზებულია თუ რას ნიშნავს „სათანადო გენერირება“. თავში მოცემულია რისკების მინიმალიზაციისთვის საჭირო კონკრეტული რეკომენდაციები. აღნიშნული ხელს უწყობს ტექნოლოგიის სწორ გამოყენებას, რათა სინთეზურ მონაცემს მიენიჭოს ანონიმიზაციის სტატუსი.

4.1. სინთეზურ მონაცემთან დაკავშირებული რისკები

ძირითადი რისკფაქტორები იდენტიფიცირებულია ჩვენს წინა ნაშრომში³⁷, კერძოდ: 1) გენერატორის ხარისხი; 2) სინთეზის მიდგომა; 3) რეალური მონაცემთა ნაკრების თვისებები (აღკვეთის არსებობა, სიმცირე და ა.შ.); 4) თავდამსხმელის ხელთ არსებული ინფორმაცია (საფრთხის მოდელი). ეს ფაქტორები შეესაბამება ევროკავშირის მონაცემთა დაცვის ზედამხედველის ("EDPS")³⁸ მიერ გამოვლენის სინთეზურ მონაცემთან დაკავშირებულ საფრთხეებს. აღნიშნული რისკები პრაქტიკაში შეიძლება შემცირდეს კონფიდენციალობის შეფასებისას პროაქტიული და რაოდენობრივი მიდგომის მიღებით.^{39/40}

³⁵ See Octopize's communication on the CNIL evaluation in the following presentation:

<https://documentation-snds.health-data-hub.fr/files/presentations/meetup-snds7/20210318_Octopize_Deck-OctopizeHdhCom_MLP-2.0.pdf> [30.07.2024].

³⁶ See CNIL's Letterto Statice GmbH on Anonymeter,

<https://www.anonos.com/hubfs/Documents/Reports/CNIL_Anonymeter.pdf> [30.07.2024].

³⁷ Panfilo D., Boudewijn A. T., Ferraris A. F., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R., Measuring Privacy Protection in Structured Synthetic Datasets: A Survey, in: Hideyuki Matsumi, Paul De Hert et al. (ed) Privacy and Data Protection: Ideas that Drive Our Digital World, 2024.

³⁸ Wiewiórowski W., Synthetic Data: What Use Cases as Privacy Enhancing Technology? IPEN Webinar on Synthetic Data, European Data Protection Supervisor.

³⁹ Kaabachi B., Despraz J., Meurers T., Otte K., Halilovic M., Prasser F., Raisaro J. L., Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics, 2023.

⁴⁰ Boudewijn A. T. P., Ferraris A. F., Panfilo D., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R., Privacy Measurements in Tabular Synthetic Data: State of the Qrt and Future Research Directions, NeurIPS 2023 Workshop on Synthetic Data Generation with Generative AI, 2023.

რეკომენდაცია: სინთეზურ მონაცემებთან მომუშავე პრაქტიკოსებმა უნდა იცოდნენ კონფიდენციალობის პოტენციური რისკები. მეტიც, მათ უნდა გამოიყენონ რაოდენობრივი და ობიექტური მეთოდები კონფიდენციალობის რისკების შესაფასებლად და შესამცირებლად. ჩვენი ბოლო გამოკითხვა კონფიდენციალობის რაოდენობრივ განსაზღვრასთან დაკავშირებით სიღრმისეულად აანალიზებს ამგვარი მეთოდებს და მათ უპირატესობებს. გარდა ამისა, წარმოგიდგენთ დამატებით პრაქტიკულ რეკომენდაციებს ამ მეთოდების ოპტიმალური გამოყენებისთვის. დამატებით გირჩევთ გამოიყენოთ სხვადასხვა ზომები, რათა დარწმუნდეთ, კონფიდენციალობასა და სარგებლიანობას შორის სწორი ბალანსის არსებობაში.

4.2. სინთეზური მონაცემსა და გენერაციაზე დაფუძნებული კონფიდენციალობა

სინთეზური მონაცემის ტექნოლოგიებთან მიმართებით ფუნდამენტური შეკითხვაა კონფიდენციალობის დაცვა წარმოადგენს სინთეზური მონაცემის (შემდგომ - სინთეზური მონაცემებზე დაფუძნებული) თუ გენერატორის (შემდგომ: გენერატორზე დაფუძნებული) საკუთრებას. ეს შეხედულებები გავლენას ახდენს პრაქტიკაში კონფიდენციალობის რაოდენობრივ შეფასებაზე. სხვადასხვა პერსპექტივის საილუსტრაციოდ, განვიხილოთ ე.წ. „მუდმივ მაიმუნთა თეორია“ („infinite monkey theorem“)⁴¹. ეს თეორია ამტკიცებს, რომ თუკი მაიმუნი, შემთხვევითობის პრინციპით, საბჭადი მანქანის კლავიშებს მუდმივად დააჭერს თითს, დროის გარკვეულ მომენტში აკრეფს შექსპირის ნაშრომს. ანალოგიურად მოქმედებს გენერატორიც, რომელიც თავისი შემთხვევითობრივი („stochasticity“) ხასიათის გამო, ქმნის (თითქმის) რეალური ინდივიდის იდენტურ მონაცემებს. ჩნდება კითხვა:⁴² ირღვევა თუ არა ამ პიროვნების კონფიდენციალობა? „სინთეზური მონაცემებზე დაფუძნებული“ კონფიდენციალობის პირობებში, პასუხი არის „დიახ“, რადგან სინთეზური მონაცემთა ნაკრები ავლენს ინდივიდს. „გენერატორზე დაფუძნებული“ კონფიდენციალობის პირობებში, პასუხი არის „არა“, რადგან ინდივიდის მონაცემების შექმნა არ ეფუძნება მოდელის მიერ სასწავლო ნაკრების ჩანაწერების დაცვის ნაკლებობას.

პრაქტიკაში უფრო გავრცელებულია „სინთეზური მონაცემებზე დაფუძნებული“ კონფიდენციალობა: ბოლოდროინდელმა ლიტერატურულმა მიმოხილვამ როგორც სასარგებლო, ისე კონფიდენციალობის რაოდენობრივ განსაზღვრაზე სამედიცინო კონტექსტში აღმოაჩინა, რომ ნაშრომების 81.2% (22-დან 18), რომელიც სინთეზურ მონაცემთან მიმართებით კონფიდენციალობის რაოდენობრივი მიდგომას იყენებს, არის „სინთეზური მონაცემებზე დაფუძნებული“; მხოლოდ 9.1% (22-დან 2) არის

⁴¹ იხ. ნაშრომის საწყისი ნაწილი ალბათობის თეორიის შესახებ.

⁴² „infinite monkey“ თეორემისგან განსხვავებით, გენერატორი, როგორც წესი, არ გამოიმუშავებს ინდივიდის ჩანაწერს. გამომდინარე იქედან, რომ გენერატორი ზუსტად აყალიბებს შედეგებს, განსხვავებით უკვე აღნიშნულ ფარგლებში, მასში მოხვედრილი საკითხების ერთგვაროვანი განაწილებისგან. ამგვარად, გენერატორი სულაც არ წარმოქმნის ყველა შესაძლო ალბათობის კომბინაციას, უსასრულო რაოდენობის განსაზღვრით, ხოლო შემთხვევა, როდესაც გენერატორი ქმნის ჩანაწერს, რომელიც ზედმეტად ჰგავს რეალურ პირს, რომლის მონაცემები არ იყო გამოყენებული, ეს თავსდება მისი შესაძლებლობების სფეროში.

„გენერატორზე დაფუძნებული“. დანარჩენი 9.1% იყენებს ორივეს კომბინაციას⁴³. „სინთეზურ მონაცემებზე დაფუძნებული“ კონფიდენციალობის პოპულარობას სავარაუდოდ ორი მიზეზი განაპირობებს. პირველ რიგში, უსასრულო მაიმუნის თეორია ავლენს მოდელზე დაფუძნებული კონფიდენციალობის ხარვეზებს. მეორეც, მონაცემთა ბაზაზე დაფუძნებული კონფიდენციალობა შეიძლება შეფასდეს ისეთი კრიტერიუმის გამოყენებით, რომელიც ადვილად გასაგებია და პირდაპირ უკავშირდება რეალურ სიტუაციებს. აღნიშნული კრიტერიუმები, როგორც წესი, ზომავს: 1. რამდენად სავარაუდოა, რომ გენერირებული ჩანაწერები დაკოპირებულია რეალურიდან, 2. სარისკო მსგავსებას სინთეზურ და რეალურ ჩანაწერებს შორის; 3. რამდენად წარმატებულია განზრახი თავდასხმები.⁴⁴

გენერატორზე დაფუძნებული კონფიდენციალობა გთავაზობთ რამდენიმე უპირატესობას. პირველი რიგში, ის, როგორც წესი, ინტეგრირებულია გენერირების პროცესში მომხმარებლის მიერ კონტროლირებადი, პროაქტიული გზით. აღნიშნულის ყველაზე გავრცელებული მაგალითია განზოგადების კონტროლი⁴⁵ ადრეული გაჩერების მეშვეობით და დიფერენციალური კონფიდენციალობა, სადაც მომხმარებელი თავად ადგენს „კონფიდენციალობის ბიუჯეტს“. გარდა ამისა, დიფერენციალური კონფიდენციალობა იყენებს კომპოზიციის თეორიას, რომლებიც ამტკიცებს რომ მათემატიკური მანიპულირება ვერ შეუქმნის საფრთხეს კონფიდენციალობის დაცვას. აღნიშნულს დიდი მნიშვნელობა ენიჭება იმის განსასაზღვრად ანონიმიზაციის პროცესი იყო თუ არა წარმატებული. თუმცა, არის გამოწვევები: „კონფიდენციალობის ბიუჯეტის“ ინტერპრეტაცია პრაქტიკაში საკმაოდ ძნელია^{46,47}. უფრო მეტიც, კომპოზიციის თეორია იცავს მათემატიკური მანიპულაციისგან, მაგრამ არა კომბინირებული დამხმარე ინფორმაციის („compounding auxiliary information“) გამოყენებისგან.

რეკომენდაცია: ზემოაღნიშნულის გათვალისწინებით, გირჩევთ გამოიყენოთ მონაცემთა და გენერატორზე დაფუძნებული მეთოდების კომბინაცია. მონაცემთა ბაზაზე დაფუძნებული მეთოდები ფოკუსირებულია სინთეზურ მონაცემთა ნაკრებებზე, რომლებიც იყენებენ კონფიდენციალობის ემპირიულ შეფასებებს და მსგავსებების შეფასებებს, რათა უზრუნველყონ, რომ ინფორმაცია არ იყოს იდენტიფიცირებადი. ამის საწინააღმდეგოდ, მოდელზე დაფუძნებული ტექნიკა, კონფიდენციალობის მექანიზმების უშუალოდ მონაცემთა გენერირების პროცესში ჩართვის მეშვეობით, იძლევა ძლიერ თეორიულ გარანტიებს. ეს მეთოდები უზრუნველყოფენ, რომ თავად გენერაციული მოდელები არ აამკარავებენ ცალკეულ მონაცემებს. კომბინირებული მიდგომა მაქსიმალურად ზრდის კონფიდენციალობას, რაც ეხება როგორც მოდელს, ისე მონაცემებს.

⁴³ Kaabachi B., Despraz J., Meurers T., Otte K., Halilovic M., Prasser F., Raisaro J. L., Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics, 2023.

⁴⁴ For a thorough survey on both SD-based and generator-based quantification of privacy, see: Boudewijn A. T. P., Ferraris A. F., Panfilo D., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R., Privacy Measurements in Tabular Synthetic Data: State of the Qrt and Future Research Directions, NeurIPS 2023 Workshop on Synthetic Data Generation with Generative AI, 2023.

⁴⁵ Dwork C., Roth A., The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, 9(3-4), 2014, 211-407.

⁴⁶ Lee J., Clifton C., How Much is Enough? Choosing for Differential Privacy.

⁴⁷ International Conference, ISC 2011, Proceedings 14, Springer Berlin Heidelberg, 2011, 325-340.

4.3. „შინაარსთან დაკავშირებული“ და სინთეზური მონაცემები

ლოპეზი და ელბი ამტკიცებენ, რომ დარღვევად უნდა ჩაითვალოს მხოლოდ იმ ინფორმაციაზე წვდომა, რომელიც „შინაარსობრივად“ დაკავშირებულია ინდივიდთან.⁴⁸ აღნიშნული თეორია საკმაოდ პრაქტიკულია, რადგან საჯაროდ არსებული სტატისტიკური მონაცემების გამოყენებით შესაძლებელია კონკრეტული ინდივიდების იდენტიფიცირება. მაგალითად რეგიონის საშუალო შემოსავლის მიხედვით, შეიძლება ამ რეგიონის ხალხის მიმართ გარკვეული მიკერძოება ან ცრურწმენა ჩამოაყალიბოს.

ამ მოსაზრების შესაბამისად სინთეზური მონაცემის გამოყენებისას ჩნდება კითხვა, აძლევს თუ არა სინთეზურ მონაცემზე წვდომა თავდამსხმელებს კონკრეტულ ინდივიდებთან დაკავშირებულ ინფორმაციას. სინთეზური მონაცემი (მათ შორის, გენერაციული) მხოლოდ იმ შემთხვევაში უქმნის რისკს კონფიდენციალობას, თუ მასზე წვდომით შესაძლებელია კონკრეტულ ინდივიდზე იმ ინფორმაციის მოპოვება, რომლის განცალკევება ზოგადი ინფორმაციიდან შეუძლებელი იქნებოდა. აღნიშნული რელევანტურია „ვარაუდის“ (“inference”) სახის თავდასხმის შემთხვევა, რადგან ასეთ დროს გამოიყენება პიროვნების დამახასიათებელი ნიშნები.

ჯიომის და სხვების⁴⁹ მიერ შემუშავებული “The Anonymeter framework” მოიცავს „ვარაუდის“ (“inference”) სახის თავდასხმის შეფასების მეთოდს, რომელიც, მათ შორის, ითვალისწინებს ინფორმაცია არის თუ არა სპეციფიკური თუ ზოგადი. კერძოდ, აღნიშნული მეთოდი ერთმანეთს ადარებს თუ რა შემთხვევაში მოხდა „ვარაუდის“ (inference) სახის თავდასხმის იდენტიფიცირება სინთეზური მონაცემის გამოყენებით და რამდენ შემთხვევაში მაკონტროლებელი ჯგუფის მიერ. თავის მხრივ, მაკონტროლებელი ჯგუფი შედგება იმ რეალური მონაცემებისგან, რომლებიც არ გამოიყენებულა გენერატორის სწავლებისთვის. თუკი აღნიშნული მაჩვენებლები მსგავსია, სინთეზური მონაცემით მოპოვებული ინფორმაცია ზოგადი ხასიათისაა. მეორეს მხრივ, თუკი სინთეზური მონაცემიდან იმაზე მეტი ინფორმაციის მიღება შეიძლება, ვიდრე მაკონტროლებელი ჯგუფისგან, აღნიშნული ინფორმაცია შინაარსობრივად დაკავშირებულია კონკრეტულ პირთან და მიიჩნევა კონფიდენციალობის დარღვევის რისკად.⁵⁰

რეკომენდაცია: კონფიდენციალობის (კერძოდ, „ვარაუდის“ (“inference”) სახის თავდასხმის რისკის) შეფასების დახვეწისთვის, მნიშვნელოვანია გამოიყენოთ იმ რეალური მონაცემებისგან შემდგარი „მაკონტროლებელი ჯგუფი“, რომლებიც არ გამოიყენება გენერატორის სწავლებისთვის. ამით მკვლევრებს შეუძლიათ უფრო ზუსტად განსაზღვრონ, არის თუ არა სინთეზური მონაცემებიდან მიღებული ინფორმაცია ჭეშმარიტად ზოგადი, ან სპეციფიკური დეტალების არასწორი გამოვლენით, ხომ არ ექმნება საფრთხე კონფიდენციალობას.

⁴⁸ López C.A.F., Elbi A., On The Legal Nature of Synthetic Data, NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research, 2022.

⁴⁹ Giomi M., Boenisch F., Wehmeyer C., Tasnádi B., A Unified Framework for Quantifying Privacy Risk in Synthetic Data, 2022

⁵⁰ Platzner M., Reutterer T., Holdout-Based Empirical Assessment of Mixed-Type Synthetic Data, Frontiers in Big Data, 2021.

4.4. გენერატორის სწავლება, როგორც მონაცემთა დამუშავების ფორმა

მიუხედავად იმისა, რომ სწორად გენერირებული სინთეზური მონაცემი ანონიმიზებულია, შესაბამის გენერატორს სჭირდება მექანიკური სწავლება რეალური მონაცემების გამოყენებით, აღნიშნული პროცესი კი, მონაცემთა დაცვის კანონმდებლობის შესაბამისად, კლასიფიცირდება, როგორც მონაცემთა დამუშავება. გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხებელო ორგანო (“ICO”)⁵¹, ცალსახად განმარტავს, რომ ზემოაღნიშნული მექანიკური სწავლების პროცესში მკაცრად უნდა იქნას დაცული შესაბამისი კანონმდებლობა.

კერძოდ, სინთეზური მონაცემების გენერატორების მიერ, საკანონმდებლო რეგულაციებიდან გამომდინარე, მხედველობაში უნდა იქნეს მიღებული შემდეგი გარემოებები:

- სამართლებრივი საფუძველი და მიზანი: დამუშავებისთვის პასუხისმგებელმა პირს უნდა ჰქონდეს მკაფიო და კანონიერი საფუძველი პერსონალური მონაცემების დასამუშავებლად, განსაკუთრებით მაშინ, როდესაც ის მოიცავს განსაკუთრებული კატეგორიის მონაცემებს, როგორიცაა ჯანმრთელობასთან დაკავშირებული მონაცემები (“GDPR” მე-6 და მე-9 მუხლები). ამასთან, მონაცემთა დამუშავების მიზანი უნდა იყოს მკაფიოდ განსაზღვრული და დოკუმენტირებული, და უნდა შეესაბამებოდეს მიზნის შეზღუდვის პრინციპებს.
- მონაცემთა დაცვაზე ზეგავლენის შეფასება (“DPIA”): “DPIA” მეტად მნიშვნელოვანია, მაშინ, როდესაც მონაცემთა დამუშავებამ, შესაძლოა, მაღალი ალბათობით გამოიწვიოს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვა. ეს შეფასება დეტალურად უნდა ასახავდეს მონაცემთა ნაკადებს, ასევე, უნდა აფასებდეს სინთეზის პროცესთან დაკავშირებულ რისკებს და აღწერდეს ზომებს ამ რისკების შესამცირებლად. უნდა აღინიშნოს, რომ “DPIA” არ არის ერთჯერადი პროცესი, არამედ, საჭიროა მისი პერიოდული განახლება, რათა მასში ასახულ იყოს დამუშავების აქტივობებში განხორციელებული მნიშვნელოვანი ცვლილებები და გადაიჭრას მონაცემთა უსაფრთხოებასთან დაკავშირებული სადაო საკითხები.
- ტექნიკური და ორგანიზაციული ზომები: პერსონალური მონაცემების მთლიანობისა და კონფიდენციალობის უზრუნველსაყოფად, “GDPR”-ის 32-ე მუხლი დამუშავებისთვის პასუხისმგებელი პირებისგან მოითხოვს შესაბამისი ტექნიკური და ორგანიზაციული ღონისძიებების მიღებას. აღნიშნული გულისხმობს სინთეზური მონაცემების გენერატორის სწავლების ფაზაში მონაცემთა უსაფრთხო დამუშავების პრაქტიკების მიღებას, ასევე მონაცემთა მინიმიზაციასა და ფსევდონიმიზაციის ტექნიკების შემუშავებას.
- ინფორმაციის აღრიცხვა და შესაბამისობა: მონაცემთა დამუშავების პროცესებთან დაკავშირებული ინფორმაციის აღრიცხვა უნდა მოხდეს “GDPR”-ის მოთხოვნების შესაბამისად (30-ე მუხლი)⁵². აღნიშნული მოიცავს, დამუშავების პროცესის, მიზნების, მონაცემთა კატეგორიის, სუბიექტების და მონაცემთა მიმღებების დეტალურ აღწერას.

⁵¹ Information Commissioner’s Office (ICO), Anonymisation: Managing Data Protection Risk Code of Practice, 2012.

⁵² As provided by the Accountability principle ex art. 5.2 GDPR.

- სერტიფიკატები და სტანდარტების შესაბამისობა: აღიარებული სტანდარტების დაცვა, როგორიცაა “ISO/IEC 27001” და სერტიფიკატების მოპოვება, როგორიცაა “Europrivacy™/®⁵³”, კიდევ უფრო უკეთ უზრუნველყოფს “GDPR”-თან შესაბამისობას და გააძლიერებს ანონიმიზაციის პროცესების სანდოობას. “Europrivacy™/®” აფასებს შესაბამისობას “GDPR”-თან და იმართება სერტიფიკაციისა და კონფიდენციალობის ევროპული ცენტრის მიერ (“ECCP”), რომელიც შეესაბამება “ISO/IEC 17065”-სა და “GDPR”-ის 42-ე მუხლს.
- ეთიკური მოსაზრებები: კანონთან შესაბამისობის გარდა, ყურადღება უნდა მიექცეს ეთნიკურ საკითხებსაც. კერძოდ, პროცესმა არ გააძლიეროს ან გააუარესოს თავდაპირველ მონაცემებში არსებული თავდაპირველი ბალანსი. ეს ხელს უწყობს სამართლიანობის შენარჩუნებას და მონაცემთა გამოყენებისას ეთიკური სტანდარტების დაცვას.
- გამჭვირვალობა და ანგარიშვალდებულება: “GDPR” ხაზს უსვამს გამჭვირვალობასა და ანგარიშვალდებულებას. დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემები უნდა დაამუშაონ გამჭვირვალედ, მათ შორის, სუბიექტებს უნდა მიაწოდონ შესაბამისი ინფორმაცია სინთეზური მონაცემის გამოყენების და კონფიდენციალობის დაცვის ზომების შესახებ. აღნიშნული კომუნიკაცია უნდა იყოს მკაფიო და საჭიროების შემთხვევაში უნდა მოხდეს “DPIA”-ს გამოქვეყნებაც.

რეკომენდაცია: სინთეზური მონაცემების გენერირებაში ჩართულმა პრაქტიკოსებმა უნდა შექმნან სამართლებრივი საფუძველი და განსაზღვრონ ანონიმიზაციის მკაფიო მიზანი, დაიცვან “GDPR”-ის მოთხოვნები. მიზანშეწონილია ჩატარდეს რეგულარული აუდიტი და უწყვეტი მონიტორინგი, მონაცემთა დაცვაზე ზეგავლენის შეფასების (“DPIA”) განახლებებთან ერთად, ტექნოლოგიურ და მარეგულირებელ ცვლილებებთან შესაბამისად. “DPIA”-მ, რომელიც სავალდებულოა “GDPR”-ის 35-ე მუხლით, უნდა შეაფასოს რისკები და გამოკვეთოს მათი შემცირების სტრატეგია.

გარდა ამისა, სინთეზური მონაცემების პრაქტიკის საერთაშორისო სტანდარტებთან გათანაბრებას (“ISO/IEC 27001” და სერტიფიკატების მიღება, როგორიცაა “Europrivacy™/®”), შეუძლია გააძლიეროს შესაბამისობის სანდოობა. “Europrivacy™/®” აღიარებულია ევროკავშირისა და EEA-ს წევრ ქვეყნებში, აფასებს “GDPR”-ის შესაბამისობას და იმართება სერტიფიკაციისა და კონფიდენციალობის ევროპული ცენტრის მიერ (“ECCP”), იცავს “ISO/IEC 17065”-სა და “GDPR”-ის 42-ე მუხლს. ეს მიდგომა ხელს უწყობს სინთეზურ მონაცემთა გამოყენებისას სამართლებრივი და ეთიკური ნორმების დაცვას.

5. დასკვნა

მონაცემთა უსაფრთხოების და კონფიდენციალობის რისკების ზრდის პერიოდში, სინთეზური მონაცემის გენერირება წარმოადგენს ანონიმიზაციის სტრატეგიას. ნაშრომში საფუძვლიანად შეფასდა სინთეზური მონაცემები არაერთი

⁵³ See Aindo’s entry in the Europrivacy/registry:

<<https://repository.europrivacy.org/en/certifications/edit/d9064da7-603a-4377-b596-b654824e365f>> [30.07.2024].

თვალსაზრისით, კერძოდ იურიდიული, თეორიული და პრაქტიკული. აღნიშნული ხაზს უსვამს სინთეზური მონაცემის, როგორც კონფიდენციალობის გამაძლიერებელი ტექნოლოგიის ("PET"), ეფექტურობას. კვლევის შედეგი ადასტურებს, რომ სინთეზური მონაცემის სწორი გენერაციის პირობებში დაცულია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ ("GDPR") და სხვა მსგავსი კანონმდებლობით აღიარებული ანონიმიზაციის მკაცრი კრიტერიუმები.

მონაცემების ისეთ მდგომარეობამდე მიყვანა, როდესაც ინდივიდის იდენტიფიცირება შეუძლებელი ხდება კრიტიკულად მნიშვნელოვანია, რადგან ანონიმიზაციის ტრადიციული ტექნიკები „ხელახალი იდენტიფიკაციის“ ("re-identification") ახალ მეტად დახვეწილ საშუალებებს ვერ უმკლავდებიან. სინთეზური მონაცემები, ხელოვნური მონაცემთა ნაკრების შექმნით, გვთავაზობს პრობლემის გადაჭრის თანამედროვე გზას. მონაცემთა ნაკრები ასახავს რეალური მონაცემების სტატისტიკურ ნიმუშებს, რომელიც გამორიცხავს მათ კონკრეტულ პიროვნებასთან დაკავშირების ან/და იდენტიფიცირების საშუალებას. აღნიშნული გზით ერთის მხრივ დაცულია კონფიდენციალობა, ხოლო მეორეს მხრივ, შესაძლებელია მონაცემების გამოყენება მონაცემთა მეცნიერებისა და ხელოვნური ინტელექტის განვითარებისთვის.

სინთეზური მონაცემის, როგორც ანონიმიზაციის საშუალების, საკანონმდებლო დონეზე აღიარება სულ უფრო და უფრო პოპულარული ხდება. ესპანეთის და საფრანგეთის მონაცემთა დაცვის სამსახურებმა, ასევე ევროკავშირის გაერთიანებულმა კვლევითმა ცენტრმა სინთეზური მონაცემები ანონიმიზაციის ერთ-ერთ საშუალებად უკვე აღიარა. ამასთან სინთეზური მონაცემის მნიშვნელობას კიდევ უფრო ზრდის ისეთი სერტიფიკატები, როგორიცაა "Europrivacy™/®", რომელიც ადასტურებს, რომ სინთეზური მონაცემის გამოყენება შეესაბამება "GDPR"-სა და სხვა მარეგულირებელ კანონმდებლობას.

მიუხედავად ზემოაღნიშნულისა, სინთეზურ მონაცემთა გენერირება მეტად საფრთხილოა. მნიშვნელოვანია მკაცრად შეფასდეს ისეთი ფაქტორები, როგორიცაა გენერატორის ხარისხი, სინთეზის მეთოდოლოგია, მონაცემთა წყაროს მახასიათებლები და გაბატონებული საფრთხის მოდელი. კონფიდენციალობის შესაფასებლად რაოდენობრივი მეთოდების გამოყენება და გაერთიანებული მიდგომის მიღება, რომელიც აერთიანებს მონაცემებზე და გენერატორზე დაფუძნებულ კონფიდენციალობის სტრატეგიებს, სასიცოცხლოდ მნიშვნელოვანია პოტენციური რისკების ეფექტურად შესამცირებლად. გარდა ამისა, აუცილებელია გენერატორების სწავლების დროს მონაცემთა დაცვის კანონმდებლობის დაცვა და კონფიდენციალობის ემპირიულ შეფასებებში კონტროლის ჯგუფების ჩართვა.

მოსალოდნელია, რომ მონაცემთა ანონიმიზაციის სფერო განვითარდება მოწინავე ტექნოლოგიების გამოყენებით, ასევე, მკაცრი სამართლებრივი რეგულაციებითა და დეტალური ემპირიული რისკის შეფასებებით. აღნიშნული ნაშრომი ხაზს უსვამს, სწორი და სტრატეგიული გამოყენების პირობებში სინთეზური მონაცემების დიდ პოტენციალს ციფრულ სამყაროში მონაცემთა კონფიდენციალობის გამოწვევების დასაძლევად.

ბიბლიოგრაფია:

1. European Commission, “Regulation of the European Parliament and of the Council: on European Data Governance (Data Governance Act)”.
2. European Commission, “Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT) and Amending Certain Union Legislative Acts”.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
4. *Agencia Española de Protección de Datos (AEDP)*, “Approach To Data Spaces From GDPR Perspective”, 2023.
5. *Agencia Española de Protección de Datos (AEDP) and European Data Protection Supervisor (EDPS)*, 10 Misunderstanding related to Anonymization, 2021.
6. *Barth-Jones D.*, The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now, 2012.
7. *Beduschi A.*, Synthetic Data Protection: Towards a Paradigm Change in Data Regulation? *Big Data & Society*, 11(1), 2024.
8. *Bellovin Steven M., Dutta, Preetam K., Reitering N.*, Privacy and Synthetic Datasets, *Stanford Technology Law Review*, Vol. 22, 2018.
9. *D’Acquisto G., Naldi M.*, Big Data e Privacy by Design, Anonimizzazione, Pseudonimizzazione, Sicurezza, Giappichelli, 2017.
10. *De Montjoye Y. A., Hidalgo C. A., Verleysen M., Blondel V. D.*, Unique in the Crowd: The Privacy Bounds of Human Mobility, *Scientific Reports*, 3(1), 2013, 1-5.
11. *Dwork C., Roth A.*, The Algorithmic Foundations of Differential Privacy, *Foundations and Trends in Theoretical Computer Science*, 9(3–4), 2014, 211-407.
12. *Finocchiaro G., Landi A., Polifronei G., Ruffo D., Torlontano F.*, Il Futuro Regolatorio Dei Dati Sintetici. La Sintetizzazione dei Dati Come Risorsa per Ricerca Scientifica, Innovazione e Politiche Pubbliche nel Panorama Giuridico Europeo, 2024.
13. *Foglia C.*, Il Dilemma (ancora aperto) dell’Anonimizzazione e il Ruolo della Pseudonimizzazione nel GDPR, in *Circolazione e Protezione dei Dati Personali*, tra Libertà e Regole del Mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al Novellato d.lgs. n. 196/2003 (Codice Privacy), 2019.
14. *Giomi M., Boenisch F., Wehmeyer C., Tasnádi B.*, A Unified Framework for Quantifying Privacy Risk in Synthetic Data, 2022.
15. *Hern A.*, New York Taxi Details Can Be Extracted from Anonymised Data, Researchers Say, *The Guardian*, 2014.
16. *Hradec J., Craglia M., Di Leo M., De Nigris S., Ostlaender N., Nicholson N.*, Multipurpose Synthetic Population for Policy Applications, JRC Technical Report, 2022.
17. *Hu J., Bowen C.M.*, Advancing Microdata Privacy Protection: A Review of Synthetic Data, 2023.
18. *Information Commissioner’s Office (ICO)*, “Anonymisation: Managing Data Protection Risk Code of Practice”, 2012.

19. *Jordon J., Jarrett D., Saveliev E., Yoon J., Elbers P., Thorat P., van der Schaar M.*, Hide-and-Seek Privacy Challenge: Synthetic Data Generation vs. Patient Re-Identification, In NeurIPS 2020 Competition and Demonstration Track, 2021.
20. *Jordon J., Szpruch L., Houssiau F., Bottarelli M., Cherubin G., Maple C., Weller A.*, Synthetic Data-What, Why and How? 2022.
21. *Kaabachi B., Despraz J., Meurers T., Otte K., Halilovic M., Prasser F., Raisaro J. L.*, Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics, 2023.
22. *Lee J., Clifton C.*, How Much is Enough? Choosing ϵ for Differential Privacy, In Information Security: 14th International Conference, ISC 2011, Proceedings 14, Springer Berlin Heidelberg, 2011, 325-340.
23. *López C.A.F., Elbi A.*, On The Legal Nature of Synthetic Data, NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research, 2022.
24. *Narayanan A., Shmatikov V.*, How to Break Anonymity of the Netflix Prize Dataset, 2006.
25. *OECD*, "Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches," OECD Digital Economy Papers (OECD, 2023).
26. *Panfilo D., Boudewijn A. T., Ferraris A. F., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R.*, Measuring Privacy Protection in Structured Synthetic Datasets: A Survey, in: Hideyuki Matsumi, Paul De Hert et al. (ed) Privacy and Data Protection: Ideas that Drive Our Digital World, 2024.
27. *Platzer M., Reutterer T.*, Holdout-Based Empirical Assessment of Mixed-Type Synthetic Data, Frontiers in Big Data, 4, 2021.
28. *Stalla-Bourdillon S., Knight A.*, Anonymous Data v. Personal Data-False Debate: an EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Journal, 2017.
29. *Task C., Bhagat K., Howarth G.*, SDNist v2: Deidentified Data Report Tool, 2023, <<https://data.nist.gov/od/id/mds2-2943>> [30.07.2024].
30. *Tempestini L., D'Acquisto G.*, Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dei dati sensibili, in Le nuove frontiere della privacy nelle tecnologie digitali, Aracne, 2016.
31. *Wiewiórowski W.*, Synthetic Data: What Use Cases as Privacy Enhancing Technology? IPEN Webinar on synthetic data, European Data Protection Supervisor.

ელექტრონული სანოტარო რეესტრი და მონაცემთა უსაფრთხოება

2024 წლის პირველი მარტიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ამოქმედებასთან ერთად განსაკუთრებული მნიშვნელობა შეიძინა მონაცემთა ბაზების მართვისა და უსაფრთხოების განახლებულმა წესებმა. საკანონმდებლო და ინსტიტუციურმა სიახლეებმა გამოკვეთა ელექტრონული სანოტარო რეესტრის ფუნქციონირების შესწავლის საჭიროება, რათა გაირკვეს, რა ვალდებულება ეკისრება ნოტარიუსს მონაცემთა დამუშავებისას და რა შედეგს იწვევს, ნოტარიუსისთვის მონაცემთა უსაფრთხოების წესების დარღვევა.

საკვანძო სიტყვები: პერსონალურ მონაცემთა დაცვის სამსახური, ელექტრონული სანოტარო რეესტრი, საქართველოს ნოტარიუსთა პალატა, ნოტარიუსი, მონაცემთა უსაფრთხოება.

1. შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალმა კანონმა საქართველოში მონაცემთა დაცვის მნიშვნელოვანი, ევროკავშირის მონაცემთა დაცვის ძირითად რეგულაციასთან შესაბამისი სამართლებრივი სისტემა დაამკვიდრა, რომელიც უზრუნველყოფს პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვას.¹

საქართველოს ნოტარიუსთა პალატა, როგორც საჯარო სამართლის პირი, რომელიც თვითმმართველობის პრინციპით აგებული ნოტარიუსების გაერთიანებაა და ემყარება ნოტარიუსთა სავალდებულო წევრობას,² კანონის სიახლეების წინა ხაზზე აღმოჩნდა. გამომდინარე იქედან, რომ ელექტრონული სანოტარო რეესტრი ნოტარიუსთა პალატასა და ნოტარიუსებს პერსონალური მონაცემების კონკრეტული

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასოცირებული პროფესორი, სამართლის დოქტორი, სანოტარო სამართლის სამეცნიერო-კვლევითი ინსტიტუტის დირექტორი, საქართველოს ნოტარიუსი.

** ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის მკვლევარ-ანალიტიკოსი.

¹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, პირველი მუხლი. ასევე, იხ. ბერნსდორფი ნ., ევროპის კავშირის „მონაცემთა დაცვის სამართალი“, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №2, 2023, 14-15.

² საქართველოს კანონი „ნოტარიატის შესახებ“, 04/12/2009, მე-4 მუხლი.

მიზნით დამუშავების შესაძლებლობას ანიჭებს, იგი სანოტარო მომსახურების განუყოფელ ნაწილად მიიჩნევა და უნდა აკმაყოფილებდეს მონაცემთა უსაფრთხოების მოთხოვნებს.

კვლევის მიზანია, შეფასდეს პირობები, რომელთა საფუძველზეც ელექტრონულ სანოტარო რეესტრში მუშავდება ფიზიკურ პირთა პერსონალური მონაცემები, დადგინდეს მისი შესაბამისობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნებთან და განხილულ იქნეს ევროკავშირის ნოტარიუსთა საბჭოს წევრი ქვეყნების სანოტარო რეესტრების წარმოების სიახლეები.

2. ელექტრონული სანოტარო რეესტრის ტიპები

ნოტარიუსი ვალდებულია აწარმოოს სანოტარო რეესტრი, რომელშიც რეგისტრირდება შესრულებული სანოტარო მოქმედებები.³ რეესტრი სანოტარო მოქმედების მიმღებ მოქალაქეთა პერსონალური მონაცემების ბაზაა და აერთიანებს ღია და დახურული ტიპის შიდა სისტემებს.⁴ ნოტარიუსი პროფესიული საქმიანობის განხორციელებისას, მოქალაქეთა პერსონალურ მონაცემებს ამუშავებს მონაცემთა დამუშავების პრინციპების და საფუძვლების დაცვით, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს და არასრულწლოვნის პერსონალურ მონაცემებს.

ღია ტიპის შიდა სისტემის ფუნქცია ნოტარიუსებს სანოტარო მოქმედებებთან დაკავშირებული სუბიექტების მონაცემებზე წვდომის შესაძლებლობას ანიჭებს. მასში რეგისტრირებულ სანოტარო მოქმედებებთან წვდომა აქვს ყველა ნოტარიუსს, მიუხედავად იმისა, თუ ვინ განახორციელა მოქმედება რეესტრში, ეს არის:

- სამემკვიდრეო საქმეთა რეესტრი;
- ანდერძების რეესტრი;
- სააღსრულებო ფურცლის შესახებ ინფორმაცია საერთო რეესტრიდან.

სამემკვიდრეო საქმეთა რეესტრის ღიაობა იმითაა განპირობებული, რომ სამკვიდროზე ორი სხვადასხვა ნოტარიუსის მიერ არ გაიცეს მსგავსი შინაარსის სამკვიდრო მოწმობები. ნოტარიუსმა არ გახსნას სამკვიდრო კანონისმიერ მემკვიდრეებზე, თუ სხვა ნოტარიუსთან უკვე ინახება მამკვიდრებლის ანდერძი. ასევე, უძრავ ქონებაზე არ გაიცეს ილენტური შინაარსის რამდენიმე სააღსრულებო ფურცელი და ა.შ.

დახურული ტიპის შიდა სისტემაში რეგისტრირებულ სანოტარო მოქმედებებთან წვდომა გააჩნია მხოლოდ იმ ნოტარიუსს, რომელმაც განახორციელა მოქმედება რეესტრში, ეს არის:

- საერთო რეესტრი, სადაც რეგისტრირდება ყველა სანოტარო მოქმედება, გარდა უკვე აღნიშნული მოქმედებებისა;
- თამასუქებისა და ჩეკების გაპროტესტების რეესტრი;
- ფულისა და ფასიანი ქაღალდების რეესტრი;
- დადგენილებათა რეესტრი.

განხილვის საგანია, თუ რა ფორმით უნდა იყოს ხელმისაწვდომი ღია ტიპის შიდა სისტემაში დაცული მონაცემები სხვა ნოტარიუსებისთვის, მათ შორის, სანოტარო

³ შეად. European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 7.

⁴ საქართველოს იუსტიციის მინისტრის ბრძანება „სანოტარო მოქმედებათა შესრულების წესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“, 31/03/2010, 33-ე მუხლი.

საქმიანობის ფარგლებს გარეთ, საჯარო დაწესებულებებისთვის: მაგალითად, საჯარო რეესტრისთვის. ერთი მხრივ, ნოტარიუსს ეკისრება პროფესიული საიდუმლოების დაცვის ვალდებულება, თუმცა, მეორე მხრივ, მის მიერ განხორციელებული მოქმედებების (შედეგების) ნაწილი ხელმისაწვდომია კოლეგა ნოტარიუსებისთვის და რეესტრთან კავშირში მყოფი სხვა პირებისთვის. მაგალითად, ნოტარიუსს, სხვა პირს, რომელმაც დაადასტურა ანდერძი, მოწმეს, ასევე პირებს, რომლებმაც ხელი მოაწერეს ანდერძს მოანდერძის ნაცვლად, უფლება არა აქვთ სამკვიდროს გახსნამდე გაამხილონ ცნობები, რომლებიც შეეხება ანდერძის შინაარსს, მის შედგენას, შეცვლას ან გაუქმებას,⁵ თუმცა ამ ცნობების/პერსონალური მონაცემების ელექტრონულ სანოტარო რეესტრში აღრიცხვა, შეიძლება ანდერძის შედგენის ფაქტის და შინაარსის გამჟღავნებას და მისი გაცნობის საშუალებას წარმოადგენდეს სხვა პირებისთვის.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლი ადგენს მონაცემთა უსაფრთხოების მოთხოვნებს. ეს მოთხოვნები პირობითი ხასიათისაა და მისი დაცვის მნიშვნელობას გამოხატავს, თუმცა სანოტარო საქმიანობის განხორციელებისას ამ პირობების დაცვა და დაუცველობის სამართლებრივი შედეგები გარკვეული თავისებურებით ხასიათდება. ზოგადად, თემის ირგვლივ შეიძლება გამოიყოს მონაცემთა უსაფრთხოების განახლებული მოწესრიგება, მონაცემთა უსაფრთხოების დარღვევაზე რეაგირების წესი და მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება.⁶

ახალი კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან უზრუნველყონ ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა. არაელექტრონული ფორმით არსებულ მონაცემთა დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან უზრუნველყონ მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ ინფორმაციის) აღრიცხვა.⁷ სანოტარო რეესტრთან მიმართებით ეს მოთხოვნა შეიძლება გავიგოთ, როგორც ზოგადად, რეესტრის სისტემური გამართულობისთვის პასუხისმგებლობის ნაწილში, ასევე, კონკრეტულად, სანოტარო მოქმედების განხორციელებისას.⁸

სანოტარო რეესტრში სანოტარო მოქმედების განსახორციელებლად სავალდებულოა მიეთითოს სხვადასხვა მონაცემი:

- სანოტარო მოქმედების რეგისტრაციის თარიღი და ნომერი;

⁵ საქართველოს სამოქალაქო კოდექსი, 26/06/1997, 1363-ე მუხლი.

⁶ მონაცემთა ბაზების განვითარებასთან დაკავშირებით იხ.: პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის 2022 წლის ანგარიში, 96; პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის 2023 წლის ანგარიში, 52-53.

⁷ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, 27-ე მუხლის მე-4 პუნქტი. ასევე, შეად. ჟუდარსკი ა., სირდაძე ლ., რეესტრის ჯუნგლები 21-ე საუკუნეში, მედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №6, 2020, 22.

⁸ იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაციები საჯარო დაწესებულებებისთვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან თავსებადობის მიზნით შიდაუწყებრივი სამართლებრივი აქტების გამოცემის/განახლების თაობაზე, 2023, 1-2.

- სანოტარო მოქმედების მონაწილის სახელი, გვარი, საცხოვრებელი ადგილი, პირადი ნომერი. არასრულწლოვანი ფიზიკური პირის შემთხვევაში, რომელსაც არ გააჩნია პირადობის დამადასტურებელი დოკუმენტი: სახელი, გვარი, დაბადების თარიღი. იურიდიული პირის შემთხვევაში: სახელწოდება, იურიდიული მისამართი, ხოლო რეზიდენტი იურიდიული პირის შემთხვევაში საიდენტიფიკაციო კოდი. სხვა ორგანიზაციული წარმონაქმნის შემთხვევაში: სახელწოდება და ადგილსამყოფელი.
- სანოტარო მოქმედების შინაარსი;
- სანოტარო საზღაური.

სამემკვიდრეო საქმისწარმოებისას, დამატებით მიეთითება მამკვიდრებლის ვინაობა, გარდაცვალების თარიღი და საიდენტიფიკაციო მონაცემი. ანდერძის გამოქვეყნების შესახებ ოქმის რეგისტრაციისას: საანდერძო განკარგულების შინაარსი, ანდერძით მემკვიდრის ან სათაღარიგო მემკვიდრის იდენტიფიკაციის მონაცემი, ანდერძით დანიშნული ანდერძის აღმსრულებლის სახელი და გვარი, საცხოვრებელი ადგილი, იდენტიფიკაციის სხვა მონაცემი, იმ პირის სახელი და გვარი, იდენტიფიკაციის მონაცემი, რომელსაც ანდერძით დაევალი ანდერძის აღმსრულებლის დანიშვნა, ლეგატარის (მისი არსებობისას) მონაცემი.

როგორც ვხედავთ, სანოტარო რეესტრში მოქმედების დასარეგისტრირებლად მნიშვნელოვანია პერსონალური მონაცემების მითითება, თუმცა საჯარო და კერძო აქტების მიმართ მოქმედებს ნოტარიუსის პასუხისმგებლობის განსხვავებული სტანდარტი, შეიძლება კი მსგავსი რეგულირება გავავრცელოთ მონაცემთა დაცვის მოთხოვნათა მიმართაც? მაგალითად, ერთ მხარესაა ნოტარიუსის პროფესიული საიდუმლოების ან სანოტარო კანონმდებლობის დარღვევის სამართლებრივი შედეგი, ხოლო მეორე მხარეს მონაცემთა უსაფრთხოების დარღვევის სამართლებრივი შედეგი.

არ არის გამორიცხული, რომ მონაცემთა უსაფრთხოების დარღვევა განაპირობოს სანოტარო სფეროს ფარგლებს გარეთ მონაცემთა სუბიექტების, მათი წარმომადგენლების ან სხვა ნოტარიუსებისა და საჯარო დაწესებულების თანამშრომელთა მოქმედებამ ან მონაცემთა უსაფრთხოების დარღვევა აღიქმებოდეს ნოტარიუსის პროფესიული პასუხისმგებლობის ნაწილად. მაგალითად, სხვა საჯარო დაწესებულებაში სანოტარო აქტის რეკვიზიტების გასაჯაროებით საფრთხე ექმნება მონაცემთა უსაფრთხოებას. ამ შემთხვევაში ნოტარიუსი ხელმძღვანელობს სანოტარო კანონმდებლობით, შესაბამისად, მონაცემთა უსაფრთხოების დაცვის საკითხები უკავშირდება ნოტარიუსის საქმიანობას, უფრო კონკრეტულად, საჯარო და კერძო აქტების ფორმებს,⁹ აქ კი, მნიშვნელოვანია, ერთიანი სტანდარტის დამკვიდრება მონაცემთა უსაფრთხოების მიზნებისთვის.

იქნება ეს საჯარო თუ კერძო აქტი ნოტარიუსმა საერთო წესის დაცვით უნდა განახორციელოს მოქმედებები მონაცემთა უსაფრთხოებისთვის, მაგრამ თუ მას სანოტარო რეესტრი საჯარო და კერძო აქტებთან დაკავშირებით საერთო სტანდარტის დამკვიდრების საშუალებას არ აძლევს, როგორ უნდა იმოქმედოს ამ შემთხვევაში?

ნოტარიუსს არ ეკისრება პასუხისმგებლობა კერძო აქტის კანონმდებლობასთან შეუსაბამობის ან კერძო აქტში ხელმოწერის ნების არაადეკვატურად ასახვის გამო.¹⁰

⁹ საქართველოს იუსტიციის მინისტრის ბრძანება „სანოტარო მოქმედებათა შესრულების წესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“, 31/03/2010, მე-15 მუხლი.

¹⁰ იქვე.

ნოტარიუსი (შემცვლელი პირი) ჩაიდენს მძიმე დისციპლინურ გადაცდომას, თუ დაარღვევს პროფესიული საიდუმლოების დაცვის ვალდებულებას, გარდა დისციპლინური დებულების მე-7 მუხლის „ბ“ ქვეპუნქტით გათვალისწინებული შემთხვევებისა,¹¹ რომელიც მიუთითებს, რომ განსაკუთრებით მძიმე დისციპლინურ გადაცდომად ითვლება პროფესიული საიდუმლოების დაცვის ვალდებულების დარღვევა, რასაც მძიმე შედეგი მოჰყვა. შესაბამისად, ნოტარიუსის მიერ მონაცემთა უსაფრთხოების წესის დარღვევა შეიძლება არ იწვევდეს მისთვის პროფესიული პასუხისმგებლობის დაკისრებას, რაც ბუნებრივად უნდა მივიჩნიოთ.

აღსანიშნავია, რომ საჯარო დაწესებულებებს დაევალებათ მათი საქმიანობის მარეგულირებელ კანონქვემდებარე ნორმატიულ აქტებსა და ინდივიდუალურ სამართლებრივ აქტებში მონაცემთა დამუშავებასთან დაკავშირებული ტერმინების ახალ კანონთან შესაბამისობაში მოყვანა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ამოქმედების დროისთვის.¹² 2024 წლის პირველი ივნისიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი სრულად ამოქმედდა.

3. ელექტრონული სანოტარო რეესტრის წარმოება და მონაცემთა უსაფრთხოება

ბათილია სანოტარო მოქმედება, რომელიც არ არის რეგისტრირებული სანოტარო რეესტრში, გარდა კანონით დადგენილი რამდენიმე საგამონაკლისო შემთხვევისა.¹³ ყოველ სანოტარო მოქმედებას ენიჭება ნომერი და რეგისტრირდება დოკუმენტზე ნოტარიუსის ხელმოწერისა და ბეჭდის დასმისთანავე.¹⁴ სანოტარო რეესტრში ჩანაწერს ასრულებს ნოტარიუსი ან მისი დავალებით სანოტარო ბიუროს თანამშრომელი, რომელსაც ნოტარიუსთან წერილობითი ხელშეკრულებით ნაკისრი აქვს სანოტარო მოქმედების საიდუმლოების დაცვის ვალდებულება. ასევე, ნოტარიუსის შემცვლელი პირი.¹⁵

სანოტარო რეესტრში რეგისტრაციისას ნოტარიუსის მიერ შესრულებულ სანოტარო მოქმედებას უნდა დაერთოს სანოტარო აქტის დედნის ელექტრონული ასლი.¹⁶

ელექტრონული სანოტარო რეესტრის ადმინისტრირებას და ტექნიკურ მეთვალყურეობას საქართველოს ნოტარიუსთა პალატა უზრუნველყოფს. პირები, რომლებიც სანოტარო რეესტრის ადმინისტრირებას და ტექნიკურ მეთვალყურეობას ახორციელებენ, საქართველოს ნოტარიუსთა პალატასთან გაფორმებული ხელშეკრულებით, მოვალენი არიან დაიცვან მონაცემთა დამუშავების პროცესში

¹¹ იხ. საქართველოს იუსტიციის მინისტრის №69-ე ბრძანება „ნოტარიუსთა დისციპლინური პასუხისმგებლობის შესახებ“ დებულების დამტკიცების თაობაზე, 31/03/2010.

¹² პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაციები საჯარო დაწესებულებებისთვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან თავსებადობის მიზნით შიდაუწყებრივი სამართლებრივი აქტების გამოცემის/განახლების თაობაზე, 2023, 2.

¹³ იხ. *ხარიტონაშვილი ნ.*, კონფერენცია „გერმანული და ქართული ნოტარიატის გაციფრულება“, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №4, 2023, 88-89.

¹⁴ შეად. European Judicial Systems Efficiency and Quality of Justice, Specific Study of the CEPEJ, Council of Europe, №26, 2018, 220.

¹⁵ საქართველოს კანონი „ნოტარიატის შესახებ“, 04/12/2009, 24-ე მუხლი.

¹⁶ შეად. *ხარიტონაშვილი ნ.*, ქართული ნოტარიატის გაციფრულება, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №6, 2023, 149.

მიღებული ინფორმაციის კონფიდენციალურობა და ეკისრებათ პასუხისმგებლობა სანოტარო საიდუმლოების გახმაურებისათვის.¹⁷

შედარებისთვის, ბელგიის მონაცემთა დაცვის საზედამხებდველო ორგანომ ერთ-ერთ საქმეზე აღნიშნა, რომ ნოტარიუსის, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ ფიზიკური პირის პერსონალური მონაცემების შეცდომით სხვა პირების ელექტრონულ ფოსტაზე გაგზავნა და შემდგომ, შეტყობინებების უკან გამოხმობა მონაცემთა უსაფრთხოების დარღვევაა და არა მონაცემთა დამუშავების ტექნიკური ხარვეზი.¹⁸

ნოტარიუსი ან ნოტარიუსის შემცვლელი პირი სანოტარო რეესტრთან დაშვების ავტორიზაციის მოთხოვნით მიმართავს საქართველოს ნოტარიუსთა პალატას. ნოტარიუსზე ან ნოტარიუსის შემცვლელ პირზე საქართველოს ნოტარიუსთა პალატა გასცემს სანოტარო რეესტრთან დაშვების ავტორიზაციას, შეაჩერებს ან შეწყვეტს სანოტარო რეესტრთან დაშვების ავტორიზაციას მათი უფლებამოსილების შეჩერების ან შეწყვეტის შემთხვევაში. პალატა უზრუნველყოფს სანოტარო რეესტრის მონაცემების უსაფრთხოებას და დაცვას, მათ შორის ნოტარიუსების (შემცვლელი პირების) და მათი დაქირავებული თანამშრომლების გადამზადებას სანოტარო რეესტრთან მუშაობის საკითხებზე და ამტკიცებს სანოტარო რეესტრის წარმოების ტექნიკურ ინსტრუქციას.¹⁹ აღნიშნული საკანონმდებლო მოთხოვნაა, თუმცა პრაქტიკულად ეს შეიძლება სხვაგვარად გამოიხატებოდეს. საქართველოს ნოტარიუსთა პალატა და ნოტარიუსები ერთმანეთთან თანამშრომლობისას კონკრეტული შემთხვევების გათვალისწინებით შეიძლება განვიხილოთ, როგორც თანადამუშავებისთვის პასუხისმგებელი პირები,²⁰ დამუშავებისთვის პასუხისმგებელი პირები და დამუშავებაზე უფლებამოსილი პირები, იმის მიხედვით, თუ როგორ განისაზღვრება დამუშავების მიზნები და საფუძვლები აღნიშნული დაწესებულების/პირთა მიერ. ისიც უნდა აღინიშნოს, რომ ცალკე აღებული ნოტარიუსი ძირითადად, დამუშავებისთვის პასუხისმგებელი პირია, თუმცა შეიძლება შეითავსოს შედარებით, მცირე შემთხვევებში დამუშავებაზე უფლებამოსილი პირის სტატუსი ნოტარიუსთა პალატასთან ან სხვა საჯარო დაწესებულებასთან ურთიერთობისას. მაგალითად, ნოტარიუსსა და სსიპ - საჯარო რეესტრის ეროვნული სააგენტოს შორის გაფორმებული ხელშეკრულებით ნოტარიუსს ენიჭება დამუშავებაზე უფლებამოსილი პირის, ხოლო საჯარო რეესტრს დამუშავებისთვის პასუხისმგებელი პირის სტატუსი. ამ შემთხვევაში, ნოტარიუსის, როგორც პერსონალური მონაცემების დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემების დამუშავების მიზანია მხარისთვის სააგენტოს მიერ დელეგირებული უფლებამოსილების განხორციელება, ნოტარიუსი ვალდებულია დაამუშაოს მონაცემები მხოლოდ მხარეებს შორის დადებული ხელშეკრულებით და კანონმდებლობით გათვალისწინებულ ფარგლებში. რაც შეეხება სანოტარო რეესტრს, ნოტარიუსი მას საკუთარი სახელით მართავს და რეესტრში

¹⁷ იხ.: პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, 2024, 29; პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „ინციდენტთან დაკავშირებული ღონისძიებების განხორციელების თაობაზე“, 2024, 5-6.

¹⁸ Case of the Data Protection Authority (Belgium) №52, 03/04/2024.

¹⁹ შეად. ასვანუა ნ., პერსონალურ მონაცემთა დაცვის მექანიზმები, თბ., 2023, 39-40.

²⁰ შეად. Kuner C., Bygrave L. A., Docksey C., The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 25-27.

დამოუკიდებლად ამუშავენ ფიზიკურ პირთა მონაცემებს, ამიტომ სანოტარო რეესტრთან მიმართებით ნოტარიუსი დამუშავებისთვის პასუხისმგებელი პირია.

ნოტარიუსების შემცვლელი პირები, შრომითი ხელშეკრულებით დასაქმებული ნოტარიუსები და ნოტარიუსის თანამშრომლები ნოტარიუსთან შრომით ურთიერთობაში არიან, ამიტომ, ისინი არ არიან დამუშავებაზე უფლებამოსილი პირები, რადგან უფლებამოსილი პირი პასუხისმგებელ პირთან შრომით ურთიერთობაში არ უნდა იყოს.²¹ ისინი არც დამუშავებისთვის პასუხისმგებელი პირები არიან, არამედ, დამატებით უზრუნველყოფენ სანოტარო მოქმედების უწყვეტობას და წარმოადგენენ სანოტარო ბიუროს პერსონალს.²² ამ შემთხვევაში, წამყვანი სტატუსი სანოტარო ბიუროში ნოტარიუსს აქვს.

შედარებისთვის, პოლონეთის მონაცემთა დაცვის საზედამხებელო ორგანომ განმარტა, რომ სანოტარო საქმიანობის განხორციელებისას ნოტარიუსი შეიძლება მონაცემთა დამუშავებაზე უფლებამოსილი პირიც იყოს, თუ მას ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 28-ე მუხლით გათვალისწინებული ხელშეკრულება ექნება გაფორმებული მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთან.²³

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მიხედვით, საქართველოს ნოტარიუსთა პალატა, როგორც საჯარო დაწესებულება ვალდებულია ჰყავდეს პერსონალურ მონაცემთა დაცვის ოფიცერი.²⁴ გამომდინარე იქედან, რომ საქართველოს ზოგადი ადმინისტრაციული კოდექსის 27-ე მუხლის „ა“ პუნქტის თანახმად, საჯარო დაწესებულებად მიიჩნევა ადმინისტრაციული ორგანო, სახელმწიფო ან მუნიციპალური ბიუჯეტის სახსრებიდან დაფინანსებული კერძო სამართლის იურიდიული პირი ასეთი დაფინანსების ფარგლებში და ამავე კოდექსის ტერმინთა განმარტებაში ადმინისტრაციული ორგანო განიმარტება, როგორც ყველა სახელმწიფო ან მუნიციპალიტეტის ორგანო/დაწესებულება, საჯარო სამართლის იურიდიული პირი (გარდა პოლიტიკური და რელიგიური გაერთიანებებისა), აგრეთვე ნებისმიერი სხვა პირი, რომელიც საქართველოს კანონმდებლობის საფუძველზე ასრულებს საჯარო სამართლებრივ უფლებამოსილებებს. ე.ი. საქართველოს ნოტარიუსთა პალატა, როგორც საჯარო სამართლის იურიდიული პირი, ამ ნორმების სიტყვასიტყვითი განმარტებით გვევლინება საჯარო დაწესებულებად და უდავოა, რომ მას უნდა ჰყავდეს მონაცემთა დაცვის ოფიცერი. რასაც ვერ ვიტყვით ინდივიდუალურად, ნოტარიუსის შესახებ, რადგან აღნიშნული ნორმების სიტყვასიტყვითი განმარტებით ნოტარიუსი არ შეიძლება ჩაითვალოს საჯარო დაწესებულებად, თუმცა ის ახორციელებს სახელმწიფოებრივ უფლებამოსილებას.

აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი, რომელიც ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ვალდებული არიან დანიშნონ ან განსაზღვრონ პერსონალურ

²¹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მე-3 მუხლის „ჟ“ პუნქტი.

²² შეად. European Commission for the Efficiency of Justice, Study on the Functioning of Judicial Systems in the EU Member States, Specific Study on the Facts and Figures from the CEPEJ Questionnaires 2012 to 2020, Strasbourg, 2022, 899-900.

²³ Case of the Data Protection Authority (Poland) №DKN.5131.31.2021, 07.02.2023.

²⁴ იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაციები საჯარო დაწესებულებებისთვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან თავსებადობის მიზნით შიდაუწყებრივი სამართლებრივი აქტების გამოცემის/განახლების თაობაზე, 2023, 14.

მონაცემთა დაცვის ოფიცერი. ოფიცერის დანიშვნა/განსაზღვრა არ ევალუება პირს, რომელიც ამუშავებს საქართველოს მოსახლეობის არაუმეტეს 3 პროცენტის პერსონალურ მონაცემებს, საყოველთაო აღწერის ბოლო შედეგების მიხედვით. ზოგად სტატისტიკურ ინფორმაციას თუ გადავხედავთ ცალკე აღებული ნოტარიუსი საანგარიშო წლის განმავლობაში საქართველოს მოსახლეობის 3 პროცენტზე მეტი რაოდენობის პერსონალურ მონაცემებს ვერ ამუშავებს. ამიტომ, ამ პირობითაც არ ევალუება ნოტარიუსს ოფიცერის დანიშვნა/განსაზღვრა. ეს არ ნიშნავს იმას, რომ რაოდენობრივი მაჩვენებლების ან ნორმის ცვლილების საფუძველზე ნოტარიუსს სამომავლოდ არ დაევალება ოფიცერის ნაწილის უზრუნველყოფა.

მონაცემთა უსაფრთხოების თვალსაზრისით, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა კანონის შესაბამისად დამუშავების უზრუნველსაყოფად და შეძლოს მონაცემთა დამუშავების კანონთან შესაბამისობის დადასტურება.²⁵ შესაბამისად, როგორც აღინიშნა, ამჟამად, ეს არ ავალდებულებს ნოტარიუსს, რომ სანოტარო ბიუროში ჰყავდეს მონაცემთა დაცვის ოფიცერი, რადგან შესაძლებელია, რომ პალატის ორგანიზაციულ ფარგლებში მოხდეს ამ საკითხის საერთო აღმინისტრირება.

ე.ი. ელექტრონულ სანოტარო რეესტრთან შემხებლობაში არიან:

- საქართველოს ნოტარიუსთა პალატა;
- პალატის მიერ რეესტრის მართვისთვის ხელშეკრულებით მიღებული პირები;
- პალატის პერსონალურ მონაცემთა დაცვის ოფიცერი;
- ნოტარიუსები;
- ნოტარიუსების შემცვლელი პირები;
- შრომითი ხელშეკრულებით დასაქმებული ნოტარიუსები;
- ნოტარიუსის თანამშემწეები.

მნიშვნელოვანია ყოველ კონკრეტულ შემთხვევაში განისაზღვროს მათი სტატუსი და ვალდებულებები „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის გათვალისწინებით, კერძოდ, ვინ შეიძლება მოიაზრებოდეს დამუშავებისთვის პასუხისმგებელ პირად, დამუშავებაზე უფლებამოსილ პირად ან თანადამუშავებისთვის პასუხისმგებელ პირად.²⁶

შედარებისთვის, ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი საქმის შესწავლისას დაადგინა, რომ ნოტარიუსმა სანოტარო მოქმედების განხორციელებისას ფიზიკურ პირს არ მიაწოდა ინფორმაცია საიდენტიფიკაციო მონაცემების დამუშავების მიზნის და მისთვის გადაცემულ მონაცემთა უსაფრთხოების დაცვის საშუალებების შესახებ. ნოტარიუსის განმარტებით, სანოტარო კანონმდებლობა მას არ ავალდებულებდა აღნიშნული ინფორმაციის გაცემას. საზედამხედველო ორგანომ ნოტარიუსი გააფრთხილა მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდების აუცილებლობის შესახებ მონაცემთა უშუალოდ მისგან შეგროვების შემთხვევაში, მიუხედავად იმისა, ავალდებულებს თუ არა მას აღნიშნულ შეტყობინებას სანოტარო კანონმდებლობა.²⁷

²⁵ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, პირველი პუნქტი.

²⁶ შეად. ელიზბარაშვილი ს., ადამიანის უფლებების დაცვა ტექნოლოგიური განვითარების ეპოქაში: ხელოვნური ინტელექტის რეგულირების დასაწყისი, სტატიათა კრებული - ადამიანის უფლებათა დაცვა: ევროპული გამოცდილება და ეროვნული გამოწვევები, თბ., 2023, 80-81.

²⁷ Case of the Data Protection Authority (Spain) №PS/00044, 23/10/2020.

სანოტარო კანონმდებლობა ნოტარიუსის პროფესიულ საქმიანობას არეგულირებს, რაც შეეხება მონაცემთა უსაფრთხოების საკითხს იგი გარე რეგულირების ფორმით აისახება სანოტარო საქმიანობაზე. სწორედ ასე შემოდის ახალი ტერმინები/სტატუსები,²⁸ რომლებიც შეიძლება მიიღოს ნოტარიუსმა მონაცემთა დამუშავებისას.

დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ნებისმიერი თანამშრომელი, რომელიც მონაწილეობს მონაცემთა დამუშავებაში ან რომელსაც აქვს მონაცემებზე წვდომა, ვალდებულია არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ.²⁹ დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან თანამშრომელთა უფლებამოსილებების შესაბამისად განსაზღვრონ მათი მონაცემებზე წვდომის ფარგლები და განახორციელონ ადეკვატური ღონისძიებები თანამშრომელთა მიერ მონაცემთა უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, მათ შორის, უზრუნველყონ თანამშრომელთა ინფორმირება მონაცემთა უსაფრთხოების დაცვის საკითხების შესახებ.³⁰ ყურადსაღებია ტექნიკური ინსტრუქცია, რომელიც შეიძლება ავალდებულებდეს კონკრეტულ პირებს ან ანიჭებდეს მათ უფლებამოსილებას რეესტრთან მუშაობის თვალსაზრისით. მიუხედავად იმისა, რომ ნოტარიუსები დამოუკიდებლად ახორციელებენ სახელმწიფოებრივ საქმიანობას საკუთარ სანოტარო ბიუროებში, მათ მიერ შესრულებული მოქმედებების შესახებ მონაცემები და მოქალაქეთა პერსონალური მონაცემები თავს იყრის ელექტრონულ სანოტარო რეესტრში. შესაბამისად, მიუხედავად იმისა, თუ რამდენად კანონშესაბამისად დაიცავს ცალკეული ნოტარიუსი მონაცემთა დაცვის კანონმდებლობას, ეს არ იქნება საკმარისი მონაცემთა უსაფრთხოების უზრუნველყოფისთვის.

შედარებისთვის, მონაცემთა უსაფრთხოების დარღვევასთან დაკავშირებულ ერთ-ერთ საქმეში, იტალიის მონაცემთა დაცვის საზედამხებველო ორგანოს მიმართა იტალიის ნოტარიუსთა პალატამ და სთხოვა შეესწავლა ელექტრონულ რეესტრში ფიზიკური პირების სასესიო ვალდებულებებთან დაკავშირებული მონაცემების დამუშავებისას კომერციული ბანკების და ნოტარიუსების სტატუსი, ვალდებულებები და პასუხისმგებლობა. საზედამხებველო ორგანომ დაადგინა, რომ მონაცემთა უსაფრთხოების დარღვევისთვის პასუხისმგებელი იყო ელექტრონული რეესტრის პროვაიდერი (მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი), რომელიც თვითნებურად ეცნობოდა და ამუშავებდა აღნიშნულ რეესტრში განთავსებულ მონაცემებს დამუშავებისთვის პასუხისმგებელი პირისთვის შეუტყობინებლად.³¹

ნოტარიუსი ვალდებულია დაიცვას სანოტარო რეესტრთან დაშვების მონაცემები.³² ყველა, ვისაც სხვადასხვა სამართლებრივი საფუძვლით მინიჭებული

²⁸ იხ.: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28/01/1981; General Data Protection Regulation (GDPR), 27/04/2016; Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), 18/06/2018.

²⁹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, 27-ე მუხლის მე-5 პუნქტი.

³⁰ იქვე, 27-ე მუხლის მე-6 პუნქტი.

³¹ Case of the Data Protection Authority (Italy) №9993548, 11/01/2024.

³² შეად. ზუბუა გ., სირდაძე ლ., სამართლის ტექნოლოგიები (ლიგალტექი) საქართველოში, მათი გამოყენება კერძო კომპანიებსა და საჯარო უწყებებში, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №7, 2022, 10.

აქვს სანოტარო რეესტრთან დაშვების უფლება, ვალდებულია საიდუმლოდ შეინახოს ინფორმაცია სანოტარო მოქმედებების შესახებ.³³ ვალდებულება ძალაში რჩება მას შემდეგაც, რაც ამ პირებს შეუწყდებათ სანოტარო რეესტრთან დაშვების უფლება.³⁴

დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან მიიღონ მონაცემთა დამუშავების შესაძლო და თანამდევნი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას მონაცემთა დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან.³⁵ ელექტრონული სანოტარო რეესტრის ინფორმაციული მთლიანობის შესანარჩუნებლად აუცილებელია მისი მართვისა და ფუნქციების სისტემატიზაცია.

შედარებისთვის, ბელგიის მონაცემთა დაცვის საზედამხებელო ორგანომ სხვა საქმეში აღნიშნა, რომ სანოტარო საქმიანობისას დამუშავებული პერსონალური მონაცემები, რომლებიც ინახება სანოტარო რეესტრში არ შეიძლება გადაეცეს მარეგისტრირებელ ორგანოს (სხვა საჯარო დაწესებულებას), თუ ეს მონაცემთა სუბიექტის სურვილიდან არ გამომდინარეობს.³⁶ წინააღმდეგ შემთხვევაში ნოტარიუსი დაარღვევს არა მხოლოდ მონაცემთა დაცვის კანონმდებლობას, ასევე, ეთიკურ ვალდებულებას.

მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან გაითვალისწინონ მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები, აგრეთვე პერიოდულად შეაფასონ მონაცემთა უსაფრთხოების უზრუნველსაყოფად მიღებული ტექნიკური და ორგანიზაციული ზომების ეფექტიანობა და, საჭიროების შემთხვევაში, უზრუნველყონ მონაცემთა უსაფრთხოების დასაცავად ადეკვატური ზომების მიღება ან/და არსებულის განახლება.³⁷

შეიძლება ითქვას, რომ ელექტრონული სანოტარო რეესტრის მოქმედი სისტემა ნაკლებად ითვალისწინებს თანამედროვე საინფორმაციო ტექნოლოგიების მიღწევებს, მათ შორის ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებას და პროფაილინგს.³⁸ სისტემა, ელექტრონული ფორმის მიუხედავად, სრულფასოვნად ვერ უზრუნველყოფს სანოტარო აქტის შედგენას, პროცესში

³³ შეად. პეტერფალვი ა., ესტერი დ., როდესაც ჩვენი მანქანები გვსწავლობენ: ევროპის კავშირის მცდელობები ხელოვნური ინტელექტის საფუძველზე გადაწყვეტილების მიღებისა და პროფილირების რეგულირებასთან დაკავშირებით, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2023, 72-74.

³⁴ ევროკავშირის მართლმსაჯულების სასამართლოს გენერალური ადვოკატის მოსაზრებით, საზედამხებელო ორგანო ვალდებულია, დაუყოვნებლივ იმოქმედოს პერსონალური მონაცემების უსაფრთხოების დარღვევის ფაქტის (ინციდენტის) აღმოჩენისას, საქმე "TR v Land Hessen", <<https://pdps.ge/ka/content/1068/-Datenewsroom>> [14.05.2024].

³⁵ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, 27-ე მუხლის მე-2 პუნქტი.

³⁶ Case of the Data Protection Authority (Belgium) №48, 08/04/2021.

³⁷ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, 27-ე მუხლის მე-3 პუნქტი.

³⁸ პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებებისა და პროფაილინგის შესახებ“, 2024, 4-6.

ნოტარიუსის აქტიური მონაწილეობის გარეშე. შესაბამისად, სანოტარო მომსახურების მისაღებად მოქალაქეთა მონაცემთა დამუშავების კანონიერებისა და გამართულობისთვის მნიშვნელოვანია ელექტრონულ სანოტარო რეესტრში ავტომატური დამუშავებისთვის საჭირო ფუნქციების განვითარება.

4. ევროკავშირის ნოტარიუსთა საბჭოს წევრი ქვეყნების ელექტრონული სანოტარო რეესტრების სიახლეები

ევროკავშირის ნოტარიუსთა საბჭო შედგება ევროკავშირის 22 ქვეყნის ნოტარიუსთა პალატების წარმომადგენლობისგან. 2024 წელს, საქართველოს ნოტარიუსთა პალატა ევროკავშირის ნოტარიუსთა საბჭოში დამკვირვებლის სტატუსით გაწევრიანდა. ევროკავშირის ნოტარიუსთა საბჭოს წევრ სახელმწიფოებში ერთ-ერთ ძირითად სამუშაო მიმართულებად მონაცემთა ავტომატური დამუშავების სანოტარო ბაზების სრულყოფა, მასში განახლებული საინფორმაციო ტექნოლოგიებისა და ხელოვნური ინტელექტის ინტეგრირება მიიჩნევა.³⁹

იტალიაში, 2013 წლიდან დაიწერა სანოტარო აქტის ელექტრონული მოდელი, რომელიც არ საჭიროებს ბეჭდურ ანალოგს. მომხმარებელი ელექტრონული სანოტარო რეესტრის შაბლონში ავსებს პერსონალურ მონაცემებს და სისტემა აგენერირებს სანოტარო აქტის ელექტრონულ დოკუმენტს, რომელსაც ამოწმებს სისტემაში ჩართული მორიგე ნოტარიუსი, რომელსაც აირჩევს მომხმარებელი. გაწეული მომსახურება სწრაფი და სანდო მახასიათებლებით გამოირჩევა.⁴⁰

ჩეხეთის სანოტარო რეესტრი ინტეგრირებულია სასამართლო რეესტრთან, რაც შესაძლებლობას ანიჭებს ნოტარიუსს, ჰქონდეს წვდომა მომხმარებლის განცხადების განხილვის სანოტარო და სასამართლო ეტაპებზე, თანდართულ დოკუმენტებზე. საერთო წვდომა ნოტარიუსებისთვის გარკვეული ფუნქციების დელეგირებით აიხსნება. სამემკვიდრეო წარმოების მიზნებისთვის სანოტარო და სასამართლო მოქმედებები ელექტრონულად სრულდება და მხოლოდ საბოლოო შედეგი იბეჭდება. უფლებამოსილების დელეგირებასთან ერთად, ნოტარიუსს უფლება აქვს გაეცნოს სასამართლოს მონაცემთა ბაზაში დაცულ მონაცემებს და დაამუშაოს ისინი წინასწარ განსაზღვრული საფუძვლით.⁴¹

ავსტრიაში, 2000 წლიდან მოქმედებს ელექტრონული სამუშაო დოკუმენტი, რომელსაც კავშირი აქვს სანოტარო რეესტრის სისტემასთან და არქივის ფუნქცია გააჩნია. ნოტარიუსს შეუძლია ნებისმიერი სანოტარო მოქმედება შეასრულოს აღნიშნულ დოკუმენტში და მას შემდეგ, როდესაც ნოტარიუსი დაასრულებს სანოტარო მოქმედებას სანოტარო აქტი ავტომატურად აისახება შესრულებული მოქმედებების ველში. სისტემა ხასიათდება ტევადი მოცულობით, დაცულობითა და გაზიარების მოქნილი ფუნქციით. იგი შესაძლებლობას აძლევს ნოტარიუსს, რომ მარტივად მართოს მიმდინარე და დაარქივებული სანოტარო აქტები.⁴²

³⁹ European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 7-10.

⁴⁰ Chiarini A., Forte A., Excellence in Notary Services through ISO 9001 Certification: an Investigation from Italy, Huelva, 2016, 124-125.

⁴¹ European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 10.

⁴² Hall E. G., The Common Law and Civil Law Notary in the European Union: a Shared Heritage and a Influential Future, London, 2015, 15.

რუმინეთში 2014 წლიდან ამოქმედდა ელექტრონული პლატფორმა, რომელიც აერთიანებს სხვადასხვა ტიპის სანოტარო რეესტრებს. რეესტრების მართვას უზრუნველყოფს სანოტარო რეესტრების მართვის ცენტრი. რეესტრების სისტემა აპლიკაციის ტიპისაა და შესაძლებელია მასში დოკუმენტის რეალურ დროში გენერირება, ამისთვის საჭიროა მომხმარებლის პერსონალური მონაცემების, შინაარსისა და ნოტარიუსის მითითება.⁴³

ბელგიის ნოტარიატმა შეიმუშავა უძრავი ქონების საჯარო აუქციონის ელექტრონული პლატფორმა, რომელიც მომხმარებელს შესაძლებლობას ანიჭებს სახლიდან გაუსვლელად ჩაერთოს აუქციონში. ნოტარიუსი ამ სისტემის დახმარებით არკვევს აუქციონის შედეგებს და ადგენს სანოტარო აქტს, რომლის საფუძველზეც აუქციონის გამარჯვებული მოითხოვს ქონების რეგისტრაციას. ბელგიის ნოტარიატმა დანერგა მოქალაქეებზე ორიენტირებული საკომუნიკაციო სისტემა, სადაც მომხმარებლებს შეუძლიათ შეკითხვების გაგზავნა და ამ სისტემაში ჩართული ნოტარიუსები რეალურ დროში პასუხობენ მომხმარებლების შეკითხვებს და მათი თხოვნით ახორციელებენ სანოტარო მოქმედებებს.⁴⁴

ესტონეთში, ლიეტუვასა და ლატვიაში ყველა ნოტარიუსი იყენებს ელექტრონულ საინფორმაციო სისტემას, რომელიც დაცვის მაღალი მექანიზმებით ხასიათდება და აქვს ტრანსსასაზღვრო ფუნქცია ამ სამი ქვეყნის სანოტარო ბიუროებისთვის, რადგან მასში ასახული ინფორმაციის ნაწილი აღნიშნული ქვეყნების ნოტარიუსებისთვის ღია წვდომისაა და აერთიანებს უფლების დამდგენ რეესტრებს.⁴⁵

გერმანიის ნოტარიატმა განავითარა შეზღუდული პასუხისმგებლობის კომპანიების რეგისტრაციის ინოვაციური სისტემა, რომელიც დაინტერესებული პირების მონაცემების შეყვანის გზით, ნოტარიუსს ელექტრონული ფორმის შედგენის უფლებას რთავს. აღნიშნული მომსახურების მიღების სიხშირიდან გამომდინარე, პლატფორმას დაარქივების ფუნქცია გააჩნია და აქტიურად ახლდება მიმდინარე და დაარქივებული მოქმედებების მიხედვით.⁴⁶

ევროკავშირის ნოტარიუსთა საბჭოს წევრ სახელმწიფოებში თანამედროვე ნოტარიატის უპირველესი მოთხოვნა სანოტარო აქტების გაციფრულებაა, შესაბამისად, სანოტარო რეესტრები მეტ-ნაკლებად, უკვე გაციფრულებულია. მაგალითად, ავსტრიაში, ბელგიაში, ხორვატიაში, ჩეხეთში, ესტონეთში, საფრანგეთში, გერმანიაში, უნგრეთში, ლატვიაში, ლუქსემბურგში, მალტაში, ნიდერლანდებში, პოლონეთსა და რუმინეთში მოქმედებს ანდერძისა და სამემკვიდრეო რეესტრები, რომლებიც დაკავშირებულია ევროპული გაერთიანების სამემკვიდრეო რეესტრთან, რეესტრებს შორის არსებობს ინფორმაციული კავშირი, რომელიც გაერთიანების წევრ სახელმწიფოთა ნოტარიუსებს კონკრეტულ სახელმწიფოში გაცემული სამკვიდროს შესახებ ინფორმაციას აწვდის. მეორე საკითხია, რა ფორმითაა ხელმისაწვდომი აღნიშნულ რეესტრში სანოტარო აქტი. ელექტრონულ ბაზაში რეგისტრირებულ სანოტარო აქტს, ცალკეულ შემთხვევაში

⁴³ Ruggeri L., Kunda I., Winkler S. (eds.), Family Property and Succession in EU Member States National Reports on the Collected Data, The European Commission, 2019.

⁴⁴ Verboven F., Yontcheva B., Private Monopoly and Restricted Entry - Evidence from the Notary Profession, 2022, 7.

⁴⁵ Parsova V., Gurskiene V., Kaing M., Real Property Cadastre in Baltic Countries, Jelgava, 2012, 158.

⁴⁶ Rinne T., A Guide to Corporate Forms for Doing Business in Germany, Hamburg, 2017, 23.

უნდა დაერთოს ნოტარიუსის ხელმოწერა და ბეჭედი ან მხოლოდ ელექტრონული რეკვიზიტები (უნიკალური კოდი), ხელმოწერის გარეშე.⁴⁷

საქართველოს ნოტარიუსთა პალატამ გერმანიის ნოტარიუსთა ფედერალურ პალატასთან ურთიერთანამშრომლობის მემორანდუმი გააფორმა. მემორანდუმი საქართველოსა და გერმანიის ნოტარიუსთა პალატებს შორის ურთიერთანამშრომლობით სანოტარო მომსახურების დახვეწასა და განვითარებას ითვალისწინებს, რაც უზრუნველყოფს სანოტარო საინფორმაციო ტექნოლოგიების სფეროში გამოცდილების გაზიარებას,⁴⁸ რათა გამოცდილების გაზიარება მხოლოდ თეორიული სწავლებით არ შემოიფარგლოს და შემოთავაზებული იქნეს მომხმარებელზე მორგებული ელექტრონული სერვისები.⁴⁹

5. დასკვნა

ნოტარიუსებს აქტიური შემხებლობა აქვთ მონაცემთა სუბიექტებთან. ნოტარიუსის პროფესიული საქმიანობის საფუძვლებია: საქართველოს კონსტიტუცია, „ნოტარიატის შესახებ“ საქართველოს კანონი, საქართველოს იუსტიციის მინისტრის ბრძანება „სანოტარო მოქმედებათა შესრულების წესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ და სხვა ნორმატიული აქტები, ხოლო სანოტარო მომსახურების მიმღები პირების პერსონალური მონაცემების დამუშავება ეფუძნება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონს.

მნიშვნელოვანია ჩამოყალიბდეს ელექტრონულ სანოტარო რეესტრზე წვდომის მქონე პირთა სტატუსი, შემდგომი ღია და დახურული ტიპის შიდა სისტემებზე წვდომის ფარგლებში მონაცემთა უსაფრთხოების დაცვის ძირითადი სტანდარტები, რაც მიემართება, როგორც გარეშე პირთა ისე რეესტრზე წვდომის მქონე პირთა სტატუსს, მოვალეობებსა და მათი მოქმედებების რეგულირებას მონაცემთა დაცვის კანონმდებლობით.

კვლევის შედეგად გამოიკვეთა ელექტრონული სანოტარო რეესტრის ფუნქციონირების განსაკუთრებული მნიშვნელობა და მისი დახვეწის საჭიროება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნათა გათვალისწინების, მომხმარებელზე მორგებული ელექტრონული სერვისების განვითარების და ევროკავშირის ნოტარიუსთა საბჭოს წევრი ქვეყნების პრაქტიკის მაგალითზე. სასურველია, რომ სანოტარო საქმიანობის განხორციელებისას ელექტრონული სანოტარო რეესტრი, მონაცემთა უსაფრთხოების დაცვის შესაბამისი სტანდარტებით ითვალისწინებდეს ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებას, რაც დაეხმარება ნოტარიუსს მოქალაქეთა მიმართვიანობის მართვასა და სანოტარო აქტის შედგენაში.

⁴⁷ შეაღ. გაბისონია ზ., ციფრული მმართველობა და სამართლის ტექნოლოგიები იუსტიციის სისტემაში, ჟურნ. „იუსტიცია“, №1[4], 2023, 41.

⁴⁸ დამატებით იხ.: ბოკი რ., ზოგიერთი მოსაზრება ნოტარიატის მომავალზე, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №2, 2022, 1-2; ბოკი რ., გერმანული ნოტარიატის სისტემა, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №8, 2020, 6-8.

⁴⁹ შეაღ. ვუდარსკი ა., სირდაძე ლ., რეესტრის ჯუნგლები 21-ე საუკუნეში, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №6, 2020, 30-31.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. საქართველოს კანონი „ნოტარიატის შესახებ“, 04/12/2009.
3. საქართველოს იუსტიციის მინისტრის ბრძანება „სანოტარო მოქმედებათა შესრულების წესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“, 31/03/2010.
4. ასვანუა ნ., პერსონალურ მონაცემთა დაცვის მექანიზმები, თბ., 2023, 39-40.
5. ბერნსდორფი ნ., ევროპის კავშირის „მონაცემთა დაცვის სამართალი“, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №2, 2023, 14-15.
6. ბოკი რ., ზოგიერთი მოსაზრება ნოტარიატის მომავალზე, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №2, 2022, 1-2.
7. ბოკი რ., გერმანული ნოტარიატის სისტემა, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №8, 2020, 6-8.
8. გაბისონია ზ., ციფრული მმართველობა და სამართლის ტექნოლოგიები იუსტიციის სისტემაში, ჟურნ. „იუსტიცია“, №1[4], 2023, 41.
9. ელიზბარაშვილი ს., ადამიანის უფლებების დაცვა ტექნოლოგიური განვითარების ეპოქაში: ხელოვნური ინტელექტის რეგულირების დასაწყისი, სტატიათა კრებული - ადამიანის უფლებათა დაცვა: ევროპული გამოცდილება და ეროვნული გამოწვევები, თბ., 2023, 80-81.
10. ვუდარსკი ა., სირდაძე ლ., რეესტრის ჯუნგლები 21-ე საუკუნეში, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №6, 2020, 22, 30-31.
11. პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის 2022 წლის ანგარიში.
12. პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის 2023 წლის ანგარიში.
13. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაციები საჯარო დაწესებულებებისთვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან თავსებადობის მიზნით შიდაუწყებრივი სამართლებრივი აქტების გამოცემის/განახლების თაობაზე, 2023, 1-2, 14.
14. პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „ინციდენტთან დაკავშირებული ღონისძიებების განხორციელების თაობაზე“, 2024.
15. პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, 2024.
16. პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებებისა და პროფაილინგის შესახებ“, 2024.
17. პეტერფალვი ა., ესტერი დ., როდესაც ჩვენი მანქანები გვსწავლობენ: ევროპის კავშირის მცდელობები ხელოვნური ინტელექტის საფუძველზე გადაწყვეტილების მიღებისა და პროფილირების რეგულირებასთან დაკავშირებით, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2023, 72-74.
18. ხარიტონაშვილი ნ., კონფერენცია „გერმანული და ქართული ნოტარიატის გაციფრულება“, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №4, 2023, 88-89.
19. ხარიტონაშვილი ნ., ქართული ნოტარიატის გაციფრულება, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №6, 2023, 149.

20. ხუბუა გ., სირდაძე ლ., სამართლის ტექნოლოგიები (ლიგალტექი) საქართველოში, მათი გამოყენება კერძო კომპანიებსა და საჯარო უწყებებში, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი, №7, 2022, 10.
21. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28/01/1981.
22. General Data Protection Regulation (GDPR), 27/04/2016.
23. Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), 18/06/2018.
24. Chiarini A., Forte A., Excellence in Notary Services through ISO 9001 Certification: an Investigation from Italy, Huelva, 2016, 124-125.
25. European Judicial Systems Efficiency and Quality of Justice, Specific Study of the CEPEJ, Council of Europe, №26, 2018, 220.
26. European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 7-10.
27. European Commission for the Efficiency of Justice, Study on the Functioning of Judicial Systems in the EU Member States, Specific Study on the Facts and Figures from the CEPEJ Questionnaires 2012 to 2020, Strasbourg, 2022, 899-900.
28. Hall E. G., The Common Law and Civil Law Notary in the European Union: a Shared Heritage and a Influential Future, London, 2015, 15.
29. Information Commissioner's Office (ICO), Guide to the General Data Protection Regulation (GDPR), 2018.
30. Kuner C., Bygrave L. A., Docksey C., The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 25-27.
31. Rinne T., A Guide to Corporate Forms for Doing Business in Germany, Hamburg, 2017, 23.
32. Ruggeri L., Kunda I., Winkler S. (eds.), Family Property and Succession in EU Member States National Reports on the Collected Data, The European Commission, 2019.
33. Verboven F., Yontcheva B., Private Monopoly and Restricted Entry - Evidence from the Notary Profession, 2022, 7.
34. Case of the Data Protection Authority (Italy) №9993548, 11/01/2024.
35. Case of the Data Protection Authority (Belgium) №52, 03/04/2024.
36. Case of the Data Protection Authority (Poland) №DKN.5131.31.2021, 07.02.2023.
37. Case of the Data Protection Authority (Belgium) №48, 08/04/2021.
38. Case of the Data Protection Authority (Spain) №PS/00044, 23/10/2020.

პერსონალურ მონაცემთა დაცვა მოქმედებების აღრიცხვის ჟურნალებში (ე.წ. „ლოგებში“)

სტატიაში განხილულია მოქმედებების აღრიცხვის ჟურნალებში (ე.წ. „ლოგებში“) პერსონალურ მონაცემთა დაცვის აქტუალური სამართლებრივი საკითხები. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ძალაში შესვლასთან ერთად მეტი აქტუალობით დადგა დღის წესრიგში ბალანსის აუცილებლობა მოქმედებების აღრიცხვის ჟურნალების, როგორც ინფორმაციული უსაფრთხოების სისტემის ეფექტურობასა და მასში შეგროვებული პერსონალური მონაცემების მაღალი სტანდარტით დაცულობას შორის.

საკვანძო სიტყვები: მოქმედებების აღრიცხვის ჟურნალი, პერსონალური მონაცემები, მონაცემთა უსაფრთხოება, მონაცემთა დაცვის ძირითადი რეგულაცია, პერსონალურ მონაცემთა დაცვა.

1. შესავალი

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) საქმეში: “Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González”¹ განაცხადა: „ინტერნეტის ავტომატური, მუდმივი და სისტემატური შესწავლის პროცესში, ინტერნეტში გამოქვეყნებული ინფორმაციის მოსაძიებლად, საძიებო სისტემის ოპერატორი „აგროვებს“ მონაცემებს, რომლებსაც შემდგომ „აღადგენს“, „იწერს“ და „აღაგებს“ ინდექსაციის პროგრამების ფარგლებში, „ინახავს“ სერვერებზე და საჭიროებისას, „ამჟღავნებს“ მას; ასევე, უზრუნველყოფს მასზე „წვდომას“ თავისი მომხმარებლებისათვის, საძიებო შედეგების ჩამონათვალის ფორმით.“² სასამართლოს დასკვნით, ამგვარი ქმედება არის „დამუშავება“, მიუხედავად იმისა, რომ საძიებო სისტემის ოპერატორი მსგავს ოპერაციებს ახორციელებს სხვა ტიპის ინფორმაციის მიმართ და ამ უკანასკნელს არ განარჩევს პერსონალური მონაცემებისაგან.“

ევროკავშირის კანონმდებლობის შესაბამისად „უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ბუნების, მოცულობის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო საფრთხეების გათვალისწინებით, მონაცემთა დამუშავებისთვის

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

¹ CJEU, Case 131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13/05/2014.

² იქვე, პუნქტი 28.

პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა მიიღონ რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები უსაფრთხოების უზრუნველსაყოფად [...].³

ეს ზომები მოიცავს შემდეგ ასპექტებს: პერსონალურ მონაცემთა ფსევდონიმიზაცია და დამიფვრა; დამუშავების სისტემებისა და სერვისების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა; ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, პერსონალურ მონაცემთა წვდომისა და ხელმისაწვდომობის დროული აღდგენა; დამუშავების უსაფრთხოების ტექნიკურ და ორგანიზაციულ საშუალებათა ეფექტიანობის რეგულარული შემოწმება და შეფასება.

პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტით „ლოგირება“ განიხილება, როგორც სავალდებულო მოთხოვნა და მიიჩნევა მონაცემთა უსაფრთხოების გარანტიად.

აღსანიშნავია, რომ საქართველოს კანონმდებლობა არ იცნობს ტერმინებს „ლოგი“ და „ლოგირება“. ამის მიუხედავად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი შეესაბამება ევროკავშირის, კერძოდ „GDPR“-ის სტანდარტს და დამუშავებისთვის პასუხისმგებელ პირს ავალდებულებს „უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა“⁴ - ანუ ლოგირება.

ამგვარად, საქართველოს კანონმდებლობის შესაბამისად, „ლოგირება“ გადაითარგმნა, როგორც „მოქმედებების აღრიცხვა“, ხოლო „ლოგი“ – „მოქმედებების აღრიცხვის ჟურნალი“.⁵

როგორც წესი, მოქმედებების აღრიცხვის ჟურნალის შექმნის დროს მასში თავს იყრის პერსონალური ინფორმაცია, რაც, თავის მხრივ, მოქმედებების აღრიცხვის ჟურნალებს გადააქცევს პერსონალური მონაცემების დამუშავების ადგილად. დღის წესრიგში დგება ბალანსის დაცვის აუცილებლობა მოქმედებების აღრიცხვის ჟურნალების, როგორც ინფორმაციული უსაფრთხოების სისტემის ეფექტურობასა და მასში შეგროვებული პერსონალური მონაცემების დაცულობას შორის.

ამგვარად, ჩვენი კვლევის მიზანია იმ საკანონმდებლო და პროცედურული სტანდარტების მიმოხილვა, რომლებიც ამ ბალანსის შესაძლებლობას იძლევა. შესაბამისად სტატიამი მიმოვიხილავთ მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის სტანდარტს „GDPR“-ის და საქართველოს კანონმდებლობის შესაბამისად (მეორე თავი); მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის პრინციპებს: მინიმიზაცია; ფსევდონიმიზაცია და დეპერსონალიზაცია (მესამე თავი) მოქმედებების აღრიცხვის ჟურნალებს, როგორც მონაცემთა უსაფრთხოების დაცვის გარანტს: ინციდენტის აღრიცხვა და შეტყობინება (მეოთხე თავი); ასევე, პროცედურულ მოთხოვნებს

³ 2018 წლის 25 მაისს ძალაში შევიდა ევროპარლამენტისა და საბჭოს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, 27/04/2016, <<https://gdpr-info.eu/>> [02.07.2024]. იხ. მუხლი 5.

⁴ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 27, პუნქტი 4.

⁵ ფრანგულ ენაში, შესაბამისად საფრანგეთსა და კანადაში, ასევე არ გამოიყენება ტერმინები ლოგირება და ლოგი. მათ ნაცვლად „მოქმედებების აღრიცხვა“ და „მოქმედებების აღრიცხვის ჟურნალი“ (მ.წ.).

მოქმედებების აღრიცხვის ჟურნალების მიმართ: შენახვის ვადები და წვდომაზე უფლებამოსილი პირები (მეხუთე თავი); დასკვნის სახით შემოგთავაზებთ რეკომენდაციებს ლოგირებისას და ლოგებში პერსონალური მონაცემების დაცვის მაღალი სტანდარტით უზრუნველსაყოფად.

2. მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის სტანდარტი “GDPR”-ის და საქართველოს კანონმდებლობის შესაბამისად

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მსგავსად ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვალდებულებას უზრუნველყოს მონაცემთა უსაფრთხოება, კერძოდ, კანონის 27-ე მუხლის მე-4 პუნქტი ადგენს: „დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან უზრუნველყონ ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა“.

ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედებების აღრიცხვა გამოიყენება უსაფრთხოების მიზნით, ინციდენტის მიზეზებისა და მის უკან მდგომი სუბიექტების შესახებ მოკვლევისა და გამოძიების უზრუნველსაყოფად. აღრიცხული მონაცემები გროვდება ოპერატორებისა და ინტერნეტთან დაკავშირებული მოწყობილობების საშუალებით.

ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედებები ქრონოლოგიურად იწერება ელექტრონულ ჟურნალებში. მონაცემები გენერირდება ყოველთვის და ყველგან. ისინი შეიცავს ინფორმაციას მოქმედების დროისა და თარიღის შესახებ; აღრიცხავს განხორციელებულ მოქმედებას, მოქმედების მცდელობას და მომხმარებელს, ან IP მისამართს; აღრიცხავს ავტორიზებულ ან წვდომის უფლების მქონე მომხმარებელს; აღრიცხავს სად განხორციელდა მოქმედება და სად შეიცვალა ორიგინალური მონაცემები; აღრიცხავს მიაღწია თუ არა მომხმარებელმა შედეგს. წარუმატებელი მცდელობის შემთხვევაში იწერს (ინიშნავს და იმახსოვრებს) წარუმატებლობის მიზეზს.

იმავედროულად, აღრიცხვის ჟურნალებში მუშავდება პერსონალური მონაცემები განუსაზღვრელი რაოდენობით.

“GDPR”-ით და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით⁶: პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, გეოლოკაციის მონაცემებით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით. პერსონალურ ინფორმაციად შეიძლება ჩაითვალოს, მაგალითად,

⁶ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 3, პუნქტი „ა“.

პიროვნების განრიგი, ისევე როგორც ინფორმაცია ადგილმდებარეობის შესახებ, მათ შორის მათი IP მისამართი.

ამგვარად, მოქმედებების აღრიცხვის ჟურნალები ექვემდებარება პერსონალურ მონაცემთა დაცვის კონტროლს და მათზე ვრცელდება “GDPR”-ის მე-5 და 32-ე მუხლებით, ასევე, მონაცემთა დაცვის საქართველოს კანონმდებლობით ვალდებულებები.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის მიხედვით, „მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება.“

მონაცემთა მინიმიზაციის პრინციპის⁷ დაცვისათვის საჭიროა, რომ დამუშავებული მონაცემების მოცულობა იყოს:

შემოფარგლული მხოლოდ იმით, რაც აუცილებელია: მოქმედებების აღრიცხვის ჟურნალებში არ უნდა დამუშავდეს უფრო მეტი მონაცემი, ვიდრე მიზნის მიღწევისთვის არის საჭირო. ეს კომპონენტი გულისხმობს, რომ მიზნის მიღწევა გონივრულად შეუძლებელია კონკრეტული პერსონალური მონაცემების დამუშავების გარეშე.

პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით. ამასთანავე, მონაცემთა მინიმიზაციის პრინციპი მჭიდრო კავშირშია მიზნის შეზღუდვის პრინციპთან და მისი დაცვა შესაძლებელია მხოლოდ იმ შემთხვევაში, როდესაც პასუხისმგებელი პირის მიერ კონკრეტული მიზნები მკაფიოდაა განსაზღვრული. პასუხისმგებელმა პირმა, მიზნის მიღწევის აუცილებლობის დასადგენად, უნდა გადახედოს მოქმედებების აღრიცხვის ჟურნალებში პერსონალური ინფორმაციის დამუშავების ოპერაციის თითოეულ საფეხურს და მონაცემთა თითოეულ ელემენტს.

პასუხისმგებელმა პირებმა უნდა განსაზღვრონ, სჭირდებათ თუ არა მათ პერსონალური მონაცემების დამუშავება შესაბამისი მიზნების მიღწევისთვის, უნდა გადაამოწმონ, შესაძლებელია თუ არა ნაკლები მოცულობის პერსონალური მონაცემების დამუშავებით, ნაკლებად დეტალური ან გაერთიანებული პერსონალური მონაცემებით ან საერთოდ პერსონალური მონაცემების დამუშავების გარეშე შესაბამისი მიზნების მიღწევა.

მინიმიზაცია ასევე დაკავშირებულია იდენტიფიკაციის ხარისხთან. თუ დამუშავების მიზანი არ მოითხოვს, რომ მონაცემთა საბოლოო ნაკრები მითითებას იდენტიფიცირებულ ან იდენტიფიცირებად ინდივიდზე (მაგალითად, სტატისტიკის შემთხვევაში) აკეთებდეს, თუმცა პირველადი დამუშავებისას ამის საჭიროება არსებობს (მაგალითად, მონაცემთა გაერთიანებამდე), მაშინ პასუხისმგებელმა პირმა პერსონალური მონაცემები უნდა წაშალოს ან მისი ანონიმიზაცია მოახდინოს, მას შემდეგ რაც იდენტიფიკაციის საჭიროება აღარ იარსებებს. ხოლო, თუ სხვა დამუშავების აქტივობებისთვის მუდმივი იდენტიფიკაციაა საჭირო, მონაცემთა

⁷ იქვე, მუხლი 4.

სუბიექტების უფლებების რისკის შესამცირებლად პერსონალური მონაცემების ფსევდონიმიზაცია უნდა განხორციელდეს⁸.

მოქმედებების აღრიცხვის ჟურნალები შეიცავს დიდი რაოდენობით მონაცემებს, მათი უმრავლესობა პერსონალური მონაცემებია. რაც უფრო მსხვილია ორგანიზაცია, მით მეტი პერსონალური ინფორმაცია მუშავდება და ინახება ჟურნალებში, მაგალითად, IP მისამართები და გეოლოკაციის მონაცემები. იმის გათვალისწინებით, რომ ხშირად მოქმედებების აღრიცხვის ჟურნალებში მონაცემების შენახვა კანონითაა გათვალისწინებული აპრობირებული მეთოდია მოქმედებების აღრიცხვის ჟურნალში მონაცემების გაფილტვრა, მაგალითად, ელექტრონული ფოსტის მისამართების ან ტელეფონის ნომრების რედაქტირება/წაშლა⁹.

3. მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვა

ნებისმიერ შემთხვევაში, მონაცემთა დამუშავებაზე უფლებამოსილმა პირმა უნდა შექმნას ისეთი სისტემა, რომელიც უზრუნველყოფს მოქმედებების აღრიცხვის ჟურნალებში დაცული მონაცემების კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის გარანტიას. უფრო ზუსტად, შეგროვებული მონაცემების გამოყენება უნდა იყოს ფორმალიზებული და დოკუმენტირებული წინასწარ დადგენილი წესებითა და პროცედურებით.

იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა ინახებოდეს პირის იდენტიფიცირების გამომრიცხავი ფორმით.

უფლებამოსილი პირი, რომელსაც აქვს წვდომა დამუშავებაზე, ინფორმირებული უნდა იყოს მოქმედებების აღრიცხვის ჟურნალის გამოყენების წესების, შეგროვებული მონაცემების სახეობისა და მათი შენახვის ვადის შესახებ. ამის მიღწევა შესაძლებელია, მაგალითად, საინფორმაციო შეტყობინების საშუალებით ავტორიზაციის დროს/დამშვების წინ.

მონაცემების დამუშავებისას უზრუნველყოფილი უნდა იყოს მათი მთლიანობა, უსაფრთხოება და დაცვა უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვის, განადგურებისა და დაზიანებისგან¹⁰.

“GDPR”-ის 32-ე მუხლი აფართოებს მე-5 მუხლში ჩამოყალიბებული მთლიანობისა და კონფიდენციალურობის ფუნდამენტურ პრინციპს და იძლევა მონაცემთა დაცვის შესაძლებლობას ფსევდონიმიზაციისა და დეპერსონალიზაციის საშუალებით, რომელიც ასევე ვრცელდება მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დამუშავებაზე.

„პერსონალურ მონაცემთა შესახებ“ საქართველოს კანონით მონაცემთა დეპერსონალიზაცია არის მონაცემთა იმგვარი დამუშავება, როდესაც შეუძლებელია მონაცემთა სუბიექტთან მათი დაკავშირება ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს,¹¹ ხოლო მონაცემთა ფსევდონიმიზაცია – მონაცემთა იმგვარი დამუშავება, როდესაც

⁸ რეკომენდაცია „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, პერსონალურ მონაცემთა დაცვის სამსახური, 2024.

⁹ კანადის პირადი ცხოვრების დაცვის კომისარიატის გზამკვლევი მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ, <<https://www.cyber.gc.ca/sites/default/files/itsap80085-journalisation-surveillance-securite-reseau-f.pdf>> [02.07.2024].

¹⁰ იქვე.

¹¹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 2, პუნქტი „ც“.

დამატებითი ინფორმაციის გამოყენების გარეშე შეუძლებელია მონაცემების კონკრეტულ მონაცემთა სუბიექტთან დაკავშირება და ეს დამატებითი ინფორმაცია შენახულია ცალკე და ტექნიკური და ორგანიზაციული ზომების მეშვეობით მონაცემების იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან დაკავშირება არ ხდება¹².

ახალი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მასშტაბის, კონტექსტისა და მიზნების, აგრეთვე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელი რისკებისა და მონაცემთა დამუშავების პრინციპების გათვალისწინებით, დამუშავებისთვის პასუხისმგებელმა პირმა, როგორც დამუშავების საშუალებების განსაზღვრის, ისე უშუალოდ დამუშავების პროცესში უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები (მათ შორის, ფსევდონიმიზაცია ან/და სხვა). ამ ზომების მიღება უნდა უზრუნველყოფდეს მონაცემთა დამუშავების პრინციპების ეფექტიან იმპლემენტაციას და მონაცემთა დამუშავების პროცესში დაცვის მექანიზმების ინტეგრირებას მონაცემთა სუბიექტის უფლებების დასაცავად.¹³

4. მოქმედების ადრიცხვის ჟურნალები, როგორც მონაცემთა უსაფრთხოების დაცვის გარანტი: ინციდენტის ადრიცხვა და შეტყობინება

“GDPR”-ის 33-ე მუხლით, ისევე როგორც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლით: „დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია ადრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები და ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს“. ასევე „დამუშავებაზე უფლებამოსილი პირი ვალდებულია ინციდენტის შესახებ დაუყოვნებლივ აცნობოს დამუშავებისთვის პასუხისმგებელ პირს“.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის¹⁴ შესაბამისად, შეტყობინება უნდა შეიცავდეს შემდეგ ინფორმაციას:

- ა) ინციდენტის გარემოებების, სახისა და დროის შესახებ;
- ბ) ინციდენტის შედეგად უნებართვოდ გამჟღავნებული, დაზიანებული, წაშლილი, განადგურებული, მოპოვებული, დაკარგული, შეცვლილი მონაცემების სავარაუდო კატეგორიებისა და რაოდენობის, აგრეთვე იმ მონაცემთა სუბიექტების სავარაუდო კატეგორიებისა და რაოდენობის შესახებ, რომლებსაც ინციდენტის შედეგად შეექმნათ საფრთხე.

მოქმედების ადრიცხვის ჟურნალები, რომლებიც ადრიცხავენ სისტემის შიდა ფუნქციონირებას, წარმოადგენს ერთადერთ მონაცემთა ბაზას, რომელიც საშუალებას აძლევს დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს რეაგირებისა და შეტყობინების უზრუნველსაყოფად.

¹² იქვე, პუნქტი „ძ“.

¹³ იქვე, მუხლი 26.

¹⁴ იქვე, მუხლი 29.

5. პროცედურული მოთხოვნები მოქმედებების აღრიცხვის ჟურნალების მიმართ: შენახვის ვადები და წვდომაზე უფლებამოსილი პირები

5.1. მოქმედებების აღრიცხვის ჟურნალების შენახვის ვადები

“GDPR”-ის 30-ე მუხლი და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლი აწესებს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულებას, კერძოდ, დამუშავებისთვის პასუხისმგებელი პირი და მისი სპეციალური წარმომადგენელი (ასეთის არსებობის შემთხვევაში) ვალდებული არიან წერილობით ან ელექტრონულად უზრუნველყონ მონაცემთა დამუშავებასთან დაკავშირებული შემდეგი ინფორმაციის აღრიცხვა: მონაცემთა შენახვის ვადების შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, მათი შენახვის ვადის განსაზღვრის კრიტერიუმების თაობაზე.

მოქმედებების აღრიცხვის ჟურნალები ხშირად დიდი ხნის განმავლობაში ინახება. მათი დანიშნულებიდან გამომდინარე შენახვის ვალდებულება უალტერნატივოა, რადგან ისინი შეიცავს მნიშვნელოვან ინფორმაციას ინციდენტის ან ინციდენტის მცდელობის შემთხვევაში ეფექტური გამოძიების ჩასატარებლად. იმავდროულად, მათში თავმოყრილი პერსონალური მონაცემების უვადოდ და გაუმართლებლად დიდი ხნით შენახვა არაგონივრული რისკია.

მართალია, “GDPR” არ აკონკრეტებს პერსონალური მონაცემების შენახვის ზუსტ ვადას, თუმცა საქმეში *Digital Rights Ireland*¹⁵ ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) იმსჯელა მონაცემთა შენახვის დირექტივის კანონიერებაზე¹⁶. “CJEU” შეეხო მონაცემთა შენახვის დირექტივაში ობიექტურ კრიტერიუმთა არარსებობასაც, რომელთა საფუძველზეც უნდა განისაზღვროს მონაცემთა შენახვის ზუსტი პერიოდი - მინიმალური 6 თვიდან მაქსიმალურ 24 თვემდე.

ამგვარად, მოქმედებების აღრიცხვის ჟურნალების შენახვის ვადა ევროკავშირის ქვეყნების კარგი პრაქტიკის¹⁷ გათვალისწინებით მერყეობს 6 თვიდან - 12 თვემდე. განსაკუთრებულ შემთხვევებში ეს ვადა შესაძლებელია გაგრძელდეს 24 თვემდე.

“GDPR”-ის მე-5 მუხლისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის შესაბამისად მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან

¹⁵ CJEU, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 08/04/2014.

¹⁶ დირექტივა მიზნად ისახავდა შიდასახელმწიფოებრივი დებულებების ჰარმონიზებას ისეთი პერსონალური მონაცემების შენახვასთან დაკავშირებით, რომლებიც მოპოვებული და დამუშავებულია საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო სერვისების ან ქსელების საშუალებით და შეიძლება გადაეცეს უფლებამოსილ უწყებას ორგანიზებულ დანაშაულსა და ტერორიზმთან ბრძოლის მიზნებით. მონაცემთა დაცვის დირექტივა აღგენდა მონაცემთა შენახვას, „სულ მცირე, 6 თვის ვადით, ისე, რომ არ განარჩევდა ამავე დირექტივის მე-5 მუხლით გათვალისწინებულ მონაცემთა კატეგორიებს იმის მიხედვით, თუ რამდენად გამოსადეგი იყო დასახული მიზნის მისაღწევად ან რომელ პირებს მიემართებოდა“.

¹⁷ საფრანგეთის ინფორმაციისა და თავისუფლების ეროვნული კომისიის (“CNIL”) დადგენილება №2021-122 „მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ“.

შენახული უნდა იქნეს დეპერსონალიზებული ფორმით, გარდა იმ შემთხვევისა, თუ მონაცემთა დამუშავება განსაზღვრულია კანონით ან/და კანონის შესაბამისად გამოცემული კანონქვემდებარე ნორმატიული აქტით და მონაცემთა შენახვა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში აღმატებული ინტერესების დასაცავად.

დამუშავებისთვის პასუხისმგებელი პირის მიერ შენახვის ვადის განსაზღვრისას გათვალისწინებული უნდა იქნეს მისაღწევი მიზნის პროპორციული დროის მონაკვეთი. მაქსიმალური - 24 თვიანი ვადა უნდა დასაბუთდეს. ნებისმიერ შემთხვევაში, შეუძლებელია მაქსიმალური ვადის გამართლება მხოლოდ სისხლის სამართლის დანაშაულის ხანდაზმულობის ვადით.

დამუშავებისას სხვადასხვა ფაქტორების გათვალისწინებით შესაძლებელია შენახვის მაქსიმალური ვადის განსაზღვრა ჩაითვალოს გამართლებულად¹⁸, მაგალითად:

- როდესაც კანონმდებლობით დადგენილია ჩანაწერების შენახვის კონკრეტული ვადა;
- კონკრეტული მიზნისთვის, რომლის მიღწევა მხოლოდ მოქმედების ადრიცხვის ჟურნალების მონაცემების გამოყენებითაა შესაძლებელი, მაგალითად, დამუშავების კონტექსტში, რომელიც საშუალებას მისცემს დავის მონაწილეებს, გაეცნონ დოკუმენტებსა და შესაბამის მასალებს, რათა უზრუნველყოფილი იქნას პროცესის გამჭვირვალობა დაინტერესებული მხარეებისთვის;
- როდესაც არსებობს თავდასხმის შემდგომი ან შეჭრის მცდელობის შემდგომი ანალიზის განხორციელების აუცილებლობა, რომელიც დაკავშირებულია სამომავლოდ, გრძელვადიან პერსპექტივაში საფრთხის გაანალიზების აუცილებლობასთან.

მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელი პირმა ზუსტად და დოკუმენტურად დაასაბუთოს ის მიზეზები, რის გამოც მას უფრო ხანგრძლივი ვადის დადგენა უწევს¹⁹, მაგალითად, კონკრეტული სამართლებრივი ვალდებულების ან სპეციფიკის მითითებით, რომლებიც დაკავშირებულია მიზანთან. მონაცემთა უფრო ხანგრძლივად შენახვის აუცილებლობა შეიძლება ასევე გამართლებული იყოს იმით, რომ ეს ღონისძიება არის ერთადერთი გზა, რათა მოხდეს მაღალი რისკის ქვეშ მყოფი ფიზიკური პირების მიმართ მონაცემთა დაცვაზე ზემოქმედების შეფასებისა (“AIPD”) ან ექვივალენტური შესწავლის. ეს ანალიზი უნდა განხორციელდეს ინდივიდუალურად, “GDPR”-ის პრინციპების გამოყენებით, სადაც ეს შესაძლებელია, რათა განისაზღვროს საჭირო გარანტიები უსაფრთხოების პირობების, ხელმისაწვდომობისა და მონაცემთა შენახვის მიზნების თვალსაზრისით.

5.2. უფლებამოსილი პირების წვდომა მოქმედების ადრიცხვის ჟურნალებზე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის მე-6 პუნქტის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან თანამშრომელთა უფლებამოსილებების შესაბამისად განსაზღვრონ მონაცემებზე წვდომის ფარგლები და განახორციელონ ადეკვატური ღონისძიებები თანამშრომელთა მიერ მონაცემთა

¹⁸ იქვე.

¹⁹ იქვე.

უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, მათ შორის, უზრუნველყონ თანამშრომელთა ინფორმირება მონაცემთა უსაფრთხოების დაცვის საკითხების შესახებ.

პირი, რომელიც სარგებლობს მოქმედებების აღრიცხვის ჟურნალებზე წვდომის უფლებით, ვალდებულია, არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ²⁰.

თავდაპირველი მიზნისგან განსხვავებით, შეგროვებული მონაცემების ნებისმიერი ხელახალი დამუშავება ნიშნავს დამუშავების საბოლოო მიზნის ცვლილებას. ამიტომ, მიზანშეწონილია დამუშავებაზე პასუხისმგებელმა პირმა მიიღოს ტექნიკური და ორგანიზაციული ზომები, რომლებიც შესაძლებლობას მისცემს შეამციროს რისკები. მაგალითად, დაავალდებულოს მოქმედებების აღრიცხვის ჟურნალებზე წვდომაზე უფლებამოსილი პირები დაიცვან მონაცემების გამოყენების წესები (წინასწარ დადგენილი) ან სპეციალური გაფრთხილების სისტემის არსებობით მოახდინოს მოქმედებების აღრიცხვის ჟურნალებში უკანონოდ განხორციელებული ცვლილებების პრევენცია.

6. დასკვნა და რეკომენდაციები

კვლევამ აჩვენა, რომ მოქმედებების აღრიცხვის ჟურნალები წარმოადგენს შეუცვლელ და მნიშვნელოვან შესაძლებლობას ინციდენტთან დაკავშირებული საფრთხეების მისაკვლევად და გამოსავლენად, სისტემების დაცვის პრევენციული ღონისძიებების დასაგეგმად და განსახორციელებლად. თუმცა იმისათვის, რომ ჟურნალებში თავმოყრილი პერსონალური მონაცემები “GDPR”-ისა და საქართველოს კანონმდებლობის შესაბამისად მაღალი ხარისხით იქნეს დაცული, მონაცემთა დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა გაითვალისწინონ და პრაქტიკაში დანერგონ შემდეგი რეკომენდაციები:

- მოქმედებების აღრიცხვის ჟურნალებში მონაცემების დამუშავება უნდა შეესაბამებოდეს შემდეგ პრინციპებს: სამართლიანობა, კანონიერება და გამჭვირვალობა;
- დამუშავების მიზანი უნდა იყოს კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური. არ შეიძლება მოქმედებების აღრიცხვის ჟურნალებში შეგროვებული მონაცემების გამოყენება სხვა მიზნით;
- მოქმედებების აღრიცხვის ჟურნალებში უნდა შეგროვდეს მხოლოდ ის მონაცემები, რომლებიც საჭიროა იმისთვის, რომ უზრუნველყოს მონაცემთა უსაფრთხოების დაცვა ინციდენტის, ან ინციდენტის მცდელობის აღსაკვეთად, გასაანალიზებლად ან გამოსაძიებლად;
- მოქმედებების აღრიცხვის ჟურნალებში მონაცემები უნდა ინახებოდეს მხოლოდ წინასწარ დადგენილი ვადით;
- მოქმედებების აღრიცხვის ჟურნალები უნდა ინახებოდეს უსაფრთხოდ, სასურველია გარე სერვერებზე. ეს მონაცემები შენახული იქნას ძირითადი სისტემისგან განცალკევებულად. წვდომა განსაზღვრული უნდა იყოს წინასწარ განსაზღვრული ფორმით მხოლოდ უფლებამოსილი პირებისთვის.

²⁰ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 27, პუნქტი 5.

მოქმედებების აღრიცხვის სისტემა უნდა იყოს აღჭურვილი დუბლირება-
კოპირების/გადაწერის პრევენციული ტექნიკური საშუალებებით;

- რეკომენდირებულია მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემები იყოს დაშიფრული.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. ევროპარლამენტისა და საბჭოს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, 27/04/2016, <<https://gdpr-info.eu/>> [02.07.2024].
3. კანადის პირადი ცხოვრების დაცვის კომისარიატის გზამკვლევი მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ, <<https://www.cyber.gc.ca/sites/default/files/itsap80085-journalisation-surveillance-securite-reseau-f.pdf>> [02.07.2024].
4. რეკომენდაცია „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, პერსონალურ მონაცემთა დაცვის სამსახური, 2024, <<https://personaldata.ge>> [02.07.2024].
5. საფრანგეთის ინფორმაციისა და თავისუფლების ეროვნული კომისიის („CNIL“) დადგენილება №2021-122 „მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ“, <https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation_-_journalisation.pdf> [02.07.2024].
6. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება, CJEU, Case 131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC]*, 13/05/2014.
7. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება, CJEU, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC]*, 08/04/2014.

არასრულწლოვნის პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული გამოწვევები

არასრულწლოვნის პერსონალური მონაცემების დაცვა ერთ-ერთი აქტუალური და პრობლემური საკითხია. საკითხის აქტუალობას განსაზღვრავს არასრულწლოვნის, როგორც მონაცემთა სუბიექტის სტატუსის, უფლებებისა და ამ უფლებების გამოხატვის საკანონმდებლო მოწესრიგების თავისებურებები. განსაკუთრებით საყურადღებოა ციფრული ტექნოლოგიების გავლენა არასრულწლოვნების ყოველდღიურობასა და უფლებების განხორციელებაზე. ნაშრომი მიმოიხილავს არასრულწლოვნის პერსონალური მონაცემების დამუშავების ეროვნულ და საერთაშორისო სტანდარტებს, რათა განისაზღვროს არასრულწლოვნის პერსონალური მონაცემების დამუშავებისას მოსალოდნელი რისკები და გამოწვევები.

საკვანძო სიტყვები: პერსონალურ მონაცემთა დაცვის სამსახური, არასრულწლოვანთა პერსონალური მონაცემების დაცვა, არასრულწლოვანთა პერსონალური მონაცემების დამუშავება.

1. შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიზანია პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების, დაცვა. ამ დროს გასათვალისწინებელია არასრულწლოვნის, როგორც მონაცემთა სუბიექტის სტატუსი, მისი უფლებები, ამ უფლებების დამოუკიდებლად ან წარმომადგენლის მიერ განხორციელება და ძირითადი რისკების შეფასება, რაც მოიცავს დამუშავებისთვის პასუხისმგებელი პირების: სკოლების, ჯანდაცვის სექტორის და სხვა დაწესებულებების ინსპექტირებას, დარღვევათა გამოვლენას, პრევენციასა და ცნობიერების ამაღლებას, პერსონალურ მონაცემთა დაცვის კულტურის ჩამოყალიბებას.

მნიშვნელოვანია შეფასდეს არასრულწლოვნის პერსონალური მონაცემების დამუშავების საკანონმდებლო მოწესრიგება და მის საფუძველზე განისაზღვროს მოსალოდნელი რისკები, თუ რამდენად პასუხობს „პერსონალური მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონი არსებულ პრობლემებს და რა საკითხები უნდა

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, მოწვეული ლექტორი, პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის საერთაშორისო ურთიერთობებისა და სამართლებრივ საკითხთა კოორდინატორი.

გაითვალისწინონ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა არასრულწლოვნის მონაცემების დამუშავებისას.

2. არასრულწლოვანთა მონაცემთა დამუშავების მომწესრიგებელი სპეციალური ნორმა

2023 წლის ივნისში საქართველოს პარლამენტმა მიიღო კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომელიც ეფუძნება უნიკალურ სიახლეებს, ძირითად და მნიშვნელოვან სამართლებრივ დოკუმენტს წარმოადგენს საქართველოში პერსონალური მონაცემების დასაცავად.

რეგულირების სიახლე განსაზღვრა საერთაშორისო-სამართლებრივ აქტებთან (ევროპის საბჭოს 108-ე კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 108-ე კონვენციის შესწორების ოქმი, მოდერნიზებული 108-ე კონვენცია, მონაცემთა დაცვის ძირითადი რეგულაცია და სხვ.)¹ ჰარმონიზაციის საჭიროებამ, სტანდარტებისა და უფლების დაცვის მექანიზმების ქართულ კანონმდებლობაში დანერგვის აუცილებლობამ, ხოლო მეორე მხრივ, ცვლილებები ნაკარნახევი იყო პერსონალურ მონაცემთა დაცვის სამსახურის ეფექტიანობისა და ინსტიტუციური დამოუკიდებლობის, მიუკერძოებლობისა და შესაბამისი რეკომენდაციების შესრულების უზრუნველყოფით. ამ კანონის მნიშვნელობა განპირობებულია მისი დარგობრივი, ფუნქციური და ფუძემდებლური ხასიათით.²

არასრულწლოვნების პერსონალური მონაცემების დამუშავებასთან დაკავშირებით კანონის მე-7 მუხლში განისაზღვრა არასრულწლოვნის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესი და პირობები. ადმინისტრაციული სამართალდარღვევისთვის ადმინისტრაციული პასუხისმგებლობის შემამსუბუქებელ გარემოებებად იქნა მიჩნეული ადმინისტრაციული სამართალდარღვევის ჩადენა არასრულწლოვანის მიერ.³ ამ კანონით გათვალისწინებული ადმინისტრაციული სამართალდარღვევებისთვის ადმინისტრაციული პასუხისმგებლობის დამამძიმებელ გარემოებებად ჩაითვალა არასრულწლოვანის მონაცემების დამუშავება ამ კანონის მოთხოვნათა დარღვევით.⁴

არასრულწლოვანის შესახებ მონაცემთა დამუშავება მისი თანხმობის საფუძველზე დასაშვებია, თუ მან 16 წლის ასაკს მიაღწია, ხოლო 16 წლამდე არასრულწლოვანის შესახებ მონაცემთა დამუშავება – მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობით, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, მათ შორის, როდესაც მონაცემთა დამუშავებისთვის აუცილებელია 16 წლიდან 18 წლამდე არასრულწლოვანისა და მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა.⁵

¹ იხ. ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, ევროკავშირის საგამომცემლო სახლი, 2018, 20-21.

² შეად. გოშაძე კ., პერსონალურ მონაცემთა დაცვისა და დამუშავების კონსტიტუციურ-სამართლებრივი გარანტიები, საქართველოს უნივერსიტეტი, თბილისი, 2017, 43.

³ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Хმპ, 14/06/2023, 61-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი.

⁴ იქვე, 62-ე მუხლის „გ“ პუნქტი.

⁵ დამატებით იხ. შუდრა თ., ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, 1/2023, 112-115.

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს ყველა გონივრული და ადეკვატური ზომა 16 წლამდე არასრულწლოვანის მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობის არსებობის დასადასტურებლად, ხოლო არასრულწლოვანის შესახებ განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ მისი მშობლის ან სხვა კანონიერი წარმომადგენლის წერილობითი თანხმობის საფუძველზე, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა.

მნიშვნელოვანია საერთაშორისო სტანდარტების დამდგენი აქტების მიმოხილვა:

გაერთიანებული ერების ორგანიზაციის გენერალური ასამბლეის ბავშვის უფლებათა შესახებ გაეროს 1989 წლის კონვენცია საერთაშორისო დონეზე პირველი სამართლებრივი დოკუმენტია, რომელიც ბავშვების განსაკუთრებული ზრუნვისა და დაცვის საჭიროებას აღიარებს.

პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეის 2021 წლის რეზოლუცია ეხება ბავშვის ციფრულ უფლებებს, რომელშიც აღნიშნულია, რომ ბავშვები საჭიროებენ განსაკუთრებულ დაცვას. ისინი სარგებლობენ კონვენციით აღიარებული უფლებებით. ამ უფლებებით სარგებლობა მან უნდა შეძლოს ყველა სფეროში, მათ შორის ონლაინ სივრცეში. განმარტებულია, რომ ციფრული გარემო გავლენას ახდენს ბავშვის განვითარებაზე, ყოველდღიურ ცხოვრებაზე, მათ მომავალსა და შესაძლებლობებზე.

მინისტრთა კომიტეტის 2021 წლის დეკლარაცია ციფრულ გარემოში ბავშვების პირადი ცხოვრების დაცვის საჭიროების შესახებ განსაზღვრავს ციფრულ გარემოში ბავშვების პირადი ცხოვრების დაცვას. აღნიშნულია რისკები, რომლებსაც არასრულწლოვანი აწყდება თანამედროვე ტექნოლოგიების გამოყენებისას.

პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) 38-ე პუნქტის თანახმად, ბავშვები, თავიანთი პერსონალური მონაცემების დამუშავებისას, სარგებლობენ პერსონალური მონაცემების დაცვის განსაკუთრებული უფლებით, რადგან შეიძლება მათთვის ნაკლებად ცნობილი იყოს რისკები, შედეგები და დაცვის საშუალებები.

ევროპის საბჭოს 108-ე კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ და მოდერნიზებული 108-ე კონვენცია. მონაცემთა სუბიექტის თანხმობაზე მიუთითებს მოდერნიზებული 108-ე კონვენციის მე-5(2) მუხლი. ევროკავშირის სამართალში თანხმობა, როგორც მონაცემთა კანონიერი დამუშავების საფუძველი, მკაცრად არის დადგენილი GDPR-ის მე-6 მუხლით. მასზე მკაფიოდ მიუთითებს ქარტიის მე-8 მუხლიც. კანონიერი თანხმობის მახასიათებლები განმარტებულია რეგულაციის მე-4 მუხლში, ასეთი თანხმობის მოპოვების პირობები დეტალურად არის წარმოდგენილი მე-7 მუხლში, რაც შეეხება არასრულწლოვნისგან თანხმობის მიღების სპეციალურ წესებს საინფორმაციო საზოგადოების მომსახურებასთან დაკავშირებით, მათ აღგენს რეგულაციის მე-8 მუხლი.

3. არასრულწლოვანი, როგორც მონაცემთა სუბიექტი

ინფორმირებულობა პიროვნების თავისუფალი განვითარების ნაწილია და იგი დაფუძნებულია საკუთარი ნების, გადაწყვეტილების, არჩევანის შესაბამისად განვითარების შესაძლებლობაზე. პერსონალური მონაცემების დამუშავების შესახებ ინფორმაციის ზედმიწევნით ცოდნა ნებისმიერ ადამიანს, მათ შორის

არასრულწლოვანს, საშუალებას აძლევს დაიცვას და აკონტროლოს თავისი პირადი სფერო. ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით „პერსონალური მონაცემები“ განიმარტება, როგორც მონაცემი იდენტიფიცირებული ან იდენტიფიცირებადი ინფორმაცია ფიზიკური პირის შესახებ, რომლის ვინაობა ცნობილია, ან შეიძლება დადგინდეს დამატებითი ინფორმაციის საფუძველზე.⁶ გერმანიის საკონსტიტუციო სასამართლომ ჯერ კიდევ 1983 წელს განმარტა, რომ „მონაცემთა ავტომატური დამუშავების პირობებში, ადარ არსებობს უმნიშვნელო ინფორმაცია“.⁷ ნებისმიერი ინფორმაცია, რომელიც დაკავშირებულია ინდივიდთან, ერთი შეხედვით რაც არ უნდა არადამაზიანებლად აღიქმებოდეს, შესაძლოა იყოს განსაკუთრებული კატეგორიის⁸. აქედან გამომდინარე, პერსონალური მონაცემები მოიცავს ნებისმიერ ინფორმაციას, იმისგან დამოუკიდებლად ეს ეხება პიროვნების პირად ცხოვრებას, სამუშაო, ეკონომიკურ, სოციალურ გარემოსა თუ პირის შესაძლებლობებს.⁹ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მიხედვით, იდენტიფიცირებადი ფიზიკური პირი არის ის, ვისი პირდაპირ ან არაპირდაპირ იდენტიფიცირებაც შესაძლებელია ისეთი იდენტიფიკატორის გამოყენებით, როგორიცაა: სახელი, პირადი ნომერი, ინფორმაცია ადგილმდებარეობის შესახებ, ონლაინ იდენტიფიკატორი ან ფიზიკური პირის იდენტობისათვის დამახასიათებელი ერთი ან მეტი ფიზიკური, ფსიქოლოგიური, გენეტიკური, გონებრივი, ეკონომიკური, კულტურული ან სოციალური ფაქტორით.¹⁰ ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-8 მუხლის თანახმად,¹¹ მონაცემთა დაცვა საყოველთაო უფლებას წარმოადგენს და არ შემოიფარგლება ცალკეული ქვეყნის მოქალაქეებით¹².

მონაცემთა დაცვის ძირითადი რეგულაციის პრეამბულის მიხედვით, არასრულწლოვნები სარგებლობენ პერსონალური მონაცემების დაცვის განსაკუთრებული უფლებით, რადგან მათთვის შეიძლება ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, დაცვის მექანიზმები და უფლებები, რომლებიც უკავშირდება პერსონალური მონაცემების დამუშავებას.¹³ განსაკუთრებული დაცვა უნდა შეეხოს:

- არასრულწლოვნების პერსონალური მონაცემების გამოყენებას მარკეტინგის მიზნებისთვის;
- პიროვნების ან მომხმარებლის პირადი ანგარიშის შექმნას;
- არასრულწლოვნებთან დაკავშირებული პერსონალური მონაცემების შეგროვებას ისეთი მომსახურეობის გამოყენებისას, რომლის შეთავაზებაც არასრულწლოვანისათვის პირდაპირ ხდება.¹⁴

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1–88 art. 4 (1); Council of Europe, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf (2018) 15-final), 18/05/2018, article 2 (a).

⁷ German Federal Constitutional Court, 1 BvR 209/83, 269/83, 362/83, 420/83, 440/83, 484/83, 15 December 1983, margin number 150.

⁸ Commission of the European Communities, COM (90) 314, final, 13 September 1990, 19.

⁹ იხ.: WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007, 6.

¹⁰ General Data Protection Regulation, GDPR, Recital 14 sentence 1.

¹¹ კონვენცია ბავშვის უფლებების შესახებ, საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება, 1948, მუხლი 8.

¹² General Data Protection Regulation, GDPR, Recital 14.

¹³ General Data Protection Regulation, GDPR, Recital 38.

¹⁴ General Data Protection Regulation, GDPR, Recital 38.

არასრულწლოვნები მონაცემთა სუბიექტის სტატუსს ითავსებენ სხვადასხვა შემთხვევაში, განსაკუთრებით კი ციფრულ ეპოქაში, სადაც მათი პირადი მონაცემები გროვდება, მუშავდება და ინახება სხვადასხვა მიზნებისთვის. მაგალითისთვის შესაძლოა განხილული იყოს სხვადასხვა შემთხვევები:

ონლაინ სერვისები და სოციალური მედია: დღესდღეობით ბავშვებისთვის დაბრკოლებას არ წარმოადგენს გამოიყენონ სხვადასხვა ონლაინ პლატფორმა, სოციალური ქსელი, აპლიკაცია თუ საიტი, სადაც მათ პერსონალურ მონაცემებს აგროვებენ, რაც მოიცავს პირად ინფორმაციას, ფოტოებს, ვიდეოებს ან სხვა ისეთი ინფორმაციას, რომელსაც შეუძლია მათი იდენტიფიცირება.

საგანმანათლებლო დაწესებულებები: საგანმანათლებლო დაწესებულებები, მათ, შორის, სკოლები აგროვებენ და ინახავენ მონაცემებს მათი მოსწავლეების შესახებ ადმინისტრაციული, საგანმანათლებლო თუ უსაფრთხოების მიზნით. ამგვარი მონაცემები მოიცავს დასწრების ჩანაწერებს, ქულებს, ქცევის ანგარიშებსა და ჯანმრთელობის შესახებ ინფორმაციას, რაც ბავშვებს მონაცემთა სუბიექტებად აქცევს საგანმანათლებლო სივრცეში.

ჯანდაცვის სერვისები: ბავშვის მიერ სამედიცინო დახმარების ან მკურნალობის მიღებისას, ბენეფიციარების ჯანმრთელობის შესახებ ინფორმაცია გროვდება და მუშავდება ჯანდაცვის პროვაიდერების მიერ. რაც მოიცავს სამედიცინო ჩანაწერებს, დიაგნოზებს, მკურნალობის გეგმებსა და რეცეპტებს.

თამაშები და გართობა: ონლაინ თამაშები, აპლიკაციები და გასართობი პლატფორმები ხშირად აგროვებენ ბავშვების მონაცემებს ვირტუალურ გარემოსთან და პერსონაჟებთან ურთიერთობისას, რაც შემდგომში გამოიყენება მომხმარებლის გამოცდილების გასაუმჯობესებლად და შინაარსის მოსარგებად.

კვლევა და გამოკითხვა: ბავშვების მონაცემები შეიძლება დამუშავდეს კვლევითი მიზნებისთვის ან გამოკითხვებისთვის, განსაკუთრებით საგანმანათლებლო ან ფსიქოლოგიურ კვლევებში, რა შემთხვევაშიც, მნიშვნელოვანია, დაცული იყოს მათი კონფიდენციალობის უფლება.

4. არასრულწლოვანთა პერსონალური მონაცემების დამუშავებისას გასათვალისწინებელი საკითხები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონი მიუთითებს, რომ არასრულწლოვნის პერსონალურ მონაცემთა დამუშავება უნდა განხორციელდეს ბავშვის საუკეთესო ინტერესების დაცვით, თუმცა პერსონალურ მონაცემთა დამუშავების პრინციპების ჩამონათვალში არ გხვდება რაიმე დათქმა ამ პრინციპების არასრულწლოვნების მონაცემების დამუშავების დროს ცვლილების შესახებ, რაც მიანიშნებს იმას, რომ მონაცემთა დამუშავების პრინციპების საფუძველზე დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განსაზღვროს პირთა წრე ვისი პერსონალური მონაცემებიც მუშავდება.

ბავშვის უფლებათა კოდექსი არ კრძალავს ბავშვის პერსონალურ მონაცემთა დამუშავებას სხვადასხვა მიზნებისთვის, როგორებიცაა მაგალითად, ჯანმრთელობის დაცვის, განათლების და სოციალური დაცვის სფეროში. ეს უნდა განხორციელდეს ბავშვის საუკეთესო ინტერესებიდან გამომდინარე და მხოლოდ საქართველოს კანონმდებლობის შესაბამისად.¹⁵

¹⁵ კილაძე ს., ტურავა პ., ბავშვის უფლებათა კოდექსის სახელმძღვანელო კომენტარები, თბილისი, 2021, 278.

საქართველოს უზენაესმა სასამართლომ ერთ-ერთ გადაწყვეტილებაში აღნიშნა, რომ ბავშვის უფლებათა კოდექსის 71-ე მუხლი, რომლის პირველი ნაწილის მიხედვით, დაუშვებელია, რაიმე ფორმით, მათ შორის, მედიის საშუალებით, საჯარო გახდეს ადმინისტრაციულ წარმოებაში ან სასამართლო პროცესში მონაწილე ბავშვის პერსონალური მონაცემები, რომლებითაც შეიძლება გამჟღავნდეს ან არაპირდაპირ მიეთითოს ბავშვის ვინაობა (გამოსახულება, ბავშვის ან მისი ოჯახის წევრების დეტალური აღწერა, სახელები, მისამართები, აუდიო- და ვიდეოჩანაწერები და მსგავსი ინფორმაცია) - განუხრელად უნდა იქნეს დაცული. იმავე მუხლის მეორე ნაწილის თანახმად, დაუშვებელია, რაიმე ფორმით, მათ შორის, მედიის საშუალებით, საჯარო გახდეს ბავშვის პერსონალურ მონაცემთა შემცველი ისეთი დოკუმენტი ან ჩანაწერი, რომელიც უკავშირდება ბავშვის მიმართ დისციპლინური ზომის გამოყენებას, ბავშვის მიმართ ან მის მიერ ჩადენილი ძალადობის შემთხვევას, ბავშვის ჯანმრთელობის მდგომარეობას, მეზღუდული შესაძლებლობის მქონე ბავშვის ან ღარიბი ოჯახის სოციალური დახმარების ან საქველმოქმედო პროგრამაში ბავშვის მონაწილეობას და ბავშვთან დაკავშირებულ სხვა, მსგავსი შინაარსის ინფორმაციას. ნორმის მე-3 ნაწილი კი ადგენს, რომ ბავშვის პერსონალურ მონაცემთა დამუშავება დასაშვებია მხოლოდ საქართველოს კანონმდებლობის შესაბამისად. შესაბამისად, პირის პერსონალური მონაცემების დამუშავება, მათ შორის, ფოტოსურათის გამოქვეყნება, გარდა საკანონმდებლო გამონაკლისებისა, დასაშვებია მხოლოდ მონაცემთა სუბიექტის თანხმობით.¹⁶

სასამართლო ხაზგასმით აღნიშნავს, რომ ბავშვის მიმართ ნებისმიერი ქმედების განხორციელებისას გაცილებით მაღალი სტანდარტით უნდა იქნეს დაცული პერსონალური მონაცემები და გამოირიცხოს ბავშვის საუკეთესო ინტერესის ხელყოფა. სასამართლომ განმარტა, რომ საქმეში განსახილველ შემთხვევაში სიუჟეტის კონტექსტის, თემის, მასში გადმოცემული ინფორმაციის გათვალისწინებით, უდავოა, რომ ამავე სიუჟეტში არასრულწლოვნის გამოსახულების გამოქვეყნება არ იყო ბავშვის საუკეთესო ინტერესებით ნაკარნახევი, არ ემსახურებოდა ბავშვის უფლებების დაცვას და გამოიწვევდა არასრულწლოვანში ნეგატიურ განცდებს.

სასამართლო აღნიშნავს, რომ ბავშვს უფლება აქვს, მის მიმართ განხორციელებული ნებისმიერი ქმედებისას ან მასთან დაკავშირებული ნებისმიერი გადაწყვეტილების მიღებისას, შეფასდეს და უპირველესი ყურადღება დაეთმოს მის საუკეთესო/ჭეშმარიტ ინტერესებს როგორც საზოგადოებრივ, ისე კერძო სფეროში.¹⁷

სასამართლო მიუთითებს, რომ მართალია, ბავშვის უფლებათა კოდექსის 71-ე მუხლის პირველი და მეორე ნაწილებით განსაზღვრულია არასრულწლოვნის გამოსახულების გამოქვეყნების დაუშვებლობის კონკრეტული შემთხვევები, მაგრამ ეს შემთხვევები არ უნდა აღვიქვათ ამომწურავ ჩამონათვალად. ნებისმიერი შემთხვევა, რომელიც შეეხება არასრულწლოვანს, განხილულ და გადაწყვეტილ უნდა იქნეს თითოეული გარემოების მხედველობაში მიღებით, ინდივიდუალური საქმის თავისებურებების გათვალისწინებით, არასრულწლოვნის საუკეთესო ინტერესების მიღწევის საუკეთესო გზის შერჩევით. მსგავს მიდგომას მოითხოვს ჟურნალისტური ეთიკის ქარტიაც, რომლის ბავშვის უფლებების დაცვის სავალდებულობას ცალკე პრინციპად განსაზღვრავს და ადგენს, რომ ჟურნალისტი ვალდებულია, დაიცვას

¹⁶ საქართველოს უზენაესი სასამართლოს 2023 წლის 21 სექტემბრის №ას-488-2023 გადაწყვეტილება.

¹⁷ საქართველოს უზენაესი სასამართლოს 2023 წლის 25 დეკემბრის №ა-1351-შ-33-2023 გადაწყვეტილება.

ბავშვის უფლებები; პროფესიული საქმიანობისას უპირატესი მნიშვნელობა მიანიჭოს ბავშვის ინტერესებს, არ მოამზადოს და არ გამოაქვეყნოს ბავშვების შესახებ ისეთი სტატიები ან რეპორტაჟები, რომლებიც საზიანო იქნება მათთვის.¹⁸ შესაბამისად, თითოეულ შემთხვევაში, ჟურნალისტი უნდა უზრუნველყოს იმ ნეგატიური რისკებისა და შედეგების შეფასება, რაც შეიძლება მოჰყვეს არასრულწლოვნის იდენტიფიცირებას. თუკი არსებობს საფრთხე, რომ კონკრეტულ სიუჟეტში არასრულწლოვნის იდენტიფიცირებული ფორმით მონაწილეობა მის უფლებებსა და ქვეყნის ინტერესებზე უარყოფით გავლენას იქონიებს, ბავშვის გამოსახულება მხოლოდ არაიდენტიფიცირებული ფორმით უნდა გამოქვეყნდეს.¹⁹

5. არასრულწლოვნის მონაცემების დამუშავების რისკები და გამოწვევები

მონაცემთა დამუშავება მოიაზრებს ნებისმიერ ქმედებას ან ქმედებათა ერთობლიობას პერსონალურ მონაცემთან ან მონაცემთა ერთობლიობასთან მიმართებაში, რომელიც ხორციელდება ავტომატური თუ სხვა საშუალებებით. მაგალითად: შეგროვება, აღრიცხვა/ჩაწერა, ორგანიზება, სტრუქტურირება, შენახვა, ადაპტაცია ან შეცვლა, ამოღება, გაცნობა, გამოყენება, გამჟღავნება გადაცემის, გავრცელების ან ხელმისაწვდომობის სხვაგვარად უზრუნველყოფის გზით, დაჯგუფება ან კომბინირება, შეზღუდვა, წაშლა ან განადგურება.

ა. ინტერნეტის გამოყენება და სოციალური ქსელებში ბავშვის მონაცემთა დამუშავება

დიდ ყურადღებას მოითხოვს არასრულწლოვნის მიერ ინტერნეტის გამოყენების საკითხი. არასრულწლოვნები შესაძლოა უფრო მეტად და ხშირად იყენებდნენ ონლაინ რესურსებს, ვიდრე მათი მშობლები, რის გამოც მშობლებს შეიძლება საჭიროდ არ მიაჩნდეთ ამ საკითხის საფრთხის სახით განხილვა, რადგან ყოველდღიურ ურთიერთობებში ონლაინ რესურსების გამოყენება ამარტივებს კომუნიკაციის საშუალებებს. ონლაინ რესურსებზე წვდომისას არსებობს არასრულწლოვნის პერსონალური მონაცემების გამჟღავნების, დარღვევის და შესაძლო დანაშაულებრივი ქმედებების: იძულების, თაღლითობის და სხვა რისკები,²⁰ რომელიც განსაკუთრებულად საყურადღებოა. გასათვალისწინებელია ონლაინ რესურსის პლატფორმას აქვს თუ არა პერსონალურ მონაცემთა დაცვის პოლიტიკა და არასრულწლოვნის ყოველდღიურობაზე როგორც აისახება მისი სარგებლობის მასშტაბი. იცნობს თუ არა არასრულწლოვნის მშობელი ან არასრულწლოვანი იმ ონლაინ რესურსის კონფიდენციალურობისა და უსაფრთხოების პარამეტრებს, რომელსაც ყველაზე ხშირად იყენებს. არასრულწლოვნის მონაცემების ინტერნეტში ყველასთვის ხელმისაწვდომი ფორმით გასაჯაროებამ შესაძლოა არასასურველი ზეგავლენა მოახდინოს არასრულწლოვანზე (გახდეს ბულინგის ან სხვა სახის არასასურველი მოპყრობის ობიექტი).²¹

¹⁸ შეად. ფირცხალაშვილი ა., ქარდავა ე., ტურავა პ., სოციალური სამართლის სახელმძღვანელო, თბილისი, 2023, 347-348.

¹⁹ საქართველოს უზენაესი სასამართლოს 2023 წლის 21 სექტემბრის №ას-488-2023 გადაწყვეტილება.

²⁰ გურგენიძე მ., ბავშვის პერსონალური მონაცემების დაცვა ინტერნეტსივრცეში, აღმოსავლეთ ევროპის უნივერსიტეტი, თბილისი, 2020, 31-32.

²¹ European Union, Children's Online Privacy and Data Protection in Selected European Countries, 2021, No. 2021-020137, The Law Library of Congress, Global Legal Research Directorate, 18-19.

ბ. სკოლაში არასრულწლოვნის ქცევის მონიტორინგი და მოსწავლის მონაცემთა დამუშავება

სკოლა უფლებამოსილია განახორციელოს ვიდეოთვალთვალი სკოლის ტერიტორიაზე, მაგრამ მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის, არასრულწლოვნის მავნე ზეგავლენისაგან დაცვისა და საიდუმლო ინფორმაციის დაცვის მიზნებისათვის. ვიდეოგადაღება დასაშვებია მხოლოდ შესასვლელსა და გარე პერიმეტრზე. გამოსაცვლელ ოთახებსა და ჰიგიენისთვის განკუთვნილ ადგილებში ვიდეოთვალთვალი დაუშვებელია. სკოლას უფლება აქვს აკონტროლოს მოსწავლეების შენობაში შესვლა და შენობიდან გასვლა, ასევე, აღრიცხოს ვიზიტორთა სახელი და გვარი, საიდენტიფიკაციო დოკუმენტის ნომერი და სახე, მისამართი, შესვლისა და გასვლის თარიღები და დრო, ასევე შენობაში შესვლისა და შენობიდან გასვლის მიზეზები. ამ მონაცემთა შენახვის ვადა არ უნდა აღემატებოდეს კანონით განსაზღვრულ ვადას.²² სკოლას შეუძლია ფოტო/ვიდეო გადაღებით დააფიქსიროს და შემდგომ გაასაჯაროოს სასწავლო პროცესის მიმდინარეობა, მაგრამ მხოლოდ მონაცემთა სუბიექტის თანხმობით.²³ თანხმობის მიღებისას გათვალისწინებული უნდა იყოს მოსწავლის საუკეთესო ინტერესები. სკოლის ტერიტორიაზე მოსწავლის ყოფნის მთელ პერიოდში იქნება ეს საგაკვეთილო პროცესის თუ დასვენების პერიოდი უნდა განისაზღვროს ის მიზეზები, რომლებიც შეიძლება ჰქონდეს სკოლას მოსწავლის პერსონალური მონაცემების დასამუშავებლად. მაგალითად, ეს შეიძლება იყოს ვიდეომონიტორინგი იმისთვის, რომ საგაკვეთილო პერიოდი უხარვეზოდ წარიმართოს და ამ დროს მოსწავლე არ იმყოფებოდეს საკლასო ოთახს გარეთ. ასევე, ვიდეომონიტორინგი იმისთვის, რომ საგაკვეთილო პროცესში მოსწავლემ არ დატოვოს სკოლის ტერიტორია ან სკოლის ტერიტორიაზე არ მოხდეს უცხო პირთა შესვლა.²⁴ საგანმანათლებლო დაწესებულებები, ამ დაწესებულებებში დასაქმებული პირები, ასევე, არასრულწლოვანი პირების მშობლები და ოჯახის წევრები, მეტი პასუხისმგებლობით უნდა მოეკიდონ ბავშვების მონაცემების გასაჯაროებას და იმოქმედონ არასრულწლოვნის საუკეთესო ინტერესების გათვალისწინებით.²⁵

გ. სამედიცინო დაწესებულებაში ბავშვის მონაცემების დამუშავება

არასრულწლოვანთა ჯანმრთელობასთან დაკავშირებული მონაცემების გაცემის შემთხვევაში განსაკუთრებული ყურადღება უნდა დაეთმოს ინფორმაციის შემდგომი გამოყენების რისკების შეფასებას. არასრულწლოვანთა მონაცემები საქიროებს უფრო მეტ დაცვას, ამ მიზნით კი მონაცემთა თითოეული დამმუშავებელი ვალდებულია უპირველესად მოქმედებდეს არასრულწლოვნის საუკეთესო ინტერესიდან გამომდინარე. მშობლების თანხმობის მიუხედავად, ბავშვის საუკეთესო ინტერესების გათვალისწინებით, საჯარო ინფორმაციის სახით მისი ჯანმრთელობის მდგომარეობასთან დაკავშირებული ან სხვა განსაკუთრებული კატეგორიის მონაცემთა მესამე პირისთვის გამჟღავნება დაუშვებელია და განიხილება

²² შეად. European Data Protection Supervisor, Study on the Essence of the Fundamental Rights to Privacy and to the Protection of Personal Data, EDPS 2021/0932, December 2022.

²³ Guide to the General Data Protection Regulation, Bird & Bird, 2020, 6-7.

²⁴ იხ. სუხაშვილი ნ., დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა, სტატიათა კრებული: პერსონალურ მონაცემთა დაცვის აქტუალური პრობლემები და გამოწვევები, თბილისი, 2021, 9-10.

²⁵ შეად. გორგილაძე ა., ძალადობის მსხვერპლი ბავშვების პერსონალური მონაცემების დაცვა, პერსონალურ მონაცემთა დაცვის თავისებურებები (სტატიათა კრებული), 2020, 55.

არაპროპორციულ და მონაცემთა დამუშავების მიზნის შეუსაბამო მოქმედებად.²⁶ რისკების შეფასებისას მნიშვნელოვანია განისაზღვროს თუ საიდან შეიძლება გამომდინარეობდეს არასრულწლოვნის პერსონალური მონაცემების დამუშავების უფლება.²⁷

დ. პერსონალური მონაცემების დამუშავების კონტექსტში გასათვალისწინებელი საკითხები

ბავშვის სიცოცხლისა და პიროვნული განვითარების უფლება გულისხმობს, რომ ბავშვს აქვს სიცოცხლისა და პიროვნული განვითარების უფლება. სახელმწიფო იღებს ბავშვის სიცოცხლის დასაცავად საჭირო ყველა ზომას და ქმნის მისი ჰარმონიული განვითარებისთვის საჭირო ყველა პირობას ბავშვის უფლებათა კოდექსის, საქართველოს კონსტიტუციის, ბავშვის უფლებათა კონვენციის, მისი დამატებითი ოქმების, საქართველოს სხვა საერთაშორისო ხელშეკრულებებისა და სხვა სამართლებრივი აქტების შესაბამისად.

ბავშვის განათლების უფლება გულისხმობს, რომ ყველა ბავშვს აქვს ხარისხიანი და ინკლუზიური განათლების მიღებისა და თანაბარი ხელმისაწვდომობის უფლება. სახელმწიფო უზრუნველყოფს განათლების ინკლუზიური სისტემის ყველა ბავშვისთვის თანაბარ ხელმისაწვდომობას.

ბავშვის პირადი და ოჯახური ცხოვრების უფლება გულისხმობს, რომ ბავშვს უფლება აქვს, ჰქონდეს პირადი სივრცე, აწარმოოს პირადი მიმოწერა. დაუშვებელია ბავშვის პირადი და ოჯახური ცხოვრების უფლების უკანონო შეზღუდვა, მათ შორის, მის პირად სივრცეში, ოჯახურ ცხოვრებაში ან პირად მიმოწერაში დაუსაბუთებელი და არაკანონიერი ჩარევა.

ბავშვის აზრის, ინფორმაციის, მასობრივი ინფორმაციის საშუალებებითა და ინტერნეტით სარგებლობის თავისუფლების უფლებები გულისხმობს, რომ ბავშვს უფლება აქვს, თავისუფლად გამოხატოს საკუთარი აზრი. ბავშვს ასევე უფლება აქვს, მოუსმინონ მასთან დაკავშირებული გადაწყვეტილების მიღებისას და გაითვალისწინონ ბავშვის მოსაზრება მისი ასაკისა და გონებრივი და ფიზიკური განვითარების შესაბამისად. ბავშვს უფლება აქვს, თავისუფლად მოიძიოს, მიიღოს და გაავრცელოს ინფორმაცია სხვადასხვა საშუალებითა და ფორმით. ბავშვს აქვს მასობრივი ინფორმაციის საშუალებებისა და ინტერნეტის ხელმისაწვდომობის და ინტერნეტით თავისუფლად სარგებლობის უფლება.

გამოწვევათა საპასუხოდ ფართოდ უნდა განიმარტოს ნორმა, რომელიც „პერსონალურ მონაცემთა დაცვის“ შესახებ საქართველოს ახალმა კანონმა დანერგა. ამ კანონის მე-7 მუხლში მოცემულია არასრულწლოვანის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესი და პირობები. ეს მუხლი განსაზღვრავს, რომ არასრულწლოვანის შესახებ მონაცემთა დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია გაითვალისწინოს და დაიცვას არასრულწლოვანის საუკეთესო ინტერესები, ხოლო არასრულწლოვანის, მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა მონაცემთა დამუშავებაზე არ ჩაითვლება ნამდვილად, თუ მონაცემთა დამუშავება საფრთხეს უქმნის ან ზიანს აყენებს არასრულწლოვანის საუკეთესო ინტერესებს.

²⁶ სახელმწიფო ინსპექტორის სამსახურის გადაწყვეტილებები, ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავება, 2020.

²⁷ დამატებით იხ. არჩუაძე თ., პერსონალურ მონაცემთა დეპერსონალიზაცია, როგორც მონაცემთა სუბიექტის დაცვის გარანტია, საკონსტიტუციო სამართლის ჟურნალი, 5/2020, 117.

2022 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა არასრულწლოვნების პერსონალური მონაცემების დამუშავების 39 შემთხვევა, რომელთაგან 27 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, ხოლო 12 მოქალაქეთა განცხადების / შეტყობინების საფუძველზე. სამსახურში წარმოდგენილი განცხადებები ძირითადად შეეხებოდა არასრულწლოვანთა პერსონალური მონაცემების სამედიცინო დაწესებულების მიერ უკანონო გამჟღავნებას, ვიდურობათვალის წესების დარღვევას, პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა დარღვევით დამუშავებასა და სხვა ფაქტებს, სადაც კანონის მოთხოვნათა დარღვევით დამუშავდა არასრულწლოვნის პერსონალური მონაცემები.

6. დასკვნა

არასრულწლოვნის პერსონალური მონაცემების დამუშავებასთან დაკავშირებული გამოწვევების საერთო მასშტაბი ფართო და მრავალმომცველია, რადგან მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის ჯერ კიდევ არ აღიქმება ნათლად თუ რა ფორმით და ხარისხით უნდა დამუშავდეს არასრულწლოვნის პერსონალური მონაცემები.

გამომდინარე იქედან, რომ პერსონალურ მონაცემთა დაცვის სამსახურის ძირითად მიმართულებებს შორის ერთ-ერთია მონაცემთა დაცვის მდგომარეობისა და მასთან დაკავშირებული მნიშვნელოვანი მოვლენების შესახებ ინფორმაციის საზოგადოებისთვის მიწოდება და მისი ინფორმირებულობის გაზრდა, განსაკუთრებულ მნიშვნელობას იძენს არასრულწლოვნების პერსონალური მონაცემების დამუშავების შესახებ არა მხოლოდ ცნობიერების ამაღლება, არამედ ერთგვარი სტრატეგიების შემუშავება, ინსპექტირების მოქნილი მოდელისა და შესაბამისი სტანდარტების განსაზღვრა ახალი კანონის მე-7 მუხლის მოქმედებასთან დაკავშირებით.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ამოქმედებასთან ერთად საყურადღებოა კანონის მოთხოვნათა ასახვა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მოქმედებებში, რომლებიც არასრულწლოვნების პერსონალურ მონაცემებს ამუშავებენ. არასრულწლოვნებში თავიანთი უფლებების შესახებ ცნობიერების ამაღლება მნიშვნელოვნად განსაზღვრავს პერსონალურ მონაცემთა დაცვის შესახებ გამოწვევების დროულ გამოვლენას და ხელს შეუწყობს საპასუხო ნაბიჯების გადადგმას.

ბიბლიოგრაფია:

1. კონვენცია ბავშვის უფლებების შესახებ, 1948.
2. ევროპის საბჭოს 108-ე კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 1981.
3. მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR), 2016.
4. ევროპის საბჭოს 108-ე მოდერნიზებული კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2018.
5. საქართველოს კანონი „ბავშვის უფლებათა კოდექსი“, 5004-ლს, 20/09/2019.

6. საქართველოს კანონი “პერსონალურ მონაცემთა დაცვის შესახებ”, 3144-XIმს-Xმპ, 14/06/2023.
7. არჩუაძე თ., პერსონალურ მონაცემთა დეპერსონალიზაცია, როგორც მონაცემთა სუბიექტის დაცვის გარანტია, საკონსტიტუციო სამართლის ჟურნალი, 5/2020, 117.
8. გოშაძე კ., პერსონალურ მონაცემთა დაცვისა და დამუშავების კონსტიტუციურ-სამართლებრივი გარანტიები, საქართველოს უნივერსიტეტი, თბილისი, 2017, 43.
9. გორგილაძე ა., ძალადობის მსხვერპლი ბავშვების პერსონალური მონაცემების დაცვა, პერსონალურ მონაცემთა დაცვის თავისებურებები (სტატიათა კრებული), 2020, 55.
10. გურგენიძე მ., ბავშვის პერსონალური მონაცემების დაცვა ინტერნეტიზაციაში, აღმოსავლეთ ევროპის უნივერსიტეტი, თბილისი, 2020, 31-32.
11. ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, ევროკავშირის საგამომცემლო სახლი, 2018, 20-21.
12. კილაძე ს., ტურავა პ., ბავშვის უფლებათა კოდექსის სახელმძღვანელო კომენტარები, თბილისი, 2021, 278.
13. სახელმწიფო ინსპექტორის სამსახურის გადაწყვეტილებები, ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავება, 2020.
14. სუბაშვილი ნ., დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა, სტატიათა კრებული: პერსონალურ მონაცემთა დაცვის აქტუალური პრობლემები და გამოწვევები, თბ., 2021, 9-10.
15. ფირცხალაშვილი ა., ქარდავა ე., ტურავა პ., სოციალური სამართლის სახელმძღვანელო, თბილისი, 2023, 347-348.
16. შუდრა თ., ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, 1/2023, 112-115.
17. საქართველოს უზენაესი სასამართლოს 2023 წლის 21 სექტემბრის №ას-488-2023 გადაწყვეტილება.
18. საქართველოს უზენაესი სასამართლოს 2023 წლის 25 დეკემბრის №ა-1351-მ-33-2023 გადაწყვეტილება.
19. Commission of the European Communities, COM (90) 314, final, 13 September 1990, 19.
20. European Union, Children’s Online Privacy and Data Protection in Selected European Countries, 2021, No. 2021-020137, The Law Library of Congress, Global Legal Research Directorate, 18-19.
21. Guide to the General Data Protection Regulation, Bird & Bird, 2020, 6-7.
22. ICO, Children and the GDPR, 2018, 1.
23. European Data Protection Supervisor, Study on the Essence of the Fundamental Rights to Privacy and to the Protection of Personal Data, EDPS 2021/0932, December 2022.
24. WP29, Opinion 4/2007 on the Concept of Personal Data, 2007, 6.

პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები)

პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემა როგორც საქართველოს, ისე საერთაშორისო რეალობაში კომპლექსურ საკითხს წარმოადგენს. აღსანიშნავია, რომ სახელმწიფოთა თანამშრომლობის ფარგლებში, სხვადასხვა სფეროში გადაიცემა დიდი რაოდენობის პერსონალური მონაცემი, რაც საჭიროებს ეფექტიან რეგულირებას მონაცემთა სუბიექტის უფლებების დაცვის თვალსაზრისით.

საკვანძო სიტყვები: პერსონალურ მონაცემთა საერთაშორისო/ტრანსსასაზღვრო გადაცემა, პერსონალურ მონაცემთა დაცვის სამსახური, შესაბამისობის გადაწყვეტილება, მონაცემთა დაცვის სათანადო გარანტიები, მონაცემთა სუბიექტის უფლებები.

1. შესავალი

თანამედროვე სამყაროში საერთაშორისო დონეზე პერსონალური მონაცემების გადაცემის საკითხი დღითიდღე აქტუალური ხდება. სახელმწიფოთა/საერთაშორისო ორგანიზაციათა შორის, სხვადასხვა სფეროში თანამშრომლობის გაღრმავების მიზნით, უწყვეტ რეჟიმში, ხორციელდება პერსონალური მონაცემების მიმოცვლა, რაც, ერთი მხრივ, სარგებლის მომტანია, თუმცა, მეორე მხრივ, წარმოშობს გარკვეულ რისკებს პერსონალურ მონაცემთა დაცვის თვალსაზრისით.

უპირველეს ყოვლისა, გასაანალიზებელია სახელმწიფოთა შორის პერსონალურ მონაცემთა დაცვის კანონმდებლობის თავსებადობა. რიგი საკითხების განსხვავებული მოწესრიგებით შეიძლება, დაირღვეს მონაცემთა სუბიექტის უფლებები და პერსონალურ მონაცემთა დაცვის სტანდარტები. შესაბამისად, ჩნდება კითხვები: რა ეროვნული და საერთაშორისო სამართლებრივი მექანიზმები არსებობს პერსონალურ მონაცემთა საერთაშორისო გადაცემის მიმართულებით? თუ კონკრეტულ სახელმწიფოში სათანადოდ არ არის დაცული პერსონალური მონაცემები, რამდენად გამოირიცხება პერსონალურ მონაცემთა გადაცემის შესაძლებლობა? სათანადო სამართლებრივი რეგულირების არარსებობის პირობებში, როგორ უნდა იქნას უზრუნველყოფილი პერსონალურ მონაცემთა დაცულობა? რა ბერკეტები გააჩნია პერსონალურ მონაცემთა დაცვის სამსახურს

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის საერთაშორისო სამართლის მაგისტრი, პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის მკვლევარ-ანალიტიკოსი.

პერსონალურ მონაცემთა საერთაშორისო გადაცემის რეგულირების თვალსაზრისით?

წინამდებარე სტატიის ფარგლებში შეფასდება პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი ასპექტები. განიხილება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის¹ V თავით გათვალისწინებული მოთხოვნები მონაცემთა საერთაშორისო გადაცემის თაობაზე. წარმოდგენილი იქნება საერთაშორისო საკანონმდებლო ჩარჩო და სტანდარტები, ევროპული კომისიისა² და მონაცემთა დაცვის ევროპული საბჭოს („EDPB“³) მიერ შემუშავებული სარეკომენდაციო დოკუმენტები, საზღვარგარეთის მონაცემთა დაცვის საზედამხებელო ორგანოთა პრაქტიკა, რომელთა ანალიზის საფუძველზეც პასუხი გაეცემა დასმულ კითხვებს.

2. მონაცემთა საერთაშორისო გადაცემის ეროვნული მოწესრიგება

2024 წლის პირველ მარტს, ძალაში შევიდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (კანონი),⁴ რომლის ძირითადი მიზანი პერსონალური მონაცემების დაცვის სტანდარტებისა და გარანტიების უზრუნველყოფაა. ახალი კანონით ახლებურად რეგულირდება პერსონალურ მონაცემთა დაცვის სფეროში მნიშვნელოვანი საკითხები, მათ შორის, მონაცემთა საერთაშორისო გადაცემის მიმართულებით.

პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა მოწესრიგებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე მუხლით, რომლის შესაბამისადაც 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.⁵

გარდა აღნიშნულისა, 37-ე მუხლის მე-2 პუნქტის თანახმად, მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ:

- საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება ითვალისწინებს მონაცემთა გადაცემას;
- დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს;
- მონაცემთა გადაცემა ხორციელდება „გ“ ქვეპუნქტით გათვალისწინებული კანონმდებლობის საფუძველზე (სისხლის სამართლის საპროცესო კოდექსი; „უცხოელთა და მოქალაქეობის არმქონე პირთა სამართლებრივი მდგომარეობის შესახებ“ საქართველოს კანონი; „სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონი; „სამართალდაცვით სფეროში საერთაშორისო თანამშრომლობის

¹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.

² European Commission, the Executive Body of the European Union, <https://commission.europa.eu/about-european-commission_en> [03.08.2024].

³ The European Data Protection Board, <https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en> [03.08.2024].

⁴ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.

⁵ იქვე, 37-ე მუხლის პირველი პუნქტი.

შესახებ“ საქართველოს კანონი; „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონი; „ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ“ საქართველოს კანონის საფუძველზე მიღებული ნორმატიული აქტი);

- შესაბამის სახელმწიფოში მონაცემთა დაცვის სათანადო გარანტიების არარსებობისა და შესაძლო საფრთხეების შესახებ ინფორმაციის მიღების შემდეგ მონაცემთა სუბიექტი განაცხადებს წერილობით თანხმობას;
- მონაცემთა გადაცემა აუცილებელია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არ აქვს, მონაცემთა დამუშავებაზე თანხმობა განაცხადოს;
- არსებობს კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესი (მათ შორის, დანაშაულის თავიდან აცილება, გამოძიება, გამოვლენა და სისხლისსამართლებრივი დევნა, სასჯელის აღსრულება და ოპერატიულ-სამძებრო ღონისძიებების განხორციელება) და მონაცემთა გადაცემა აუცილებელი და პროპორციული ზომია დემოკრატიულ საზოგადოებაში.⁶

გასათვალისწინებელია, რომ დამუშავებისთვის პასუხისმგებელი პირის მიერ ხელშეკრულების შესაბამისად სათანადო გარანტიების უზრუნველყოფის შემთხვევაში,⁷ მონაცემთა გადაცემა შეიძლება მხოლოდ პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვის მიღების შემდეგ, რომლის გაცემის წესი დგინდება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით.⁸ აღნიშნულ შემთხვევაში, მონაცემთა გადაცემის შესახებ შეთანხმება სავალდებულო სამართლებრივი ძალის მქონე შესასრულებელ პირობებს უნდა ითვალისწინებდეს.⁹ ამასთან, ჩამოთვლილი საფუძვლებით მონაცემთა გადაცემის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია, მიიღოს მონაცემთა უსაფრთხო გადაცემისთვის აუცილებელი ორგანიზაციული და ტექნიკური ზომები.¹⁰

ამავე მუხლის მე-6 პუნქტის გათვალისწინებით, მესამე მხარისთვის სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემული მონაცემების შემდგომი გადაცემა დასაშვებია მხოლოდ იმ შემთხვევაში, თუ ამგვარი გადაცემა თავდაპირველი მიზნებითაა განპირობებული და აკმაყოფილებს მონაცემთა გადაცემისთვის ამ მუხლით გათვალისწინებულ საფუძვლებსა და მონაცემთა დაცვის სათანადო გარანტიებს.

3. პერსონალურ მონაცემთა დაცვის სამსახურის საზედამხედველო ბერკეტები მონაცემთა ტრანსსასაზღვრო გადაცემის მიმართულებით

პერსონალურ მონაცემთა დაცვის სამსახურის (შემდგომში - სამსახური) ერთ-ერთ ძირითად ფუნქციას პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის

⁶ იქვე, 37-ე მუხლის მე-2 პუნქტი.

⁷ იქვე, 37-ე მუხლის მე-2 პუნქტის „ბ“ ქვეპუნქტი.

⁸ იქვე, 37-ე მუხლის მე-3 პუნქტი.

⁹ იქვე, 37-ე მუხლის მე-5 პუნქტი.

¹⁰ იქვე, 37-ე მუხლის მე-4 პუნქტი.

კონტექსტში კანონიერების ზედამხედველობა წარმოადგენს. კერძოდ, როდესაც საქართველოს სახელით დასადები საერთაშორისო ხელშეკრულებისა და შეთანხმებების პროექტები ითვალისწინებს პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის შესაძლებლობას, შესაბამისი უწყების მომართვის საფუძველზე, სამსახური ატარებს აღნიშნული დოკუმენტების სამართლებრივ ექსპერტიზას.

სამსახური ხელშეკრულების სამართლებრივი ექსპერტიზის განხორციელებისას ითვალისწინებს შესაბამის სახელმწიფოში/საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას. აღნიშნულის გათვალისწინებით, სამართლებრივი ექსპერტიზის ფარგლებში, სამსახური შეისწავლის წარმოდგენილი ხელშეკრულებების/შეთანხმებების პროექტებს, მხარე სახელმწიფოში პერსონალურ მონაცემთა დაცვის სფეროში არსებულ საკანონმდებლო და ინსტიტუციურ მექანიზმებს, რომლის საფუძველზეც, საჭიროებისამებრ, გაიცემა შეთანხმების/ხელშეკრულების პროექტში ცვლილებების რეკომენდაცია.

პერსონალურ მონაცემთა დაცვის სამსახური, სხვა სახელმწიფოში ან/და საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას აფასებს მონაცემთა დაცვასთან დაკავშირებით ნაკისრი საერთაშორისო ვალდებულებებისა და მარეგულირებელი კანონმდებლობის, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის გარანტიების (მათ შორის, ეფექტიანი სამართლებრივი დაცვის მექანიზმების), მონაცემთა შემდგომი საერთაშორისო გადაცემის წესების, მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოს არსებობის, უფლებამოსილებებისა და საქმიანობის ანალიზის საფუძველზე.¹¹

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანებით დამტკიცებულია პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხა,¹² რომლებშიც მონაცემთა გადაცემა, სათანადო საფუძვლების არსებობის შემთხვევაში, მიიჩნევა უსაფრთხოდ. აღნიშნულ სიაში ასახულია როგორც ევროკავშირის წევრი, ასევე, ის ქვეყნები, რომლებთან მიმართებითაც ევროპული კომისიის მიერ მიღებულია შესაბამისობის გადაწყვეტილება.¹³

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 38-ე მუხლის მე-3 პუნქტის შესაბამისად, განსაზღვრული ნუსხა მინიმუმ 3 წელიწადში ერთხელ უნდა გადაიხედოს. თუ სახელმწიფო ან/და საერთაშორისო ორგანიზაცია აღარ აკმაყოფილებს კანონის მოთხოვნებს, ნორმატიული აქტით განსაზღვრულ ნუსხაში შეტანილი უნდა იქნეს შესაბამისი ცვლილებები, რომლებსაც უკუქვევითი ძალა არ ექნება.

ამასთანავე, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის პირველი მარტის №33 ბრძანების საფუძველზე, შემუშავებულია პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესი და დამტკიცებულია განაცხადის ფორმა, რომელიც

¹¹ იქვე, 38-ე მუხლის პირველი პუნქტი.

¹² პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანება „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“.

¹³ იხ. 3.2. თავი: „პერსონალური მონაცემების გადაცემა ევროკავშირის არაწევრ სახელმწიფოში, ევროპული კომისიის მიერ მიღებული შესაბამისობის გადაწყვეტილების საფუძველზე“.

განსაზღვრავს განაცხადისა და შესაბამისი დოკუმენტაციის წარდგენის, მათი განხილვის, გადაწყვეტილების მიღების, ნებართვის გაცემის წესსა და პირობებს.¹⁴

4. საერთაშორისო სტანდარტები პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის შესახებ

4.1. საერთაშორისო საკანონმდებლო ჩარჩოს ზოგადი მიმოხილვა

„პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ“ ევროპის საბჭოს 108-ე კონვენციის¹⁵ (შემდგომში - 108-ე კონვენცია) მე-12 მუხლი არეგულირებს პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემების საკითხს. მასში წარმოდგენილია დებულებები, რომლებიც უნდა იქნეს გამოყენებული სახელმწიფო საზღვარზე პერსონალური მონაცემების ნებისმიერი საშუალებით გადაცემის მიმართ. ამავე მუხლის მე-3 პუნქტის თანახმად, მხარეს მხოლოდ კონფიდენციალობის დაცვის მოტივით, უფლება არ აქვს ხელი შეუშალოს პერსონალური მონაცემების გადაცემას სხვა მხარის ტერიტორიაზე ან მოითხოვოს ამისათვის სპეციალური ნებართვა. თუმცა, კონვენციის მე-3 პუნქტი შეიცავს გამონაკლისებს, რა შემთხვევაშიც მხარე უფლებამოსილია არ დაეთანხმოს მე-2 პუნქტის დებულებას:

- თუ მისი კანონმდებლობა შეიცავს განსაკუთრებულ დებულებებს პერსონალური მონაცემების ავტომატიზებული ფაილების განსაზღვრული კატეგორიებისათვის. აღნიშნულში არ მოიაზრება ისეთი შემთხვევა, როდესაც სხვა მხარის კანონმდებლობა ითვალისწინებს ეკვივალენტურ დაცვას;
- როდესაც გადაცემა ხორციელდება სხვა ქვეყნის ტერიტორიაზე არსებული შუამავლის მეშვეობით მისი ტერიტორიიდან იმ სახელმწიფოს ტერიტორიაზე, რომელიც არ წარმოადგენს ხელშეკრულების მონაწილეს.

ევროპის საბჭოს 108-ე კონვენციის დამატებითი ოქმი¹⁶ საზედამნებლო ორგანოებისა და მონაცემთა ტრანსსასაზღვრო მიმოცვლის საკითხებს შეეხება. პრეამბულაში ყურადღება მახვილდება სახელმწიფოთა შორის პერსონალური მონაცემების მიმოცვლის ინტენსივობის ზრდის პირობებში ადამიანის უფლებებისა და ძირითადი თავისუფლებების, განსაკუთრებით პირადი ცხოვრების ხელშეუხებლობის დაცვის მნიშვნელობაზე. სამართლებრივი დოკუმენტის მე-2 მუხლი აწესრიგებს პერსონალური მონაცემების საერთაშორისო გადაცემას ისეთი მიმღებისთვის, რომელზეც კონვენციის მხარის იურისდიქცია არ ვრცელდება. პირველი პუნქტის გათვალისწინებით, მონაცემთა გადაცემისას სახელმწიფოსა თუ ორგანიზაციის მიერ სათანადო დონეზე უნდა იქნას დაცული პერსონალური

¹⁴ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის პირველი მარტის №33 ბრძანება „პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესის და პერსონალურ მონაცემთა სხვა სახელმწიფოს ან/და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე განაცხადის ფორმის დამტკიცების შესახებ“.

¹⁵ CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.

¹⁶ CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, European Treaty Series - No. 181, 2001, <<https://rm.coe.int/1680080626>> [03.08.2024].

მონაცემები. მე-2 პუნქტის შესაბამისად, ყოველ მხარეს შეუძლია პერსონალური მონაცემების გადაცემა, თუ:

- აღნიშნულის საფუძველია შიდასახელმწიფოებრივი კანონმდებლობა (მონაცემთა შინაარსისადმი არსებული კონკრეტული ინტერესების ან ლეგიტიმური უპირატესი ძალის მქონე ინტერესების არსებობა);
- პერსონალურ მონაცემთა გადაცემაზე დამუშავებისთვის პასუხისმგებელი პირი სახელშეკრულებო დებულებებიდან გამომდინარე უზრუნველყოფს უსაფრთხოების ზომებს, რომლებიც შესაბამისობაში უნდა იყოს კომპეტენტური ორგანოების შიდასახელმწიფოებრივ კანონმდებლობასთან.

ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის¹⁷ მე-14 მუხლში წარმოდგენილია დებულებები პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის თაობაზე. აღნიშნული მუხლის მიზანია ინფორმაციის თავისუფალი მიმოცვლის ხელშეწყობა. მონაცემთა საერთაშორისო მიმოცვლა ნიშნავს პერსონალური მონაცემების გადაცემას იმ მიმღებთათვის, რომლებიც სხვა იურისდიქციას ექვემდებარებიან. მონაცემთა საერთაშორისო მიმოცვლა მიმღებთან, რომელზეც ხელშემკვრელი სახელმწიფოს იურისდიქცია არ ვრცელდება, ნებადართულია მხოლოდ იმ შემთხვევაში, თუ მონაცემები დაცულია სათანადო დონეზე.¹⁸

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ („GDPR“)¹⁹ მე-5 თავი აწესრიგებს მესამე სახელმწიფოსთვის²⁰ ან საერთაშორისო ორგანიზაციისთვის პერსონალური მონაცემების გადაცემის საკითხებს. მესამე ქვეყნისთვის ან საერთაშორისო ორგანიზაციისთვის პერსონალური მონაცემების გადაცემისას უნდა იქნას უზრუნველყოფილი მონაცემთა დაცვის სტანდარტები.²¹ მოცემულ შემთხვევაში, გასათვალისწინებელია ე.წ. „ორსაფეხურიანი მიდგომა“:²² პირველ ეტაპზე, მონაცემების გადაცემა უნდა შეესაბამებოდეს ევროკავშირის მონაცემთა დაცვის მოთხოვნებს და ეფუძნებოდეს მონაცემთა სუბიექტის თანხმობას ან სხვა სავალდებულო ნებართვას; მეორე ეტაპზე, გადაცემა თანხვედრაში უნდა იყოს რეგულაციით გათვალისწინებულ მოთხოვნებთან. მონაცემთა დაცვის სათანადო გარანტიების არარსებობის შემთხვევაში, პერსონალური მონაცემები არ უნდა გადაიცეს.²³

ევროკავშირის კანონმდებლობის თანახმად, ევროპის ეკონომიკური ზონის ქვეყნებთან პერსონალური მონაცემების მიმოცვლა ისეთი მიზნებით, როგორიცაა სისხლის სამართლის დანაშაულების პრევენცია, გამოძიება, გახსნა, დამნაშავეთა

¹⁷ CoE, Convention 108 +, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.

¹⁸ CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, §102 <<https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>> [03.08.2024].

¹⁹ EU, 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), <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>> [03.08.2024].

²⁰ მესამე სახელმწიფოებში მოიაზრება ევროკავშირის არაწევრი ქვეყნები.

²¹ იქვე, Article 44.

²² The EU General Data Protection Regulation (GDPR), A Practical Guide, 117.

²³ იქვე.

დასჯა ან სისხლისსამართლებრივი სასჯელის აღსრულება, საპოლიციო სექტორში პერსონალური მონაცემების დამუშავების შესახებ ღირეუქივას ექვემდებარება.²⁴ აღნიშნულის მიზანია, პერსონალური მონაცემების გაცვლა უფლებამოსილი ორგანოების მიერ ევროკავშირის ფარგლებში არ აიკრძალოს/შეიზღუდოს მონაცემთა დაცვასთან დაკავშირებული მიზეზებით.²⁵

4.2. პერსონალური მონაცემების გადაცემა ევროკავშირის არაწევრ სახელმწიფოში, ევროპული კომისიის მიერ მიღებული შესაბამისობის გადაწყვეტილების საფუძველზე

ევროპულ კომისიას, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 45-ე მუხლის საფუძველზე, მინიჭებული აქვს უფლებამოსილება, განსაზღვროს ევროკავშირის არაწევრ სახელმწიფოში მონაცემთა დაცვის სათანადო დონის არსებობა. შესაბამისობის გადაწყვეტილების მიღება მოიცავს შემდეგ ეტაპებს:

- ევროპული კომისიის წინადადება;
- მონაცემთა დაცვის ევროპული საბჭოს („EDPB“) მოსაზრება;
- ევროკავშირის წევრი სახელმწიფოების წარმომადგენელთა თანხმობა;
- ევროპული კომისიის მიერ გადაწყვეტილების მიღება.

შესაბამისობის გადაწყვეტილების საფუძველზე, შესაძლებელია მესამე ქვეყნებში პერსონალური მონაცემების გადაცემა სხვა დამატებითი გარანტიების არსებობის გარეშე. კონკრეტულად, მოცემულ შემთხვევაში გავრცელდება იგივე სტანდარტები, რაც ევროკავშირის წევრ ქვეყნებში მოქმედებს.

ევროპული კომისია ვალდებულია, პერიოდულად გადახედოს შესაბამისობის გადაწყვეტილებას და ანალიზის შედეგების შესახებ აცნობოს ევროპულ პარლამენტსა და საბჭოს. ევროპულ პარლამენტსა და საბჭოს, ნებისმიერ დროს, შეუძლია მოსთხოვოს ევროპულ კომისიას შესაბამისობის გადაწყვეტილების ძალაში დატოვება, შესწორება ან გამოსხმობა, თუკი დაირღვევა „GDPR“-ით გათვალისწინებული მოთხოვნები.²⁶

4.3. პერსონალურ მონაცემთა გადაცემა ევროკავშირის არაწევრ ქვეყნებში, მონაცემთა დაცვის სათანადო გარანტიების საფუძველზე

ევროკავშირის არაწევრ ქვეყნებში, რომლებთან მიმართებითაც არ არის მიღებული შესაბამისობის გადაწყვეტილება, აპრიორი არ გამოირიცხება პერსონალური მონაცემების გადაცემის შესაძლებლობა. მოცემულ შემთხვევაში,

²⁴ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and repealing Council Framework Decision 2008/977/JHA.

²⁵ მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 287.

²⁶ European Commission, Adequacy decisions,

<https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> [03.08.2024].

დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს პერსონალური მონაცემების სათანადო დაცულობა ალტერნატიული საშუალებებით. ამავდროულად, ფიზიკურ პირებს უნდა შეეძლოთ მათთვის მინიჭებული უფლებებით სარგებლობა.²⁷

“GDPR”-ის 46-ე მუხლში წარმოდგენილია სხვადასხვა საშუალება, რომლის მეშვეობით, კერძო ორგანიზაციების მიერ, შესაბამისობის გადაწყვეტილების არარსებობის პირობებში, შესაძლებელია სათანადო გარანტიების დაცვა. კერძოდ, უნდა იქნას შემუშავებული:

- მონაცემთა დაცვის სტანდარტული დებულებები;²⁸
- შესასრულებლად სავალდებულო კორპორაციული წესები;²⁹
- ქვეყნის კოდექსები;
- სერტიფიცირების მექანიზმები;
- ხელშეკრულების სტანდარტული პირობები უშუალოდ მონაცემთა გადაცემის შესახებ^{30, 31}

დამატებით, მესამე ქვეყნებში პერსონალური მონაცემების გადაცემა შესაბამისობის გადაწყვეტილების არარსებობისას შეიძლება, დასაშვები იყოს მონაცემთა სუბიექტის თანხმობის საფუძველზე, რომელიც უნდა გაიცეს თავისუფალი ნებით, ასევე, ხელშეკრულებით გათვალისწინებული ვალდებულების შესასრულებლად, მნიშვნელოვანი საჯარო ინტერესის დასაცავად და სხვა.³²

წარმოდგენილ საკითხთან მიმართებით, უნდა აღინიშნოს ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”) გადაწყვეტილება “*Maximillian Schrems*”³³-ის საქმეზე, რომლის ფარგლებშიც ხაზი გაესვა ევროპის ეკონომიკური ზონის ფარგლებს გარეთ პერსონალური მონაცემების გადაცემისას, სათანადო გარანტიების არსებობასთან ერთად, დამატებითი ზომების მიღების საჭიროებას. სასამართლოს შეფასებით, მონაცემთა გადაცემისას დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა შეაფასონ ევროკავშირის არაწევრ ქვეყანაში არსებული კანონმდებლობისა და პრაქტიკის პოტენციური გავლენა სათანადო გარანტიების მოქმედების ეფექტიანობაზე.³⁴

მონაცემთა დაცვის ევროპულმა საბჭომ შეიმუშავა სახელმძღვანელო რეკომენდაციები ევროკავშირის წევრ ქვეყნებსა და ორგანიზაციებს და არაწევრ ქვეყნებსა და ორგანიზაციებს შორის პერსონალური მონაცემების გადაცემის შესახებ. აღნიშნული დოკუმენტის შემუშავების მიზანს წარმოადგენდა, “GDPR”-ით დადგენილი მოთხოვნების გათვალისწინებით, შესაბამისობის გადაწყვეტილების არარსებობის პირობებში მონაცემთა საერთაშორისო გადაცემის რეგულირება. ხელშეკრულების მხარეები არ იზღუდებიან შეთანხმებაში დამატებითი გარანტიების ასახვის თვალსაზრისით. დოკუმენტში წარმოდგენილია ხელშეკრულებაში გასათვალისწინებელი ძირითადი საკითხები, მათ შორის: ტერმინები; მონაცემთა

²⁷ GDPR, Third Countries, <gdpr-info.eu> [03.08.2024].

²⁸ Standard data protection clauses (SCCs).

²⁹ Binding corporate rules (BCRs).

³⁰ Ad hoc contractual clauses.

³¹ EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].

³² იქვე.

³³ CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.

³⁴ EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].

დამუშავების პრინციპები; მონაცემთა სუბიექტის უფლებები; მხარეთა ვალდებულებები; მონაცემთა გადაცემასთან დაკავშირებული შეზღუდვები და სხვა.³⁵

ევროპულმა კომისიამ გამოაქვეყნა მესამე ქვეყნებში პერსონალური მონაცემების გადაცემისას ხელშეკრულების სტანდარტული პირობების შესახებ დოკუმენტი,³⁶ რომელიც ეყრდნობა „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებს. მასში ხაზგასმულია, რომ თანამედროვე ტექნოლოგიების პირობებში, საერთაშორისო თანამშრომლობისა და ვაჭრობის ხელშესაწყობად, იზრდება მონაცემთა ტრანსსასაზღვრო გადაცემის საჭიროება, რა პროცესშიც, არსებითად მნიშვნელოვანია პერსონალურ მონაცემთა სათანადო დაცვა.³⁷

“GDPR”-ის 46-ე მუხლის პირველი პუნქტის შესაბამისად, შესაბამისობის გადაწყვეტილების არარსებობისას, პერსონალური მონაცემების გადაცემა დასაშვებია, თუ უზრუნველყოფილია მონაცემთა დაცვის სათანადო გარანტიები, მათ შორის, მონაცემთა სუბიექტის უფლებები და სამართლებრივი დაცვის საშუალებები. ამგვარი გარანტიები მიზანშეწონილია, ითვალისწინებდეს ევროპული კომისიის მიერ მიღებულ მონაცემთა დაცვის სტანდარტულ პირობებს, 46-ე მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის შესაბამისად.³⁸

ევროპული კომისიის მიერ შედგენილი მონაცემთა დაცვის სტანდარტული პირობების მიზანია მონაცემთა საერთაშორისო გადაცემისას სათანადო გარანტიების უზრუნველყოფა. ხელშეკრულების მხარეები არ არიან შეზღუდულნი, შეთანხმებაში ასახონ დამატებითი სტანდარტები პერსონალურ მონაცემთა დაცვის ხელშესაწყობად. აღნიშნულ დოკუმენტს თან ახლავს დანართი, რომელშიც წარმოდგენილია ხელშეკრულების სტანდარტული პირობები საერთაშორისო გადაცემის მიმართულებით.³⁹

დამატებით, მონაცემთა დაცვის ევროპულმა საბჭომ შეიმუშავა დოკუმენტი, რომელიც შეეხება მონაცემთა დაცვის სათანადო გარანტიებს ევროპის ეკონომიკური ზონისა და მესამე ქვეყნების მონაცემთა დაცვის საზედამხებდველო ორგანოებს შორის თანამშრომლობის განხორციელებისას. სახელმძღვანელოში ასახული სტანდარტები ეფუძნება “GDPR”-ის 70-ე (1)(u) და 50(a)-ე მუხლებს.⁴⁰

4.4. მონაცემთა საერთაშორისო გადაცემის შესახებ საზღვარგარეთის ქვეყნების მონაცემთა დაცვის საზედამხებდველო ორგანოთა პრაქტიკის მიმოხილვა

საზღვარგარეთის ქვეყნების მონაცემთა დაცვის საზედამხებდველო ორგანოებს არაერთ საქმეში უმსჯელიათ პერსონალურ მონაცემთა საერთაშორისო გადაცემის საკითხებზე. წინამდებარე თავის ფარგლებში საილუსტრაციოდ წარმოდგენილია

³⁵ EDPB, Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies, 15/12/2020, <edpb.europa.eu> [03.08.2024].

³⁶ European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, <eur-lex.europa.eu> [03.08.2024].

³⁷ იქვე.

³⁸ იქვე.

³⁹ იქვე.

⁴⁰ EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14/03/2022, <edpb.europa.eu> [03.08.2024].

რამდენიმე ქვეყნის პრაქტიკა, რომელიც მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებით არსებულ მიდგომებზე ზოგად წარმოდგენას ქმნის.

ა. შვედეთი

შვედეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("IMY") დამუშავებისთვის პასუხისმგებელი პირის მიერ "Google Analytics"-ის საშუალებით პერსონალური მონაცემების დამუშავების მართლზომიერებაზე იმსჯელა. საქმის ფაქტობრივი გარემოებების შესაბამისად, პლატფორმის საშუალებით, პერსონალური მონაცემები შეერთებულ შტატებში გადაიცემოდა.

საზედამხედველო ორგანომ შეაფასა მონაცემთა გადაცემის თავსებადობა "GDPR"-ის V თავით გათვალისწინებულ მოთხოვნებთან და, ამავდროულად, 44-ე მუხლთან. "Schrems II"-ის საქმეზე დაყრდნობით, აღინიშნა, რომ მხოლოდ ხელშეკრულების სტანდარტული პირობების არსებობა მონაცემთა სათანადო დაცვის უზრუნველყოფის თვალსაზრისით საკმარისი არ არის. მოცემულ შემთხვევაში, აუცილებელია ეროვნული საკანონმდებლო ჩარჩოს ანალიზი.

საზედამხედველო ორგანოს გადაწყვეტილებით, მონაცემთა გადაცემა არ იყო თავსებადი "GDPR"-ის V თავით დადგენილ მოთხოვნებთან. დამუშავებისთვის პასუხისმგებელმა პირმა ვერ უზრუნველყო მონაცემთა სუბიექტთა უფლებების დაცულობა, რის საფუძველზეც დაირღვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 44-ე მუხლი.⁴¹

ბ. ესპანეთი

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ შეისწავლა სატელეფონო კომპანია - "Vodafone"-ის მიერ პერსონალური მონაცემების დამუშავების კანონიერება, მათ შორის, მონაცემთა საერთაშორისო გადაცემის კონტექსტში.

ფაქტობრივი გარემოებების თანახმად, სატელეფონო კომპანიას ხელშეკრულება ჰქონდა გაფორმებული დამუშავებაზე უფლებამოსილ პირთან, რომელსაც, თავის მხრივ, მონაცემები უნდა დაემუშავებინა პერუში. შესაბამისად, პერსონალური მონაცემები გადაიცემოდა მესამე სახელმწიფოში. ხელშეკრულებით პერსონალურ მონაცემთა საერთაშორისო გადაცემის საკითხები არ რეგულირდებოდა. ამდენად, მონაცემთა დაცვის სათანადო გარანტიები არ იყო უზრუნველყოფილი.

წარმოდგენილი გარემოების გათვალისწინებით, საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირის მიერ "GDPR"-ის 44-ე მუხლის დარღვევა დაადგინა.⁴²

გ. ავსტრია

ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ერთ-ერთი კომპანიის მიერ "Facebook"-ის საშუალებით, შესაბამისი სამართლებრივი საფუძვლის არარსებობის პირობებში, პერსონალური მონაცემების შეერთებულ შტატებში გადაცემას უკავშირდება.

საზედამხედველო ორგანომ იმსჯელა პერსონალურ მონაცემთა საერთაშორისო გადაცემის კანონიერებასა და "GDPR"-ის V თავით დადგენილ მოთხოვნებთან შესაბამისობაზე. მსგავსად სხვა საზედამხედველო ორგანოებისა, აღნიშნულ

⁴¹ Decision of the Swedish DPA (IMY), 30/06/2023, <gdprhub.eu> [03.08.2024].

⁴² Decision of Spanish DPA, 10/03/2021, <gdprhub.eu> [03.08.2024].

შემთხვევაშიც მითითება გაკეთდა “CJEU”-ს გადაწყვეტილებაზე.⁴³ საქმის შესწავლის შედეგად დადგინდა, რომ არ არსებობდა პერსონალურ მონაცემთა გადაცემის სამართლებრივი საფუძველი. კერძოდ, “Schrems II”-ის საქმეზე ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებით ძალადაკარგულად გამოცხადდა ევროპული კომისიის მიერ მიღებული შესაბამისობის გადაწყვეტილება ევროკავშირიდან შეერთებულ შტატებში პერსონალური მონაცემების გადაცემების შესახებ. ამდენად, მონაცემთა მიმღები და გადამცემი ვერ დაეყრდნობოდა “GDPR”-ის 45-ე მუხლს.

საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია “GDPR”-ის V თავით გათვალისწინებული მოთხოვნები შეერთებულ შტატებში მონაცემთა სუბიექტის პერსონალური მონაცემების უკანონო გადაცემის გამო.⁴⁴

დ. იტალია

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ (“Garante”) ვებგვერდის ოპერატორის მიერ “Google Analytics”-ის გამოყენებით შეერთებულ შტატებში პერსონალურ მონაცემთა გადაცემის კანონიერებაზე იმსჯელა.

საზედამხედველო ორგანოს შეფასებით, შეერთებული შტატების ორგანოების მხრიდან პერსონალურ ინფორმაციაზე წვდომის მცირე ალბათობა არსებობდა, რაც ვერ იქნებოდა დამუშავებისთვის პასუხისმგებელი პირის პასუხისმგებლობისგან გათავისუფლების საფუძველი სათანადო გარანტიების უზრუნველყოფის თვალსაზრისით. საქმის ფაქტობრივი გარემოებების შესაბამისად, პერსონალური მონაცემების დაშიფვრა, წარმოადგენდა არასაკმარის ტექნიკური უსაფრთხოების ზომას.

აღნიშნულიდან გამომდინარე, დაირღვა “GDPR”-ის 44-ე და 46-ე მუხლები. დამუშავებისთვის პასუხისმგებელ პირს საზედამხედველო ორგანომ შენიშვნა გამოუცხადა და 90 დღის განმავლობაში 46-ე მუხლთან შესაბამისობის უზრუნველყოფა დაავალა. წინააღმდეგ შემთხვევაში, უნდა შეეწყვიტა პერსონალური მონაცემების გადაცემა.⁴⁵

ე. ფინეთი

პლატფორმა “Google Analytics”-ის გამოყენებით პერსონალური მონაცემების დამუშავების მართლზომიერება ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომაც შეაფასა. ფაქტობრივი გარემოებების თანახმად, დამუშავებისთვის პასუხისმგებელი პირის (მეტეოროლოგიური ინსტიტუტი) მიერ პერსონალური მონაცემები გადაიცემოდა შეერთებულ შტატებში. საზედამხედველო ორგანომ “Schrems II”-ის გადაწყვეტილებაზე დაყრდნობით იმსჯელა მონაცემთა გადაცემის კანონიერებაზე.

საზედამხედველო ორგანოს გადაწყვეტილებით, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ V თავის თანახმად, დამუშავებისთვის პასუხისმგებელი პირის მიერ პერსონალური მონაცემების გადაცემა არ ეფუძნებოდა შესაბამის სამართლებრივ საფუძველს. ამასთან, მონაცემთა დაცვის სათანადო გარანტიები არ იყო უზრუნველყოფილი. ამდენად, დამუშავებისთვის

⁴³ CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.

⁴⁴ Decision of Austrian DPA, 06/03/2023, <gdprhub.eu> [03.08.2024].

⁴⁵ Decision of Italian DPA, 9/06/2022, <gdprhub.eu> [03.08.2024].

პასუხისმგებელი პირი შეერთებულ შტატებს, “Google Analytics”-ის გამოყენებით, მონაცემთა სუბიექტების პერსონალურ მონაცემებს უკანონოდ გადასცემდა.

აღნიშნულის გათვალისწინებით, დაირღვა “GDPR”-ის 44-ე და 46-ე მუხლები. საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს შენიშვნა გამოუცხადა და შეერთებულ შტატებში სამართლებრივი საფუძვლის გარეშე გადაცემული პერსონალური მონაცემების წაშლა დაავალა.⁴⁶

5. დასკვნა

სახელმწიფოთა/საერთაშორისო ორგანიზაციათა შორის პერსონალური მონაცემების ინტენსიური მიმოცვლა საჭიროებს ეფექტიან რეგულირებას, რათა შესაბამისად იქნას დაცული მონაცემთა სუბიექტის უფლებები. სტატიამ განხილული საკითხები, მათ შორის, ევროკავშირის მართლმსაჯულების სასამართლოსა და საზედამხედველო ორგანოთა პრაქტიკა მიუთითებს პერსონალურ მონაცემთა საერთაშორისო გადაცემის აქტუალობაზე და წარმოაჩენს ამ მიმართულებით არსებულ გამოწვევებს.

როგორც გამოიკვეთა, თუ ევროკავშირის არაწევრ ქვეყანასთან მიმართებით არ არის მიღებული შესაბამისობის გადაწყვეტილება და, ამავდროულად, არ არის მონაცემთა დაცვის სათანადო გარანტიები უზრუნველყოფილი, პერსონალურ მონაცემთა გადაცემა არ გამოირიცხება, რამდენადაც შესაძლებელია საკითხის ხელშეკრულებით მოწესრიგება. მოცემულ შემთხვევაში, მიზანშეწონილია, ხელშეკრულებაში აისახოს: ძირითად ტერმინთა განმარტებები, მონაცემთა დამუშავების პრინციპები, მონაცემთა სუბიექტის უფლებები, მხარეთა ვალდებულებები და ა.შ.

პერსონალური მონაცემების გადაცემამდე, მნიშვნელოვანია კონკრეტულ სახელმწიფოში ეროვნული კანონმდებლობისა და მონაცემთა დაცვის სტანდარტების შეფასება. ამასთან, სათანადო გარანტიების არსებობის დადგენა. აღნიშნული მიზნით, გასათვალისწინებელია სტატიამ განხილული საერთაშორისო საკანონმდებლო ჩარჩო და სტანდარტები და, ასევე, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის V თავით დადგენილი მოთხოვნები.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის №23 ბრძანება „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“, 29/02/2024.
3. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის №33 ბრძანება „პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესის და პერსონალურ მონაცემთა სხვა სახელმწიფოს ან/და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე განაცხადის ფორმის დამტკიცების შესახებ“, 01/03/2024.
4. მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 287.

⁴⁶ Decision of Finnish DPA, 24/03/2023, <gdprhub.eu> [03.08.2024].

5. CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.
6. CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, European Treaty Series - No. 181, 2001.
7. CoE, Convention 108 +, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.
8. CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018.
9. EU, 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).
10. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and repealing Council Framework Decision 2008/977/JHA.
11. The EU General Data Protection Regulation (GDPR), a Practical Guide.
12. European Commission, Information Regarding the Adequacy Decisions.
13. GDPR, Information Regarding the Third Countries.
14. EDPB, Overview of International Data Transfers.
15. CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
16. EDPB, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, 15 December 2020.
17. European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
18. EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14 March 2022.
19. Case of the Data Protection Authority (Sweden), 30/06/2023.
20. Case of the Data Protection Authority (Spain), 10/03/2021.
21. Case of the Data Protection Authority (Austria), 06/03/2023.
22. Case of the Data Protection Authority (Italy), 09/06/2022.
23. Case of the Data Protection Authority (Finland), 24/03/2023.

დავით ქანთარია*

კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობა და პერსონალური მონაცემების დაცვა

კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობა პრობლემური საკითხია და მას არსებითი მნიშვნელობა აქვს კანონით განსაზღვრული ლეგიტიმური მიზნების მისაღწევად. სახელმწიფოს აკისრია მთელი რიგი ვალდებულებები, რომელთა საფუძველზე დგინდება არასრულწლოვანთა უფლებების დაცვის ადეკვატური გარანტიები.

განსაკუთრებით საინტერესოა არასრულწლოვანთა მართლმსაჯულების კოდექსისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნები აღნიშნულ საკითხთან დაკავშირებით. მათ შორის, კანონთან კონფლიქტში მყოფი არასრულწლოვნის სტიგმატიზებისგან დაცვა და მისი უმტკივნეულო რეინტეგრაცია საზოგადოებაში. იგი მოიცავს კომპლექსურ ღონისძიებებს, რომლებიც პრაქტიკაში უნდა რეალიზდეს.

საკვანძო სიტყვები: კანონთან კონფლიქტში მყოფი არასრულწლოვანი, ეტიკეტირება, პერსონალური მონაცემები, პირადი ცხოვრების ხელშეუხებლობა, რესოციალიზაცია, პროფესიული ეთიკა.

1. შესავალი

არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობა სისხლის სამართლის პროცესის ნებისმიერ ეტაპზე უნდა იყოს დაცული და გარანტირებული. არასრულწლოვანთა მართლმსაჯულებაში გაცხადებულია ერთ-ერთი მთავარი იდეა, რომ უნდა მოხდეს არასრულწლოვნის რესოციალიზაცია და მისი თავისუფალი ინტეგრაცია საზოგადოებაში. ამის მიღწევა კი მარტივი როდია. როცა საქმე ეხება არასრულწლოვანს, რომელიც სჩადის დანაშაულს, მათ შორის, მძიმე კატეგორიის დანაშაულს, საზოგადოების ნაწილი ვერ ხედავს, რომ რეალურად საქმე ეხება ბავშვს და მომეტებულ სიმკაცრეს იჩენს, რაც დემოკრატიულ საზოგადოებაში

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის აპარატის სამართლებრივი საკითხების სპეციალისტი.

მიზანშეწონილი არაა. ასევე, მეტად მნიშვნელოვანია დანაშაულის მსხვერპლი არასრულწლოვნის დაცვა მეორეული ვიქტიმიზაციისაგან.

არასრულწლოვანთა მართლმსაჯულება, ამ მხრივ, მეტად საინტერესო რამაა. მისი პრაქტიკაში რეალიზება სიფრთხილეს მოითხოვს, რადგან ძალიან რთულია განსაზღვრო, რა იქნება პროპორციული ღონისძიება არასრულწლოვანთან მიმართებით.

კანონთან კონფლიქტში მყოფი არასრულწლოვნის საქმის განხილვა მთელი რიგი თავისებურებებით გამოირჩევა და ერთგვარ კოლიზიაშია საქმის საჯაროდ განხილვის უფლებასთან, ასევე, გამოხატვისა და ინფორმაციის მიღების უფლებებთან.

პირადი ცხოვრების უფლება საკმაოდ ფართო კონცეფციაა და მისი ასპექტების *Numerus Clausus* პრინციპით ამოწურვა შეუძლებელია. წინამდებარე ნაშრომი მიზნად ისახავს, წარმოაჩინოს არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობის პრობლემური სამართლებრივი საკითხები არასრულწლოვანთა მართლმსაჯულებაში და შეაფასოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დადებითი ეფექტი.

2. კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობის დაცვა

საქართველოს კონსტიტუცია ადიარებს და უზრუნველყოფს ადამიანის უფლებებს. აღნიშნულ უფლებებს შორის მნიშვნელოვანი ადგილი უჭირავს პირადი ცხოვრების უფლებას. პირადი ცხოვრება არ არის მხოლოდ ადამიანის შინაგანი სამყარო, არამედ იგი ასევე მოიცავს პირის შესაძლებლობას, ჰქონდეს გარე სამყაროსთან ურთიერთობა. პირადი ცხოვრების ხელშეუხებლობა არის ძალიან მნიშვნელოვანი ქვეყნისთვის, საზოგადოების ჯანსაღი განვითარებისა და არსებობისთვის¹. შესაბამისად, მისი გამოყენება ანგარებით ან პოლიტიკური მიზნებისთვის ყოვლად დაუშვებელია. პირადი ცხოვრების ხელშეუხებლობის დაცვის უფლება ის ფასეულობაა, რომელიც ყოველდღიურ ცხოვრებაში აისახება და იგი ერთ-ერთი უმნიშვნელოვანესი უფლებაა დემოკრატიულ საზოგადოებაში. ტექნოლოგიური განვითარების პირობებში, როდესაც პროგრესს სისტემატურად განიცდის ჩვენი გარე სამყარო, აღნიშნული უფლება ახალ შინაარსს იძენს.

საქართველოს კონსტიტუციის მე-15 მუხლი იცავს ადამიანის პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებას, რომელიც, თავისი არსით, ბუნებრივია, სცდება კონსტიტუციის ერთი კონკრეტული მუხლის ფარგლებს. სწორედ, აღნიშნულიდან გამომდინარე, მიიჩნევა ადამიანის უფლებათა ევროპული სასამართლო და საქართველოს საკონსტიტუციო სასამართლო, რომ პირადი ცხოვრების უფლების ფუნდამენტური მნიშვნელობა მის მრავლისმომცველობასთანაა დაკავშირებული იგი მოიცავს, ფიზიკური და მორალური ხელშეუხებლობის, პირადი მონაცემების, ოჯახური და სქესობრივი ცხოვრების საიდუმლოების, სახელის, მიმოწერისა და სატელეფონო საუბრების საიდუმლოს ხელშეუხებლობის უფლებას, და ასევე, რასობრივ ან ეთნიკურ

¹ ივანიძე მ., არასრულწლოვანი და მისი საუკეთესო ინტერესები, არასრულწლოვანთა კანონმდებლობის ანალიზი და სასამართლო პრაქტიკა, თბ., 2017, 545.

კუთვნილებასთან, ნასამართლობასა და განრიდებასთან, ბიომეტრიულ თუ გენეტიკურ ინფორმაციასთან დაკავშირებულ საკითხებს, თუმცა, მისი ყველა ასპექტის წინსწრებად ჩამოთვლა შეუძლებელია.²

პირადი ცხოვრების უფლების დაცვა განსაკუთრებით მნიშვნელოვანია არასრულწლოვნებთან მიმართებით. ბავშვებთან ურთიერთობა განსაკუთრებულ მიდგომას საჭიროებს ნებისმიერ სივრცეში, მით უმეტეს მართლმსაჯულების კუთხით და მისი საკანონმდებლო მოწესრიგებაც სწორედ აღნიშნული ფაქტორების სრულფასოვანი გააზრებით უნდა განხორციელდეს. არასრულწლოვნის უფლების დაცვის სფეროში ბოლო წლებში დიდი ტრანსფორმაცია განიცადა. ადრე თუ არასრულწლოვანი არ განიხილებოდა დამოუკიდებელი უფლებების მატარებლად, გასული საუკუნის 20-იან წლებში მიღებულმა „ჟენევის დეკლარაციამ“ ვითარება არსებითად შეცვალა. შემდგომ წლებში კი აღნიშნული სფერო კიდევ უფრო მეტად დაიხვეწა. შესაბამისად, საინტერესოა, რა გზა განვლო და როგორ უზრუნველყოფს კანონმდებლობა არასრულწლოვნის პირადი ცხოვრების დაცვას ამ ეტაპზე.

ბავშვის უფლებები, მათ შორის პირადი ცხოვრების უფლება, მარტივად შეიძლება დაირღვეს. ამიტომ საზოგადოებას აკისრია უდიდესი პასუხისმგებლობა – დაიცვას ბავშვთა ინტერესები და ხელი შეუწყოს მათი უფლებების დაცვას.

პირველი ნაბიჯი, რომელიც გადაიდგა ბავშვის უფლებების დასაცავად იყო ჟენევის დეკლარაცია, რომლითაც შესაძლებელი გახდა ბავშვთა უფლებების აღიარება და რომელიც ორიენტირებული იყო რამდენიმე მნიშვნელოვან ასპექტზე. კერძოდ, ბავშვის განვითარების, მისი შემწეობისა და დაცვის, ასევე ბავშვის კეთილდღეობასთან დაკავშირებულ საკითხებთან³. აღნიშნული დეკლარაცია გახდა საფუძველი 1959 წელს გაერთიანებული ერების ორგანიზაციის მიერ ბავშვთა დეკლარაციის მიღებისა, რომლითაც განისაზღვრა „ბავშვის საუკეთესო ინტერესების“ სტანდარტი. 1985 წელს კი მიიღეს ე.წ. „პეკინის წესები“, რომელიც არასრულწლოვანთა სისხლის სამართლის ადმინისტრირების შესახებ მნიშვნელოვან საკითხებს მოიცავდა. მისი დახმარებით შესაძლებელი გახდა არასრულწლოვანთა სტიგმატიზაციის თავიდან აცილება, ვინაიდან აიკრძალა მასობრივი ინფორმაციის საშუალებებითა და საჯარო დაწესებულებების მიერ არასრულწლოვანთა მაიდენტიფიცირებელი ინფორმაციის გამჟღავნება. 1989 წელს მიიღეს „ბავშვის უფლებათა კონვენცია“, რომლის რატიფიცირებაც მსოფლიოს 195 ქვეყანაში განხორციელდა. გაერომ ბავშვის უფლებათა კონვენციის არაერთი დამხმარე ინსტრუმენტი მიიღო, რომლის მიზანიც უფრო მოსახერხებელი სტანდარტის შექმნა და აღნიშნულ სისტემაში მონაწილე პროფესიონალებისათვის სახელმძღვანელო პრინციპების მიწოდება იყო.⁴

ასევე მნიშვნელოვანია „ჰავანას წესები“, რომელიც 1990 წელს იქნა მიღებული. აღნიშნული დოკუმენტი ითვალისწინებს არასრულწლოვანთა მართლმსაჯულების არსებით პერსპექტივებს, კერძოდ, სისტემა უნდა მოიცავდეს არასრულწლოვანთა ფიზიკური და გონებრივი მდგომარეობის წამახალისებელ უფლებებსა და გარანტიებს. კანონის დარღვევაში ბრალდებულ და მსჯავრდებულ

² გოგნიაშვილი ნ., პირადი ცხოვრების დაცვის მნიშვნელობა და მისი სპეციფიკა არასრულწლოვანთან მიმართებაში, ქართულ გერმანული სამართლის ჟურნალი, 2023, 3.

³ იმერლიშვილი ი., არასრულწლოვნის უფლებები: საერთაშორისო გამოცდილება და საქართველოში არსებული მდგომარეობა, კრებულში: ადამიანის უფლებათა დაცვა, კონსტიტუციური რეფორმა და სამართლის უზენაესობა საქართველოში, თბ., 2017.

⁴ გოგნიაშვილი ნ., პირადი ცხოვრების დაცვის მნიშვნელობა და მისი სპეციფიკა არასრულწლოვანთან მიმართებაში, ქართულ გერმანული სამართლის ჟურნალი, 2023, 3.

არასრულწლოვნებთან მოპყრობა უნდა განსხვავდებოდეს იმავე მდგომარეობაში მყოფ ზრდასულებთან მოპყრობისგან, ამ ყველაფერს აქვს შემდეგი საფუძვლები: – მიიჩნევა, რომ ბავშვი ნაკლებად აგებს პასუხს თავის ქმედებებზე, მისი პასუხისმგებლობა იზრდება ასაკის მატებასთან ერთად – ზრდასრულებთან შედარებით ბავშვები, რომლებიც დანაშაულს სჩადიან უფრო ადვილად ექვემდებარებიან გამოსწორებას და სწავლობენ ქცევის სხვაგვარ წესებს – ბავშვები და ახალგაზრდები, რომლებიც მოთავსებულნი არიან წინასწარი პატიმრობის საკნებსა და ციხეებში, დაუცველნი არიან ძალადობისა და არასათანადო მოპყრობისაგან და ნაკლებად შეუძლიათ თავის დაცვა. ასევე, გაეროს სახელმძღვანელო პრინციპები არასრულწლოვანთა მიერ ჩადენილ დანაშაულთან დაკავშირებით – „რიალის სახელმძღვანელო პრინციპები“, რომელიც დანაშაულის პრევენციის კუთხით ერთ-ერთი ყველაზე მნიშვნელოვანი დოკუმენტი იყო, სადაც ძირითადი აქცენტი, კანონიერ, სოციალურად სასარგებლო საქმიანობაში ჩაბმასა და საზოგადოების მიმართ ჰუმანური დამოკიდებულების შექმნაზე იყო გაკეთებული.⁵

საერთაშორისო სტანდარტების მიხედვით, ბავშვებს, ზრდასრული ადამიანებისგან განსხვავებით, აქვთ პირადი ცხოვრების სრული პატივისცემის უფლება საქმის განხილვის ყველა სტადიაზე. ბავშვის უფლებათა კომიტეტმა მე-10 ზოგად კომენტარში დაადგინა, რომ „საქმის განხილვის ყველა სტადია“ იწყება სამართალდამცავ ორგანოებთან პირველი კონტაქტიდან (მაგ. ინფორმაციისა და იდენტიფიცირების მოთხოვნა) ზედამხედველობიდან ან პატიმრობიდან განთავისუფლებამდე.⁶

პირადი ცხოვრების პატივისცემის უფლების მიზანია იმ ზიანის თავიდან აცილება, რომელიც შეიძლება მიაღგეს ბავშვს საქმის გაუმართლებელი საჯაროობით. უარყოფითმა გასაჯაროებამ შეიძლება მოახდინოს ბავშვის სტიგმატიზაცია და უარყოფითად აისახება ბავშვის შესაძლებლობაზე, მიიღოს განათლება, მოიძიოს სამუშაო და საცხოვრებელი ადგილი, ასევე ზოგადად მის რეინტეგრაციაზე⁷. ბავშვის უფლებათა კომიტეტმა კანონთან კონფლიქტში მყოფი ბავშვების პირადი ცხოვრების ხელშეუხებლობის უფლების ფართო გაგებით განმარტა. სახელმწიფოებმა მკაფიოდ უნდა განსაზღვრონ კანონმდებლობაში, რომ როდესაც მიმდინარეობს ბავშვის გასამართლება დანაშაულის ჩადენის გამო, განხილვა უნდა გაიმართოს დახურულ კარს მიღმა⁸.

გასაჯაროების აკრძალვის პრინციპი და მიზანი ნათლად არის მოცემული უგანდის ბავშვთა აქტის (1996) 102-ე მუხლში - „პირადი ცხოვრების პატივისცემის უფლების დაცვა და გამოქვეყნების შეზღუდვა“. ბავშვის პირადი ცხოვრების პატივისცემის უფლება დაცული უნდა იყოს სასამართლო პროცესის მანძილზე, რათა თავიდან ავიცილოთ მისთვის ზედმეტი საჯაროობით ზიანის მიყენება და ოჯახური და საბავშვო სასამართლოს წინაშე წარმდგარ ბავშვთან დაკავშირებით არავინ უნდა გამოაქვეყნოს რაიმე ინფორმაცია, რომელსაც შეუძლია გამოიწვიოს ბავშვის

⁵ ერემაძე ქ., ძირითადი უფლებები თავისუფლებისთვის, წიგნი მეორე, ილიას სახელმწიფო უნივერსიტეტის გამომცემლობა, 2021, 201.

⁶ ბავშვის უფლებათა კომიტეტი, ზოგადი კომენტარი N10 (2007); პუნქტი 64.

⁷ პეკინის წესების მე-8 წესი. იხ., აგრეთვე, ბავშვის უფლებათა კომიტეტის ზოგადი კომენტარი N10 (2007); პუნქტი 64.

⁸ ჰამილტონი ქ., არასრულწლოვანთა მართლმსაჯულების საკანონმდებლო რეფორმის სახელმძღვანელო მითითებები, 2011, 88.

იდენტიფიცირება. გარდა ამისა, ნებისმიერ პირს, რომელიც არღვევს ამ უფლების დაცვისა და შეზღუდვის წესს, შეიძლება დაეკისროს ჯარიმა და დაისაჯოს.⁹

ეროვნულ კანონმდებლობაში კანონთან კონფლიქტში მყოფი არასრულწლოვნის მონაცემთა დაცვის საკანონმდებლო ბაზა ჯერ კიდევ შექმნისა და დახვეწის პროცესშია. საქართველოს არასრულწლოვანთა მართლმსაჯულების კოდექსის მე-13 მუხლის მე-2 ნაწილი, რომელიც ბლანკეტური ხასიათისაა და გვამისამართებს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონზე, ამასთან, კანონთან კონფლიქტში მყოფი არასრულწლოვნის პერსონალური მონაცემების დამუშავების საკითხები დამატებით გაბნეულია არაერთ კანონქვემდებარე ნორმატიულ აქტში, კერძოდ, თითოეული საჯარო დაწესებულება დაწყებული საგამოძიებო ორგანოებიდან დამთავრებული სასჯელაღსრულებითი დაწესებულებით განსაზღვრავენ კონკრეტულ შემთხვევებში რა მონაცემები მუშავდება, რა ვადით ინახება, განადგურების წესი და ა. შ. მოცემული რეგულაციები არ წარმოადგენს არასრულწლოვნის პერსონალური მონაცემებისა და პირადი ცხოვრების უფლების დაცვის სათანადო გარანტს, ვინაიდან ხშირად არასრულწლოვანია ამ საკითხის მომწესრიგებელი კანონქვემდებარე ნორმატიული აქტები¹⁰.

საერთაშორისო სტანდარტების თანახმად, მნიშვნელოვანია კანონმდებლობაში ასახული იყოს „სპეციალური მოთხოვნები“, რათა ბავშვის საჭიროებები სათანადოდ იქნეს დაკმაყოფილებული. ასეთ „სპეციალურ მოთხოვნად“ მოიაზრება არასრულწლოვნის პირადი ცხოვრების უფლების პატივისცემა საქმის განხილვის ყველა სტადიაზე; კანონმდებლობა მკაცრად უნდა კრძალავდეს სხდომაზე დამსწრე პირთა მიერ კანონთან კონფლიქტში მყოფი არასრულწლოვნის ვინაობის გამჟღავნებას. ამ თვალსაზრისით, აუცილებელია სათანადო მყარი სამართლებრივი გარანტია არსებობდეს არასრულწლოვნის პირადი ცხოვრების უფლების დასაცავად; კვლევამ ცხადყო, რომ უშუალოდ ბავშვის უფლებების მარეგულირებელი ეროვნული საკანონმდებლო ჩარჩო, არ შეიცავს მკაფიო ჩანაწერს, რომელიც აუკრძალავს მედიის წარმომადგენლებს არასრულწლოვანთა მართლმსაჯულების სისტემაში მოხვედრილ ბავშვთა ვინაობის გამჟღავნებას. „ბავშვის უფლებათა კოდექსი შეიცავს სპეციალურ მუხლს, რომელიც არეგულირებს მედიის მიერ არასრულწლოვნის პერსონალური მონაცემების დაცვის საკითხს. თუმცა ამ ნორმის მოქმედება არ ვრცელდება სისხლის სამართლის დანაშაულისა და ადმინისტრაციული სამართალდარღვევის საქმეთა წარმოებაზე და კოდექსი მიუთითებს, რომ ეს საკითხი წესრიგდება არასრულწლოვანთა მართლმსაჯულების კოდექსით¹¹. თუმცა, ამკ არ შეიცავს რაიმე სპეციალურ დებულებებს მედიის მიერ არასრულწლოვნის პერსონალური მონაცემების დაცვის საკითხთან დაკავშირებით; აღნიშნული პრობლემის გადაჭრის მიზნით, მიზანშეწონილია, პირველ რიგში, ჟურნალისტების მიერ პროფესიული ეთიკის დარღვევის ფაქტებზე რეაგირების მექანიზმი თვითრეგულირების ფარგლებში გაძლიერდეს, რათა დარღვევის ფაქტებზე დისციპლინური პასუხისმგებლობის

⁹ იხ. უგანდის ბავშვთა აქტი, 1996, ნაწ. 102.

¹⁰ *ქვერივიშვილი თ.*, კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის გარანტიები არასრულწლოვანთა მართლმსაჯულებაში, სადისერტაციო ნაშრომი (თსუ), 2022, 47.

¹¹ *შეკილაძე ხ.*, კანონთან კონფლიქტში მყოფი არასრულწლოვნის საუკეთესო ინტერესების პრიორიტეტულობა არასრულწლოვანთა მართლმსაჯულების (სისხლის სამართლის საქმის წარმოების) პროცესში, თბ., 2019

დონეზე მოხდეს ქმედითი რეაგირება. ამასთან, ვინაიდან ბავშვის უფლებათა დაცვის სფეროში მოქმედი ინსტრუმენტები უფრო მკაცრი ზომების მიღებას მოითხოვენ იმ ჟურნალისტებთან მიმართებით, რომლებიც უხეშად არღვევენ არასრულწლოვნის პირადი ცხოვრების უფლებას, საჭიროა შესაბამისი საკანონმდებლო ბაზის არსებობა. აღსანიშნავია, რომ ხორვატიამ არასრულწლოვანთა პირადი ცხოვრების უფლების დაცვის მიზნით სპეციალური მუხლიც კი შემოიღო სისხლის სამართლის კოდექსში, რომელიც ითვალისწინებს სისხლის სამართლის წესით იმ პირთა დასჯადობას, რომლებიც ხელყოფენ ბავშვის პირადი ცხოვრების უფლებას მისი ფოტოების ან სხვა მაიდენტიფიცირებელი გარემოებების გამჟღავნებით, თუ ამან გამოიწვია ბავშვის მღელვარება, თანატოლებისგან ან სხვა პირებისგან დაცინვა ან სხვა მხრივ საფრთხე შეექმნა ბავშვის კეთილდღეობას. ამასთან, იგივე ქმედების ჩადენა საჯარო მოხელის ან მედიის წარმომადგენლის მიერ, წარმოადგენს დამამძიმებელ გარემოებას.

3. არასრულწლოვნის დაცვა ეტიკეტირებისგან

ეტიკეტირების ფენომენი საკმაოდ გავრცელებულია. მის ნიმუშს წარმოადგენს რობერტ როზენტალის გამოკვლევა. მისი ვარაუდით, ღარიბი და ფერადკანიანი მოსწავლეები სკოლაში კარგად ვერ სწავლობენ იმიტომ, რომ მასწავლებლები მათგან წარმატებას არ ელიან და შესაბამისად, მათ როგორც უნიჭოებს ეპყრობიან. ეს კი ბადაებს სწორედ იმ ქცევას, რომლის მოლოდინიც ჰქონდათ მასწავლებლებს¹².

ეტიკეტირების თეორია ამტკიცებს, რომ დევიაციური ქცევის სუბიექტად ანუ დევიანტად უნდა ჩაითვალოს ის, ვისაც საზოგადოება ასეთად მიიჩნევს. ამ თვალთახედვით, დევიაცია განისაზღვრება არა სპეციფიკური აქტებით, არამედ ადამიანზე რეაქციებით. ეტიკეტირების თეორიის თანახმად, დამნაშავედ გახდომის შემდეგი ეტაპები არსებობს: 1) პირველად ჩადენილი დანაშაული; 2) საზოგადოებაში დამნაშავის ინტეგრირების პრობლემა; 3) დამნაშავის მიერ მისი სტატუსის აღიარება; 4) კრიმინალის ჩამოყალიბება; 5) განმეორებითი დანაშაულის ჩადენა.

ეტიკეტირების თეორიის თანახმად, დევიანტური ქცევა შეიძლება სხვადასხვა მიზეზებიდან და პირობებიდან გამომდინარეობდეს, მაგრამ მას შემდეგ რაც პირს დევიანტის „იარლიყს მიაკრავენ“, ისინი ხშირად აწყდებიან ახალ პრობლემებს, რომლებიც გამომდინარეობს საკუთარი თავისა და სხვების რეაქციიდან უარყოფით სტერეოტიპებზე.¹³ ეტიკეტირების თეორია ძირითადად შეისწავლის ადამიანის დევიანტად ეტიკეტირების შედეგებს: 1. ადამიანის დევიანტად ეტიკეტირებით იზრდება იმის ალბათობა, რომ ეს ადამიანი შემდგომშიც გააგრძელებს დევიაციურ ქცევას. ჯერ ერთი, ადამიანის ეტიკეტირება დევიანტად ზრდის ბარიერს მასსა და დანარჩენ საზოგადოებას შორის; მეორე, დევიანტის ეტიკეტი უკვე „კვალიფიკაციაა“, რომელიც ამ ინდივიდის შეფასებაში გადამწყვეტ როლს ასრულებს. საზოგადოებისთვის ეს ადამიანი ხდება დევიანტი საერთოდ, და არა კონკრეტულ საკითხში ან სფეროში. მისგან ყველაფერში დევიაციას მოელოან და შესაბამისად ეპყრობიან. მაგ: ადამიანს, რომელსაც ერთხელ დაერქვა „ქურდი“, აღარ ენდობიან.

¹² Rosenthal, L. Jacobson, Pygmalion im Unterricht. Lehrererwartungen und Intelligenzentwicklung der Schüler. Beltz 1983. S.129

¹³ ჟერივიშვილი თ., კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის გარანტიები არასრულწლოვანთა მართლმსაჯულებაში, სადისერტაციო ნაშრომი (თსუ), 2022, 56.

სასჯელის მოხდის შემდეგ მას მეგობრები არა მხოლოდ იმიტომ გაურბიან, რომ არ უნდათ სახელგატეხილ ადამიანთან მეგობრობა, არამედ იმიტომაც, რომ „ქურდმა“ მათაც შეიძლება რაიმე მოჰპაროს. 2. ეტიკეტირებული პირის მიმართ ამგვარი მიდგომა ამცირებს მის შანსებს ჩვეულებრივად იცხოვროს და იგი ცხოვრების დევიაციურ სტილს ანუ დევიაციურ კარიერას ირჩევს. ეტიკეტირებული პირები მხოლოდ მათსავით უარყოფითად ეტიკეტირებულ ადამიანებს სცნობენ თავისიანად, მჭიდრო კავშირებს აყალიბებენ და ერთმანეთს სოლიდარობას უცხადებენ.¹⁴

ეტიკეტირების თეორიის თანახმად, მეორეულ დევიაციას იწვევს, აგრეთვე ე. წ. „თვითქმნადი წინასწარმეტყველება“ ანუ განსაკუთრებული ფენომენი, როდესაც ნავარაუდევია მოვლენა წარმოშობს საკუთარ თავს ანუ თვითრეალიზდება. ამ შემთხვევაში, თუ რას ფიქრობენ ადამიანები კონკრეტული ინდივიდის სამომავლო დევიაციური ქცევის შესახებ სწორედ ამგვარ ქცევას წარმოშობს.

ეტიკეტირების თეორიის მიმოხილვის საფუძველზე, შეიძლება ითქვას, რომ არასრულწლოვნის დამნაშავედ სტიგმატიზება არსებითად ზემოქმედებს მის მომავალ ცხოვრებაზე.¹⁵ თუ არასრულწლოვნის ნასამართლობის შესახებ ინფორმაცია კონფიდენციალური არ დარჩება, ამგვარ პირობებში პატიმრობაც კი ვერ მოახდენს ისეთ მძიმე ზეგავლენას არასრულწლოვანზე, როგორც არაფორმალური ეტიკეტირება. ამან, შესაძლოა, გამოიწვიოს მისი უარყოფა თანატოლების მხრიდან და არასრულწლოვნის დაახლოება დევიანტური თვითკონცეფციის მქონე პირებთან, რაც ზრდის არასრულწლოვნის მიერ განმეორებითი დანაშაულის ჩადენის რისკებს. სწორედ ამიტომ, არასრულწლოვანთა მართლმსაჯულების პროცესში პირადი ცხოვრების უფლების დაცვას საქმის განხილვის ყველა სტადიაზე, რაც მას იცავს ვინაობის გამჟღავნებისა და სტიგმატიზებისგან, არსებითი მნიშვნელობა აქვს.

4. არასრულწლოვანთა საქმეების გაშუქება

გამოხატვის თავისუფლების უფლება ნებისმიერი პირისათვის გარანტირებული უფლებაა. იგი მოიცავს შეხედულების ქონის უფლებას, ინფორმაციის და იდეების მიღების და გავრცელების უფლებას საჯარო უწყებების ჩარევის გარეშე, თუმცა, სახელმწიფოებს გააჩნიათ უფლება, დააწესონ ლიცენზირების მოთხოვნა მაუწყებლების, ტელევიზიებისა ან კინო საწარმოებისათვის.¹⁶

ეს უფლება არის დემოკრატიული საზოგადოების არსებითი ელემენტი და ძირითადი პირობა მისი პროგრესისათვის და თითოეული პირის თვითრეალიზაციისათვის. გამოხატვის თავისუფლების საზღვრები უფრო ვრცელია, ვიდრე ინფორმაცია და იდეები, რომლებსაც დადებითად აღიქვამენ ან მიიჩნევენ არაშეურაცხმყოფელად ან ნეიტრალურად, და მოიცავს ინფორმაციას, რომელიც შეიძლება იყოს შეურაცხმყოფელი, შოკისმომგვრელი ან აღმამფოთებელი.

მედიის წარმომადგენლები მიიჩნევიან საზოგადოებრივ მოდარაჯებად, რომლებიც უმნიშვნელოვანეს როლს ასრულებენ დემოკრატიულ საზოგადოებაში. მათ აქვთ ვალდებულება, გაავრცელონ ინფორმაცია და საზოგადოებას გააცნონ

¹⁴ ახალაშვილი ნ., იურიდიული ფსიქოლოგია, თბ., 2009, 244.

¹⁵ შალიკაშვილი მ., მიქანაძე გ., არასრულწლოვანთა მართლმსაჯულება (სახელმძღვანელო), მეორე გამოცემა, თბილისი, ფრაიბურგი, სტრასბურგი, 2016, 48.

¹⁶ დანელია ნ., ბავშვთა საკითხების გაშუქება ქართულ სატელევიზიო სივრცეში, მედიის განვითარების ფონდი, თბ., 2011, 38.

ყველა საინტერესო საკითხი, რომლის მიღების უფლებაც საზოგადოებას გააჩნია.¹⁷ ჟურნალისტის გამოხატვის თავისუფლება არ არის აბსოლუტური. ჟურნალისტებს გააჩნიათ უფლებები და პასუხისმგებლობები. ამ თვალსაზრისით, ტერმინი „უფლებები“ განიმარტება, როგორც ჟურნალისტის პრეროგატივა, განახორციელოს საკუთარი პროფესიული მოვალეობები და გააშუქოს საზოგადოებისათვის საინტერესო საკითხები, ხოლო „პასუხისმგებლობები“ ნიშნავს, რომ ჟურნალისტმა უნდა იმოქმედოს კეთილსინდისიერად და მიაწოდოს ზუსტი და სანდო ინფორმაცია, ჟურნალისტური ეთიკის შესაბამისად.¹⁸

ჟურნალისტი ვალდებულია, გამოქვეყნებამდე გადაამოწმოს ფაქტები. თუმცა, იგივე მოთხოვნა არ ვრცელდება ჟურნალისტების მიერ მოსაზრების გაშუქებისას ან თვალსაზრისის შესახებ ინფორმაციის გავრცელებისას.¹⁹ ამის მიუხედავად, მოსაზრებებიც უნდა ემყარებოდეს რაიმე ფაქტობრივ საფუძველს. მედიის როლი და მისი გავლენა არასრულწლოვანთა მართლმსაჯულებაზე სამ ასპექტში ვლინდება: 1) მედიის გავლენა ბავშვებზე, მედიის გავლენა არასრულწლოვანთა კანონმდებლობის ფორმირებაზე და მედიის გავლენა არასრულწლოვანთა მართლმსაჯულების პროცესზე.²⁰

ხაზგასმით უნდა აღინიშნოს, რომ სასამართლო პროცესების გაშუქებისას როგორც სასამართლო პერსონალს მოეთხოვება სამართლებრივ სფეროში კომპეტენტურობა და პასუხისმგებლობა, ასევე მოეთხოვება მასობრივი ინფორმაციის საშუალებების წარმომადგენლებსაც, რაც ამავდროულად საკუთარი პროფესიის პატივისცემას ემსახურება მიზნად.²¹ მით უმეტეს რომ დღევანდელ რეალობაში მომეტებული ყურადღების ცენტრში ის დანაშაულები გვხვდება, რომლებშიც არასრულწლოვნები ფიგურირებენ.²²

ეს არის კონკურენცია ორ უფლებას შორის: გამოხატვის თავისუფლებასა და არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობას შორის. გამოხატვის თავისუფლება არ წარმოადგენს აბსოლუტურ უფლებას. საქართველოს საკონსტიტუციო სასამართლო განმარტავს, რომ გამოხატვის თავისუფლების შეზღუდვა დასაშვებია თანაზომიერების პრინციპის შესაბამისად, მხოლოდ კანონით მოწესრიგების ფორმალური მოთხოვნის დაცვითა და მკაფიოდ და ამომწურავად განსაზღვრული ლეგიტიმური მიზნების უზრუნველსაყოფად.²³

მედიის მიერ კანონთან კონფლიქტში მყოფი არასრულწლოვნის შესახებ ინფორმაციის გაშუქების სტანდარტს არაერთი საერთაშორისო თუ ევროპული

¹⁷ *ხიდეშელი ს.*, ბავშვთა უფლებების დაცვა მედიაში – დემოკრატიული სახელმწიფოს ფორმირების მნიშვნელოვანი ასპექტი, კრებულში: ადამიანის უფლებათა დაცვა და სახელმწიფოს დემოკრატიული ტრანსფორმაცია, *კორკელია კ. (რედ.)*, თბ., 2020, 37.

¹⁸ *გოცირიძე ე.*, გამოხატვის თავისუფლება კონფლიქტურ ღირებულებათა სამართლიანი დაბალანსების კონტექსტში, თბ., 2007, 27.

¹⁹ *გომაძე კ.*, პერსონალურ მონაცემთა დაცვის ძირითადი უფლება, 2020, 102.

²⁰ *ჯორბენაძე ს., ბახტაძე უ., მაჭარაძე ზ.*, მედიასამართალი, *ჯორბენაძე ს. (რედ.)*, თბ., 2014, 59.

²¹ *ალვარტი ჰ.*, საჯაროობის პრინციპი გერმანული სისხლის სამართლის პროცესის მიხედვით, კრებულში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, *თუმანიშვილი გ., ჯიშკარიანი ბ., შრამი ე. (რედ.)*, თბ., 2019, 437- 438.

²² *ხერხეულიძე ი.*, არასრულწლოვანთა დანაშაული და მისი გამომწვევი მიზეზები იუვენალური იუსტიციის სისტემებში, „სამართლის ჟურნალი“, №2, 2013.

²³ საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 17 დეკემბრის №2/6/1311 გადაწყვეტილება საქმეზე „მპს სტერეო+“, ლუკა სევერინი, ლაშა ზილფიმიანი, რობერტ ხახალავი და დავით ზილფიმიანი საქართველოს პარლამენტისა და საქართველოს იუსტიციის მინისტრის წინააღმდეგ.

ინსტრუმენტი აღგენს. „პეკინის წესები“ დაუშვებლად მიიჩნევა კანონთან კონფლიქტში მყოფი არასრულწლოვნის შესახებ ინფორმაციის გამოქვეყნებას მასობრივი ინფორმაციის საშუალებების მიერ. „ბავშვზე მორგებული მართლმსაჯულების შესახებ“ გაიდლაინებში კი დეტალურადაა გაწერილია ის შესაძლო საშუალებები, რითაც უზრუნველყოფილი იქნება მედიის მიერ საზოგადოების ინფორმირებისას არასრულწლოვნის პირადი ცხოვრების დაცულობა. ამ თვალსაზრისით აუცილებელ ღონისძიებებს წარმოადგენს, *inter alia*, არასრულწლოვნისთვის ანონიმურობის ან ფსევდონიმის მინიჭება, დაფარვა ან შეცვლილი ხმების გამოყენება, სახელებისა და სხვა ელემენტების წაშლა, რამაც შეიძლება გამოიწვიოს ბავშვის იდენტიფიკაცია ნებისმიერი დოკუმენტიდან, ნებისმიერი ფორმით (ფოტო, აუდიო, ვიდეო) ჩაწერის აკრძალვა და ა. შ. ამასთან, გაიდლაინები ითვალისწინებს აღნიშნული წესიდან გამონაკლისს, როდესაც განსაკუთრებულ შემთხვევებში, პრესაში არასრულწლოვნის მაიდენტიფიცირებელი ინფორმაციის გავრცელება ბავშვის ინტერესთან იყოს თავსებადი და საქმის შესახებ გარკვეული მონაცემების გამჟღავნებითა და გასაჯაროებით, არასრულწლოვნისთვის სასარგებლო შედეგის მომტანი აღმოჩნდეს.

2019 წელს საქართველოს პარლამენტის მიერ მიღებული „ბავშვის უფლებათა კოდექსი“, რომელიც ქმნის ბავშვის ძირითადი უფლებების დაცვისა და მხარდაჭერის სისტემის ფუნქციონირების სამართლებრივ საფუძვლებს, ითვალისწინებს სპეციალურ მუხლს, რომელიც არეგულირებს მედიის მიერ არასრულწლოვნის პერსონალური მონაცემების დაცვის საკითხს. 71-ე მუხლის პირველი ნაწილის თანახმად, მედიას ეკრძალება ადმინისტრაციულ წარმოებაში ან სასამართლო პროცესში მონაწილე ბავშვის პერსონალური მონაცემების გასაჯაროება, როგორც პირდაპირი ისე ირიბი იდენტიფიცირება. ხოლო ამავე მუხლის მე-2 ნაწილი კრძალავს, მათ შორის, ბავშვის მიერ ჩადენილი ძალადობის შემთხვევის დამადასტურებელი დოკუმენტის ან ჩანაწერის გასაჯაროებას. კანონმდებელი იქვე აკეთებს დათქმას, რომ ეს დებულებები არ ვრცელდება სისხლის სამართლის დანაშაულისა და ადმინისტრაციული სამართალდარღვევის საქმეთა წარმოებაზე, რაც წესრიგდება არასრულწლოვანთა მართლმსაჯულების კოდექსით.²⁴

მართლმსაჯულების სისტემაში მოხვედრილ ბავშვთა პირადი ცხოვრების უფლების დასაცავად მედიის მიერ დანაშაულის საკითხის გაშუქების კონტექსტში. მიზანშეწონილია, „ბავშვის უფლებათა კოდექსის“ 71-ე მუხლის მოქმედება გავრცელდეს სისხლის სამართლის დანაშაულზეც.²⁵ ალტერნატივის სახით, შესაძლოა, არასრულწლოვანთა მართლმსაჯულების კოდექსის მე-13 მუხლს დაემატოს მე-3 ნაწილი მსგავსი შინაარსის ფორმულირებით, რომელიც აუკრძალავს მედიის წარმომადგენლებს არასრულწლოვანთა მართლმსაჯულების პროცესში მონაწილე ბავშვის ისეთი პერსონალური მონაცემების გასაჯაროებას, რომლებითაც შეიძლება მოხდეს მისი როგორც პირდაპირი ისე ირიბი იდენტიფიცირება.²⁶

არასრულწლოვანთა საუკეთესო ინტერესების გამო რომ შესაძლებელია შეიზღუდოს გამოხატვის თავისუფლება, ეს ადამიანის უფლებათა ევროპულმა

²⁴ საქართველოს კანონი „ბავშვის უფლებათა კოდექსი“, საქართველოს პარლამენტი, 20/09/2019, მე-2 მუხლის პირველი პუნქტი.

²⁵ *მეყილაძე ხ.*, კანონთან კონფლიქტში მყოფი არასრულწლოვნის საუკეთესო ინტერესების პრიორიტეტულობა არასრულწლოვანთა მართლმსაჯულების (სისხლის სამართლის საქმის წარმოების) პროცესში, თბ., 2019, 39.

²⁶ *ქარივიშვილი თ.*, კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების დაცვის გარანტიები, სადისერტაციო ნაშრომი (თსუ), 2022, 194.

სასამართლომ არაერთ საქმეში დაადასტურა. ერთ-ერთი ასეთი საქმე იყო ჰენდისაიდი გაერთიანებული სამეფოს წინააღმდეგ. ფაქტობრივი გარემოებების თანახმად, ლონდონის ერთ-ერთმა გამომცემლობამ გამოსცა წიგნი სახელწოდებით „პატარა წითელი სახელმძღვანელო“, რომელიც განკუთვნილი იყო 12-დან 18 წლამდე სასკოლო ბავშვებისთვის. წიგნის შინაარსი დაკავშირებული იყო სქესობრივი ცხოვრების საკითხებთან. ვინაიდან, დიდი ბრიტანეთის სასამართლომ წიგნის გამოცემა აკრძალა, განმცხადებელმა ეს კონვენციის მე-10 მუხლის დარღვევად მიიჩნია. ევროპულმა სასამართლომ შემოფოთება გამოხატა იმ ფაქტთან დაკავშირებით, რომ წიგნი განკუთვნილი იყო მოზარდებისთვის, რომელსაც შესაძლოა ნეგატიური ზემოქმედება მოეხდინა შთაბეჭდილებების ზეგავლენის ქვეშ ადვილად მოქცევად ფსიქიკაზე და კანონსაწინააღმდეგო ქმედებისკენაც კი ებიძგებინა ახალგაზრდებისათვის. სასამართლომ მიიჩნია, რომ სახელმწიფო ორგანოების ქმედება ნაკარნახევი და შეზღუდული იყო „მკაცრი საჭიროების/აუცილებლობის“ ჩარჩოთი.²⁷

პასუხისმგებლიანი ჟურნალისტიკა ნიშნავს, რომ ჟურნალისტები იქცევიან პროფესიონალურად და მოქმედებენ კეთილსინდისიერად და ავრცელებენ ინფორმაციას ჟურნალისტური ეთიკის შესაბამისად. ჟურნალისტები უზრუნველყოფენ დაბალანსებულ გაშუქებას, რისთვისაც უკავშირდებიან დაინტერესებულ პირებს კომენტარის მისაღებად, მასალის გამოქვეყნებამდე.

სამართლებრივი შეფასებისას მნიშვნელოვანი ელემენტია, პირად ინფორმაციას აქვეყნებს ჟურნალისტი, რომელიც იცავს პასუხისმგებლიანი ჟურნალისტიკის პრინციპებს, თუ ტაბლოიდური გამოცემები, რომლებიც ინფორმაციას აქვეყნებენ მხოლოდ საზოგადოების ცნობისმოყვარეობის დასაკმაყოფილებლად. პასუხისმგებლიანი ჟურნალისტები სარგებლობენ გამოხატვის თავისუფლების დაცვის უფრო მაღალი დონით. თუმცა, ეროვნული ხელისუფლების გადასაწყვეტი არ არის, გაშუქების რა მეთოდებს გამოიყენებს ჟურნალისტი.

როცა საქმე ეხება ბავშვებს, ჟურნალისტებმა უნდა გამოიყენონ მაქსიმალურად მაღალი სტანდარტები. საქართველოში ეს სტანდარტები ნელ-ნელა და ეტაპობრივად დაინერგა. ეს სტანდარტები არ გვქონდა სახეზე, როდესაც წლების წინ შუქდებოდა არასრულწლოვანთა საქმეები. ჟურნალისტებს თავიანთი პროფესიიდან გამომდინარე, შეუძლიათ ადამიანებისგან, განსაკუთრებით კი არასრულწლოვნებისგან, „მტრის ხატი“ შექმნან. ეს ძალიან საფრთხილო საქმეა. ეს ეტიკეტირების ძალიან მაღალ საფრთხეს ქმნის. თუკი ვამბობთ, რომ არასრულწლოვანთა მართლმსაჯულებაში ძირითადი იდეა არასრულწლოვნის რესოციალიზაციაა, ეს ერთ-ერთი ხელშემშლელი ფაქტორია. დღეს სხვადასხვა ინტერნეტ-პლატფორმაზე იძებნება ის სიუჟეტები, რომლებიც მართლაც ქმნის „მტრის ხატს“ არასრულწლოვნისაგან. ამგვარი სიუჟეტები არ უნდა იყოს ხელმისაწვდომი ფართო საზოგადოებისათვის, რადგანაც ისინი ნამდვილად ლახავს არასრულწლოვნის კანონიერ ინტერესებს.

დღეს ჟურნალისტები ქართულ სინამდვილეში შედარებით მაღალი პროფესიონალიზმით გამოირჩევიან არასრულწლოვანთა საქმეების გაშუქების

²⁷ Handyside v United Kingdom [1976] ECHR 5 at para. 48, (1976) 1 EHRR 737, [1976] ECHR 5493/72 (7 December 1976), European Court of Human Rights.

პროცესში, მაგრამ უფრო მეტია გასაკეთებელი, რათა ბავშვები შემდგომი სტიგმატიზაციისგან მაქსიმალურად იყვნენ დაცულნი.

5. კანონთან კონფლიქტში მყოფი არასრულწლოვნის პერსონალური მონაცემების დაცვა, როგორც მისი პირადი ცხოვრების უფლების გარანტია

XXI საუკუნის ერთ-ერთ მთავარ გამოწვევას პერსონალურ მონაცემთა დაცვა წარმოადგენს²⁸. მათი დაცვა დაკავშირებულია ადამიანის ავტონომიურობასთან, იგი ადამიანის უფლებებისა და თავისუფლებების დაცვის ჭრილში განიხილება, კერძოდ, პირადი ცხოვრების ხელშეუხებლობის შემადგენელ კომპონენტად.

საქართველოს კონსტიტუცია არ იცნობს ტერმინს „პერსონალური მონაცემი“, თუმცა საკონსტიტუციო სასამართლოს დადგენილი პრაქტიკის თანახმად, იგი კერძო ცხოვრების ხელშეუხებლობის კონსტიტუციური უფლების ერთ-ერთი შემადგენელი ელემენტია და დაცულია საქართველოს კონსტიტუციის მე-15 მუხლით. ხოლო ფიზიკური პირის პერსონალური მონაცემის გამჟღავნებისგან დაცვის ინტერესზე სასამართლო მსჯელობს კონსტიტუციის მე-18 მუხლის მე-3 პუნქტით გარანტირებული ინფორმაციული თვითგამორკვევის უფლების ფარგლებში.²⁹

ბავშვის უფლებათა სამართალში, პერსონალურ მონაცემთა დაცვის უფლება წარმოადგენს ბავშვის უფლებათა კონვენციის მე-16 მუხლით დაცულ ბავშვის პირადი ცხოვრების უფლების შემადგენელ უფლებრივ ნაწილს, რომლის პატივისცემის ვალდებულება ყველა პირს აკისრია, დაწყებული პროცესის მწარმოებელი ორგანოდან დამთავრებული მისი კანონიერი წარმომადგენლით. კონვენცია საქმისწარმოების ყველა ეტაპზე ავალდებულებს შესაბამის ორგანოს უზრუნველყოს კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების დაცვა. შესაბამისად, უზრუნველყოფილი უნდა იყოს მისი პერსონალური მონაცემების სათანადოდ დაცვა გამჟღავნებისაგან.

ტექნოლოგიური პროგრესის პირობებში არასრულწლოვანთა პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვა კიდევ უფრო მეტი გამოწვევაა, ვინაიდან ახალ შესაძლებლობებთან ერთად იზრდება ამ უფლებაში უკანონო ჩარევის საფრთხეები. ამიტომ ბავშვთა მონაცემების დამუშავების პროცესში განსაკუთრებული როლი აკისრიათ იმ საჯარო და კერძო დაწესებულებებს, რომლებიც ბავშვების მონაცემებს აგროვებენ, იყენებენ, ინახავენ, ასაჯაროვებენ. ისინი ვალდებული არიან, იხელმძღვანელონ ბავშვის საუკეთესო ინტერესებით ამასთან, მონაცემების დამუშავებელმა ორგანომ უნდა უზრუნველყოს პერსონალური მონაცემების დაცვა მესამე მხარის ან საზოგადოებისაგან, რათა არასრულწლოვნის პირადი ცხოვრების უფლება არ შეილახოს. განსაკუთრებულ რისკებს შეიცავს პერსონალური მონაცემების გამჟღავნება ინტერნეტ სივრცეში, რამაც არასრულწლოვნის კიბერბულინგის საფრთხე შეიძლება შექმნას.³⁰

²⁸ გოშაძე კ., პერსონალურ მონაცემთა დაცვის ძირითადი უფლება, 2020, 6.

²⁹ კოპალეიშვილი მ., კონსტიტუციით დადგენილი ბალანსი სასამართლო აქტებზე საჯარო ხელმისაწვდომობის უფლებასა და პერსონალური მონაცემების ხელმისაწვდომობისგან დაცვის უფლებას შორის, კვლევა და რეკომენდაციები საკონსტიტუციო სასამართლოს გადაწყვეტილების შესაბამისად საკანონმდებლო მოწესრიგების საჭიროებაზე, 2020, 17.

³⁰ ფაჩულია თ., არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები, კრებული: პერსონალურ მონაცემთა დაცვის აქტუალური პრობლემები და გამოწვევები, თოლორაია ლ., ფირცხალაშვილი ა. (რედ.), 2021, 45.

არასრულწლოვნის პერსონალური მონაცემების დაცვის გარანტიები უზრუნველყოფილია კომპლექსური მექანიზმის არსებობით, როგორებიცაა საერთაშორისო ნორმატიული ბაზა უშუალოდ პერსონალურ მონაცემთა დაცვის სფეროში, აგრეთვე ბავშვის უფლებათა სფეროში მოქმედი საერთაშორისო და ეროვნული აქტები, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ და დარგობრივ კანონთა კომპლექსი. ამასთან, ევროპული საკონსულტაციო და საზედამხებლო ორგანოები და მათ შორის, მონაცემთა დაცვის ეროვნული ორგანო - პერსონალურ მონაცემთა დაცვის სამსახური, უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლს.

კანონთან კონფლიქტში მყოფი არასრულწლოვნის პერსონალური მონაცემების დაცვა წარმოადგენს პირადი ცხოვრების უფლებრივ ნაწილს. როგორც ეროვნული ისე საერთაშორისო ინსტრუმენტების თანახმად, როდესაც მუშავდება კანონთან კონფლიქტში მყოფი არასრულწლოვნის მონაცემები, იგი პერსონალურ მონაცემთა დაცვის უფლებით მოსარგებლე სუბიექტად გვევლინება. ვინაიდან, არასრულწლოვნის მოწყვლადობის გამო, მისი პერსონალური მონაცემების გამჟღავნებას განსაკუთრებით ნეგატიური გავლენა შეიძლება ჰქონდეს მის მომავალ ცხოვრებაზე, ამ თვალსაზრისით მონაცემების დაცვის უფრო მაღალი ინტერესი არსებობს, სრულწლოვანთა მონაცემებთან შედარებით.

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, არასრულწლოვნის ნასამართლობა წარმოადგენს განსაკუთრებული კატეგორიის მონაცემს, რომელიც გამიჯნულია ჩვეულებრივი პერსონალური მონაცემის დაცვის რეჟიმისგან და ვინაიდან იგი განსაკუთრებით მგრძნობიარე მონაცემთა კატეგორიას განეკუთვნება, დაცვის უფრო მაღალი გარანტიებით სარგებლობს. შესაბამისად, ამ მონაცემის კონფიდენციალურობის დაცვას საქმისწარმოების ყველა ეტაპზე უნდა მიექცეს ყურადღება, რათა არასრულწლოვნის ინტერესებს ზიანი არ მიაღგეს³¹. როგორც წესი, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აკრძალულია, თუმცა კანონით განსაზღვრულ შემთხვევებში შეიძლება დამუშავდეს კანონთან კონფლიქტში მყოფი არასრულწლოვნის ამ კატეგორიის მონაცემებიც. კერძოდ, სისხლის სამართლის პროცესში მისი პირადი საქმეებისა და რეესტრების წარმოებისას, მსჯავრდებული არასრულწლოვნის მიმართ მის მიერ სასჯელის მოხდის ინდივიდუალური დაგეგმვის ან/და სასჯელის მოხდისგან პირობით ვადამდე გათავისუფლებასთან და მისთვის სასჯელის მოუხდელი ნაწილის უფრო მსუბუქი სახის სასჯელით შეცვლასთან დაკავშირებული საკითხების განხილვისას; აგრეთვე იმ შემთხვევაში, თუ მონაცემები მუშავდება „დანაშაულის პრევენციის, არასაპატიმრო სასჯელთა აღსრულების წესისა და პრობაციის შესახებ“ საქართველოს კანონის მე-2 მუხლით გათვალისწინებული სამართლებრივი აქტების აღსრულების მიზნით; არასრულწლოვან მსჯავრდებულთა და ყოფილ პატიმართა რესოციალიზაციისა და რეაბილიტაციის, დანაშაულის პრევენციის ღონისძიებების განხორციელებისა და არასრულწლოვანთა რეფერირების პროცესის კოორდინაციის მიზნით.

„ბავშვზე მორგებული მართლმსაჯულების შესახებ“ გაიდლაინები, განსაკუთრებულ ყურადღებას ამახვილებს არასრულწლოვნის პერსონალური მონაცემების დაცვის საკითხზე და წევრ სახელმწიფოებს მოუწოდებს, რომ

³¹ *კოპლენიშვილი მ.*, კონსტიტუციით დადგენილი ბალანსი სასამართლო აქტებზე საჯარო ხელმისაწვდომობის უფლებასა და პერსონალური მონაცემების ხელმისაწვდომობისგან დაცვის უფლებას შორის, კვლევა და რეკომენდაციები საკონსტიტუციო სასამართლოს გადაწყვეტილების შესაბამისად საკანონმდებლო მოწესრიგების საჭიროებაზე, 2020, 17.

არასრულწლოვნის მაიდენტიფიცირებელი არანაირი ინფორმაცია არ გახდეს საჯარო და არ გამოქვეყნდეს. არასრულწლოვნის ჩანაწერებზე წვდომა უნდა იყოს მკაცრად შეზღუდული, ხოლო ასეთი ინფორმაციის მიწოდების აუცილებლობის შემთხვევაში, სახელმწიფოებმა უნდა უზრუნველყონ მონაცემთა დაცვის შესახებ შესაბამისი კანონმდებლობის მიღება. პრაქტიკაში არასრულწლოვნების საქმეების გამოთხოვა შეუძლებელია, თუმცა სამეცნიერო მიზნებისთვის უნდა იყოს აღნიშნული გადაწყვეტილებები ხელმისაწვდომი. რასაკვირველია, ამ შემთხვევაში დაინტერესებულ პირს გადაწყვეტილებები უნდა მიეწოდოს სრულად დეპერსონალიზებული სახით. სამეცნიერო-კვლევითი მიზნებისთვის აღნიშნული ქმედება სავსებით გამართლებული იქნება.

საკონსტიტუციო სასამართლოს მიერ მიღებულმა გადაწყვეტილებამ შესაბამის საკანონმდებლო მოწესრიგებამდე, განაპირობა საერთო სასამართლოების მიერ არასრულწლოვნის მიმართ გამოტანილი განაჩენების ხელმისაწვდომობის საკითხზე არაერთგვაროვანი პრაქტიკის დანერგვა.³² ნაწილი სასამართლოებისა განაჩენებს გასცემს დეპერსონალიზებული სახით, ნაწილი მოითხოვს მონაცემთა სუბიექტის თანხმობას, ხოლო ნაწილი საერთოდ უარს ამბობს მის გაცემაზე. საჯარო ინფორმაციის სახით არასრულწლოვნის მიმართ გამოტანილი განაჩენების გამოთხოვის შესახებ განცხადებაზე თბილისის საქალაქო სასამართლომ უარი განაცხადა იმ არგუმენტაციით, რომ „ვინაიდან არასრულწლოვან პირთა ინტერესების დაცვის მიზნით, მათ მიმართ წარმოებული სისხლის სამართლის საქმეები განიხილება დახურულ სასამართლო სხდომაზე, ... არ ხორციელდება აღნიშნულ საქმეებზე გამოტანილი სასამართლო გადაწყვეტილებების დამუშავება და შესაბამისად, არ ხდება მათი საჯარო მონაცემთა ბაზაში განთავსება.“³³

ბავშვის უფლებათა დაცვის სფეროში მოქმედი საერთაშორისო და რეგიონული აქტები არასრულწლოვნის პერსონალური მონაცემების დაცვასთან მიმართებით განსაკუთრებულ ყურადღებას რამდენიმე ასპექტზე ამახვილებენ, რომელთა შორისაა, მონაცემთა შენახვის ვადა და გარკვეული დროის გასვლის შემდეგ მისი განადგურების აუცილებლობა. რაც შეეხება ეროვნულ კანონმდებლობას, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი შეიცავს ზოგად ჩანაწერს, რომლის თანახმად, მონაცემთა დამუშავებისას გასათვალისწინებელ ერთ-ერთ მთავარ პრინციპს წარმოადგენს მონაცემთა შენახვის ვადა. კერძოდ, „მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით, გარდა იმ შემთხვევისა, თუ მონაცემთა დამუშავება განსაზღვრულია კანონით ან/და კანონის შესაბამისად გამოცემული კანონქვემდებარე ნორმატიული აქტით და მონაცემთა შენახვა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში აღმატებული ინტერესების დასაცავად“³⁴.

³² საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის №1/4/693,857 გადაწყვეტილება საქმეზე „ა(ა)იპ მედიის განვითარების ფონდი“ და ა(ა)იპ ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ.

³³ *ქარიშიძე თ.*, კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების დაცვის გარანტიები, თბ., 2022, 159.

³⁴ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტი.

არასრულწლოვნის თითის ანაბეჭდებისა და დნმ-ის მონაცემების განუსაზღვრელი ვადით შენახვასთან დაკავშირებით ევროპული კონვენციის მე-8 მუხლის დარღვევა დაადგინა ევროპულმა სასამართლომ საქმეში ს. და მარპერი გაერთიანებული სამეფოს წინააღმდეგ.³⁵ აღნიშნულ საქმეში ერთ-ერთი განმცხადებელი იყო 11 წლის არასრულწლოვანი, რომელიც სისხლის სამართლის დანაშაულის ჩადენაში იქნა ბრალდებული. მიუხედავად იმისა, რომ იგი გამართლდა, მისგან აღებული თითის ანაბეჭდსა და დნმ-ის ნიმუშს, ინგლისსა და უელსში არსებული საკანონმდებლო რეგულაციის შესაბამისად, პოლიცია ინახავდა განუსაზღვრელი ვადით. აღნიშნულ საქმეში ევროპულმა სასამართლომ განმარტა, რომ ევროპის საბჭოს ინსტრუმენტები პერსონალურ მონაცემთა დაცვის სფეროში მოითხოვს მონაცემთა შენახვას მისი მოპოვების მიზნის პროპორციულად და ამასთან, შეზღუდული დროით, რაც განსაკუთრებით პოლიციის სექტორს მიემართება. ვინაიდან, ინგლისისა და უელსის კანონმდებლობა განუსაზღვრელი ვადით იძლეოდა აღნიშნული მონაცემების შენახვის შესაძლებლობას, სასამართლომ ეს წესი განმცხადებლის პირადი ცხოვრების პატივისცემის უფლებაში არაპროპორციულ ჩარევად მიიჩნია. ამასთან, სასამართლომ განსაკუთრებული შემოთქმა გამოხატა იმ შესაძლო მავნე შედეგების გამო, რაც შეიძლებოდა მომხდარიყო არასრულწლოვნის შემთხვევაში. ეს უკავშირდებოდა მისი განვითარებისა და საზოგადოებაში ინტეგრაციის მნიშვნელობას. ამასთან, სასამართლომ ხაზი გაუსვა გაეროს 1989 წლის ბავშვის უფლებების კონვენციის მე-40 მუხლის დებულებებს, სისხლის სამართლის სფეროში არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის მნიშვნელობას. ანალოგიურად, სასამართლომ მიიჩნია, რომ განსაკუთრებული ყურადღება უნდა დაეთმოს არასრულწლოვანთა დაცვას ნებისმიერი ზიანისგან, რაც შეიძლება გამოიწვიოს ხელისუფლების მიერ მათი პირადი მონაცემების შენახვამ სისხლის სამართლის დანაშაულში გამართლების შემდეგ.³⁶

უმნიშვნელოვანესია, რომ მესამე პირებს, რომელთაც მოსამართლე არასრულწლოვნის სასამართლო სხდომაზე დასწრების ნებართვას მისცემს, ჰქონდეთ ვალდებულება არ გაამჟღავნონ არასრულწლოვნის შესახებ ინფორმაცია. ამ მხრივ, აუცილებელია სათანადო მყარი სამართლებრივი გარანტია არსებობდეს არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის მიზნით. აღნიშნული საკითხის მომწესრიგებელი არაერთი ნორმა არსებობს საქართველოს სისხლის სამართლის საპროცესო კოდექსში. სსსკ-ის 104-ე მუხლი მართლმსაჯულებისა და მხარეთა ინტერესებიდან გამომდინარე, სასამართლოს ანიჭებს უფლებას მხარის შუამდგომლობით ან საკუთარი ინიციატივით მიიღოს გადაწყვეტილება საქმის მონაწილეთა ან/და სასამართლო სხდომის დარბაზში მყოფ პირთა მიმართ განსახილველი საქმის გარკვეული მონაცემების საჯაროდ გავრცელებისაგან დაცვის შესახებ. ხოლო სსსკ-ის 182-ე მუხლის მე-7 ნაწილი ასევე ითვალისწინებს სასამართლოს შესაძლებლობას დაავალდებულოს დახურულ სხდომაზე დამსწრე პირი, არ გაახმაუროს ის ინფორმაცია, რომელიც მისთვის ამ სხდომაზე გახდა ცნობილი. ამრიგად, ორივე მუხლი ითვალისწინებს მოსამართლის უფლებას და არა ვალდებულებას გააფრთხილოს დამსწრე პირები კონფიდენციალურობის დაცვის შესახებ. ვფიქრობთ, მიზანშეწონილია თუ ამკ-ის 29-ე მუხლს დაემატება ნორმა,

³⁵ *S. and Marper v. The United Kingdom*, [2008] ECHR, nos. 30562/04 and 30566/04, §124.

³⁶ იქვე.

რომელიც გაითვალისწინებს მოსამართლის ვალდებულებას, გააფრთხილოს კანონთან კონფლიქტში მყოფი არასრულწლოვნის სასამართლო სხდომაზე დამსწრე პირები, არ გაამჟღავნონ არასრულწლოვნის შესახებ ინფორმაცია, რომლის დაუცველობაც, დადგენილი პრაქტიკის მიხედვით სისხლის სამართლებრივ პასუხისმგებლობას გამოიწვევს საქართველოს სისხლის სამართლის კოდექსის 381-ე მუხლის მიხედვით.

მეტად მნიშვნელოვანია იმ სახელმძღვანელო პრინციპების დაცვა, რომელიც პერსონალურ მონაცემთა დაცვის სამართლითაა განმტკიცებული. ეს პრინციპები განამტკიცებს იმ ზოგადსახელმძღვანელო იდეას, რომლითაც სამართლის ეს დარგი ხელმძღვანელობს და ამ პრინციპების დარღვევას სამართალდარღვევებამდე მივყავართ.

6. დასკვნა

კვლევამ წარმოაჩინა, რომ მეტად პრობლემურია არასრულწლოვნის დაცვა ეტიკეტირებისაგან და მედიის მხრიდან ხშირად ირღვევა მათი უფლებები. რეკომენდირებულია, საქართველოს იუსტიციის უმაღლესმა საბჭომ უზრუნველყოს არასრულწლოვანთა სასამართლო სხდომის დარბაზების სათანადო პირობების შესაბამისად ინფრასტრუქტურული მოწესრიგება. სასურველია გამოიყოს სპეციალური სივრცე იმ პირთათვის, რომელთაც მიეცემათ სხდომაზე წვდომა. აქვე დამატებით აღსანიშნავია, საერთო სასამართლოებში სხდომის დარბაზებში არსებული შემინული კარის პრობლემური საკითხი, რაც დამატებით საფრთხეს ქმნის კანონთან კონფლიქტში მყოფი არასრულწლოვნის იდენტიფიცირების თვალსაზრისით.

ასევე ყურადსაღებია ის ინფორმაციაც, რომ მიმდინარეობს აქტიური მუშაობა იმის თაობაზე, რომ არასრულწლოვნებთან დაკავშირებულ საქმეებს სპეციალიზირებული ჟურნალისტები გააშუქებენ.

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონით არასრულწლოვნის პირადი ცხოვრების დაცულობა გარანტირებულია უფრო მაღალი სტანდარტით, ვინაიდან კანონი ითვალისწინებს მონაცემთა დამმუშავებელი ორგანოს ვალდებულებას არასრულწლოვნის ინტერესების შესაბამისად განახორციელოს მონაცემთა დამუშავება. მსგავსი რეგულირების პირობებში ნათლად არის ჩამოყალიბებული კანონმდებლის ნება, შექმნას კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის სათანადო სამართლებრივი გარანტიები.

წინამდებარე ნაშრომი მიზნად ისახავდა არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის გარანტიების კვლევას არასრულწლოვანთა მართლმსაჯულებაში. ნაშრომში შეფასდა ქართული კანონმდებლობის შესაბამისობა საერთაშორისო და ევროპულ სტანდარტებთან, გაანალიზდა კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების უფლების დაცვის გარანტიების პრობლემური საკითხები, რომელიც საბოლოოდ შეიძლება შეჯამდეს და ჩამოყალიბდეს შემდეგი ძირითადი დასკვნითი წინადადებებისა და რეკომენდაციების სახით: ბავშვის უფლებათა სამართალში მოქმედ ყველა საერთაშორისო თუ რეგიონულ ინსტრუმენტში აისახა არასრულწლოვნის პირადი ცხოვრების უფლება, რომლის დაცვაც უზრუნველყოფილი უნდა იყოს მართლმსაჯულების პროცესის ნებისმიერ სტადიაზე. ბავშვის უფლებათა კონვენცია, აღნიშნულ უფლებას სამართლიანი სასამართლოს გარანტიის ერთ-ერთ

ფუნდამენტურ უფლებრივ კომპონენტად განიხილავს, რომელიც მაღალი სტანდარტით უნდა იქნეს დაცული წევრი სახელმწიფოების მიერ, რათა გამოირიცხოს კანონთან კონფლიქტში მყოფი არასრულწლოვნის ვინაობის გამჟღავნებით მისი სტიგმატიზაცია; არასრულწლოვანი, როგორც უფლებების მფლობელი სუბიექტი სარგებლობს სრულწლოვანთათვის მინიჭებული ყველა უფლებით, თუმცა ბიო-ფსიქოლოგიური მახასიათებლების, ასაკის, მოწიფულობისა და სხვა გარემოებათა გათვალისწინების შესაბამისად, გარკვეული თავისებურებებით ხასიათდებიან ეს უფლებები არასრულწლოვანთა მართლმსაჯულებაში.

წინამდებარე ნაშრომში შევეცადეთ მეტ-ნაკლები სისავსით გადმოგვეტანა ის გარემოებები, რომლებიც აისახა ქართულ კანონმდებლობაში. უნდა აღინიშნოს ის, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მომეტებულად იცავს უკვე არასრულწლოვანთა პერსონალურ მონაცემებს და ცდილობს, რომ ამ მოწყვლადი ჯგუფის კანონიერი ინტერესები არ იყოს დარღვეული. ასევე საკანონმდებლო მიდწევად უნდა ჩაითვალოს ის ჩანაწერიც, რომ პერსონალურ მონაცემთა დაცვის შესახებ ახალ კანონში არასრულწლოვნის წინააღმდეგ განხორციელებული სამართალდარღვევა დამამძიმებელ გარემოებად ჩაიწერა და ეს მისასალმებელია.

ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, 1995.
2. არასრულწლოვანთა მართლმსაჯულების კოდექსი, 2015.
3. ბავშვთა უფლებათა კოდექსი, 2019.
4. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 2013.
5. გაეროს მინიმალური სტანდარტული წესები არასრულწლოვანთა მიმართ მართლმსაჯულების განხორციელების შესახებ (ე. წ. „პეკინის წესები“).
6. გაერთიანებული ერების ორგანიზაციის წესები თავისუფლებადკვეთილ არასრულწლოვანთა დასაცავად (ჰავანას წესები), 1990.
7. ალვარტი ჰ., საჯაროობის პრინციპი გერმანული სისხლის სამართლის პროცესის მიხედვით, კრებულში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, *თუბანიშვილი გ., ჯიმქარიანი ბ., შრამი ე. (რედ.)*, თბ., 2019.
8. *ახალაშვილი ნ.*, იურიდიული ფსიქოლოგია, თბ., 2009.
9. *გოგნიაშვილი ნ.*, პირადი ცხოვრების დაცვის მნიშვნელობა და მისი სპეციფიკა არასრულწლოვანთა მიმართებაში, ქართულ გერმანული სამართლის ჟურნალი, 2023.
10. *გომადე კ.*, პერსონალურ მონაცემთა დაცვის ძირითადი უფლება, 2020.
11. *გოცირიძე ე.*, გამოსატვის თავისუფლება კონფლიქტურ ღირებულებათა სამართლიანი დაბალანსების კონტექსტში, თბ., 2007.
12. *დანელია ნ.*, ბავშვთა საკითხების გაშუქება ქართულ სატელევიზიო სივრცეში, მედიის განვითარების ფონდი, თბ., 2011.
13. *ერემაძე ქ.*, ძირითადი უფლებები თავისუფლებისთვის, წიგნი მეორე, 2021.
14. *ივანიძე მ.*, არასრულწლოვანი და მისი საუკეთესო ინტერესები, არასრულწლოვანთა კანონმდებლობის ანალიზი და სასამართლო პრაქტიკა, თბ., 2017.

15. იმერლიშვილი ი., არასრულწლოვნის უფლებები: საერთაშორისო გამოცდილება და საქართველოში არსებული მდგომარეობა, კრებულში: ადამიანის უფლებათა დაცვა, კონსტიტუციური რეფორმა და სამართლის უზენაესობა საქართველოში, თბ., 2017.
16. კოპალეიშვილი მ., კონსტიტუციით დადგენილი ბალანსი სასამართლო აქტებზე საჯარო ხელმისაწვდომობის უფლებასა და პერსონალური მონაცემების ხელმისაწვდომობისგან დაცვის უფლებას შორის, კვლევა და რეკომენდაციები საკონსტიტუციო სასამართლოს გადაწყვეტილების შესაბამისად საკანონმდებლო მოწესრიგების საჭიროებაზე, 2020.
17. ფაჩულია თ., არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები, კრებულში: პერსონალურ მონაცემთა დაცვის აქტუალური პრობლემები და გამოწვევები, თოლორაია ლ., ფირცხალაშვილი ა. (რედ.), 2021.
18. ქვრივიშვილი თ., კანონთან კონფლიქტში მყოფი არასრულწლოვნის პირადი ცხოვრების დაცვის გარანტიები, თბ., 2022.
19. შალიკაშვილი მ., მიქანაძე გ., არასრულწლოვანთა მართლმსაჯულება (სახელმძღვანელო), მეორე გამოცემა, თბილისი, ფრაიბურგი, სტრასბურგი, 2016.
20. შეყილაძე ხ., კანონთან კონფლიქტში მყოფი არასრულწლოვნის საუკეთესო ინტერესების პრიორიტეტულობა არასრულწლოვანთა მართლმსაჯულების (სისხლის სამართლის საქმის წარმოების) პროცესში, თბ., 2019.
21. ხერხეულიძე ი., არასრულწლოვანთა დანაშაული და მისი გამომწვევი მიზეზები იუვენალური იუსტიციის სისტემებში, „სამართლის ჟურნალი“, №2, 2013.
22. ხიდუშელი ს., ბავშვთა უფლებების დაცვა მედიაში – დემოკრატიული სახელმწიფოს ფორმირების მნიშვნელოვანი ასპექტი, კრებულში: ადამიანის უფლებათა დაცვა და სახელმწიფოს დემოკრატიული ტრანსფორმაცია, კორკელია კ. (რედ.), თბ., 2020.
23. ჯორბენაძე ს., ბახტაძე უ., მაჭარაძე ზ., მედიასამართალი, ჯორბენაძე ს. (რედ.), თბ., 2014.
24. ჰამილტონი ქ. არასრულწლოვანთა მართლმსაჯულების საკანონმდებლო რეფორმის სახელმძღვანელო მითითებები, 2011.
25. Rosenthal, L. Jacobson, Pygmalion im Unterricht. Lehrererwartungen und Intelligenzentwicklung der Schüler. Beltz, 1983.
26. საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 17 დეკემბრის №2/6/1311 გადაწყვეტილება საქმეზე „მპს სტერეო+“, ლუკა სევერინი, ლაშა ზილფიმიანი, რობერტ ხახალავი და დავით ზილფიმიანი საქართველოს პარლამენტისა და საქართველოს იუსტიციის მინისტრის წინააღმდეგ.
27. საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის №1/4/693,857 გადაწყვეტილება საქმეზე „ა(ა)იპ მედიის განვითარების ფონდი“ და ა(ა)იპ ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ.
28. Handyside v United Kingdom [1976] ECHR 5 at para. 48, (1976) 1 EHRR 737, [1976] ECHR 5493/72 (7 December 1976), European Court of Human Rights.
29. S. and Marper v. The United Kingdom, [2008] ECHR, nos. 30562/04 and 30566/04.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობა და კონტროლი

სტატიაში განხილულია პერსონალურ მონაცემთა დამუშავების კანონიერება და ზომიერება ფარული საგამოძიებო მოქმედების ჩატარებისას, კერძოდ, თუ რამდენად ეფექტური და შესაბამისია საერთაშორისო სტანდარტებთან დღეს მოქმედი კონტროლის მექანიზმი.

სტატიაში შეფასდება პერსონალურ მონაცემთა დაცვის სამსახურის მანდატი და უფლებამოსილება, რომლის საფუძველზეც სამსახური ახორციელებს ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობას და კონტროლს. საკითხი განსაკუთრებით აქტუალურია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ძალაში შესვლის შემდგომ, როდესაც სამსახურს მიენიჭა სახელმწიფო საიდუმლოსთვის მიკუთვნებულ მონაცემთა დამუშავების კანონიერების შეფასების მანდატი.

საკვანძო სიტყვები: პერსონალური მონაცემი, ფარული საგამოძიებო მოქმედება, კონტროლის მექანიზმი, სისხლის სამართლის საპროცესო კოდექსი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.

1. შესავალი

თანამედროვე ეპოქაში, სადაც ციფრულ ანაბეჭდს ადამიანი ყველგან ტოვებს, მონაცემთა დამუშავების კანონიერების შეფასება ცალკეულ შემთხვევებში ხშირად კანონის მოქმედების ფარგლებს გარეთ რჩება. ფარული საგამოძიებო მოქმედებების ჩატარებას განსაკუთრებული ყურადღება ექცევა, გამომდინარე იქედან, რომ იგი დაკავშირებულია განზრახი მძიმე ან განზრახი განსაკუთრებით მძიმე დანაშაულის გამოძიებასთან. აღნიშნული საგამოძიებო მოქმედება ხშირ შემთხვევაში მოითხოვს დიდი რაოდენობით სხვადასხვა ტიპის მონაცემების დამუშავებას, რა დროსაც სავალდებულოა, როგორც სისხლის სამართლის საპროცესო, ისე პერსონალურ მონაცემთა დაცვის კანონმდებლობის ზედმიწევნით დაცვა და მონაცემთა დამუშავების მინიმუზაცია.

* ილიას სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის სისხლის სამართლის მიმართულების მაგისტრანტი. პერსონალურ მონაცემთა დაცვის სამსახურის იურიდიული დეპარტამენტის უმცროსი იურისტი.

ფარული საგამოძიებო მოქმედების დროს მონაცემთა დამუშავების მინიმიზაციის პრინციპი არ არის მხოლოდ ორგანიზაციულ-ტექნიკური ან პროცედურული საკითხი.

აღსანიშნავია, რომ ფარული საგამოძიებო მოქმედებების კონტროლი არ რეგულირდება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ (შემდეგში, „GDPR“), არამედ რეგულირდება საპოლიციო სექტორში პერსონალურ მონაცემთა დამუშავების შესახებ დირექტივით (შემდეგში, „LED“), აქვე აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომელიც 2024 წლის პირველ მარტს ამოქმედდა, დიდწილად შეესაბამება საერთაშორისო სტანდარტებს.

„LED“ სამართალდამცავი ორგანოების მიერ სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის განხორციელებისას პერსონალური მონაცემების დამუშავების კონკრეტულ წესებსა და სტანდარტებს ადგენს, კერძოდ, კანონიერება, სამართლიანობა, გამჭვირვალობა და მონაცემთა დამუშავება სუბიექტის ღირსების შეუღახავად, მონაცემთა დამუშავება კონკრეტულად განსაზღვრული და ლეგიტიმური მიზნით, მონაცემთა მინიმიზაცია, მონაცემთა ნამდვილობა და სიზუსტე, მონაცემთა შენახვის ვადის შეზღუდვა და მონაცემთა უსაფრთხოება. ეს წესები შექმნილია იმის უზრუნველსაყოფად, რომ მონაცემთა დამუშავების რიგი საგამოძიებო მოქმედებები იყოს აუცილებელი, პროპორციული და განხორციელდეს ინდივიდების უფლებების დაცვით.¹

კვლევის მიზანია ფარული საგამოძიებო მოქმედებების კონტროლის საკანონმდებლო ჩარჩოს მიმოხილვა. კვლევის ფარგლებში განხილული იქნება მონაცემთა მინიმიზაციის პრინციპი, ასევე საუკეთესო პრაქტიკა და მეთოდები, რომელთა გათვალისწინება განსაკუთრებით მნიშვნელოვანია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ამოქმედების შემდეგ. კვლევაში ხაზგასმულია სამართალდამცავი ორგანოების როლი და ინდივიდის ძირითად უფლებებისა და თავისუფლებების დაცვა დემოკრატიულ საზოგადოებაში.

2. ფარული საგამოძიებო მოქმედების ჩატარების სამართლებრივი ჩარჩო

სამართალდამცავი ორგანოების მიერ ჩატარებულ ფარულ საგამოძიებო მოქმედებებსა და პერსონალურ მონაცემთა დაცვას შორის ურთიერთმიმართების საკმაოდ რთული სამართლებრივი ლანდშაფტია, თუმცა აღნიშნული პროცესის კანონთან ჰარმონიზაცია დიდ გამოწვევასთან ერთად, ადამიანის ისეთი ფუნდამენტური უფლების დაცვას ემსახურება, როგორიცაა პირადი ცხოვრების ხელშეუხებლობა.

ფარული საგამოძიებო მოქმედება (ოპერატიულ-სამძებრო მოქმედება), როგორც *Ultima Ratio*, მოიაზრებს სხვადასხვა ტექნიკითა თუ საშუალებით მტკიცებულებათა შეგროვებას, რა თქმა უნდა, ინდივიდთა წინასწარი გაფრთხილების გარეშე.² ზემოთ ხსენებულ მოქმედებას სახელმწიფო უსაფრთხოების სამსახურის სსიპ „ოპერატიულ-ტექნიკური სააგენტო“ ახორციელებს,

¹ საპოლიციო სექტორში პერსონალურ მონაცემთა დამუშავების შესახებ დირექტივის მე-4 მუხლი.

² აქუბარდია ი., კონტროლის მექანიზმები ფარულ საგამოძიებო მოქმედებებზე, სტატიათა კრებული - რევაზ გოგშელიძე 65, თბ., 2022, 200.

კონკრეტული დანაშაულების მიმართ, რომლებსაც სისხლის სამართლის საპროცესო კოდექსის 34-ე მუხლის პირველი ნაწილით გათვალისწინებული ორგანოები იძიებენ.³

სხვა საგამოძიებო მოქმედებებისგან განსხვავებით, ფარული საგამოძიებო მოქმედების ჩატარება, მხოლოდ მძიმე ან განსაკუთრებით მძიმე დანაშაულის წინააღმდეგ შესაძლოა, ჩატარდეს, აგრეთვე საგულისხმოა სისხლის სამართლის საპროცესო კოდექსის 143³ მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ცალკეული დანაშაულები, სადაც შესაძლოა ზემოხსენებული საგამოძიებო მოქმედების განხორციელება, აღნიშნულ ჩამონათვალში ჩვენ ვხვდებით ისეთ დანაშაულთა ჯგუფებს, როგორებიცაა:

- დანაშაული ჯანმრთელობის წინააღმდეგ;
- ადამიანის სიცოცხლისა და ჯანმრთელობისათვის საფრთხის შექმნა;
- დანაშაული სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ;
- დანაშაული ადამიანის უფლებებისა და თავისუფლებების წინააღმდეგ;
- ეკონომიკური დანაშაული;
- დანაშაული სამეწარმეო ან სხვა ეკონომიკური საქმიანობის წინააღმდეგ;
- დანაშაული ფულად-საკრედიტო სისტემაში;
- დანაშაული მოსახლეობის ჯანმრთელობისა და საზოგადოებრივი ზნეობის წინააღმდეგ;
- კიბერდანაშაული;
- დანაშაული გარემოს დაცვისა და ბუნებრივი რესურსებით სარგებლობის წესის წინააღმდეგ;
- დანაშაული საქართველოს კონსტიტუციური წყობილებისა და უშიშროების საფუძვლების წინააღმდეგ;
- ოკუპირებული ტერიტორიების სამართლებრივი რეჟიმის დარღვევა;
- სამოხელეო დანაშაული.

გარდა მუხლობრივი განსაზღვრებისა, აუცილებლად გასათვალისწინებელია ის ლეგიტიმური მიზნები, რომელთა მისაღწევადაც ტარდება ფარული საგამოძიებო მოქმედება, კერძოდ კი:

- ეროვნული უშიშროების უზრუნველსაყოფად;
- საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად;
- უწესრიგობის თვიდან ასაცილებლად;
- დანაშაულის ჩადენის თავიდან ასაცილებლად;
- ქვეყნის ეკონომიკური კეთილდღეობის ინტერესების დასაცავად;
- სხვა პირთა უფლებებისა და თავისუფლებების დასაცავად.

ფარული საგამოძიებო მოქმედების ჩატარების ფარგლები (ინტენსივობა) ზემოაღნიშნული ლეგიტიმური მიზნების პროპორციული უნდა იყოს, რომლებიც პირდაპირ ეხმიანება ადამიანის უფლებათა საერთაშორისო სამართლის მიხედვით, ევროპული სასამართლოს პრაქტიკასა და სხვა საერთაშორისო თუ რეგიონული სამართლებრივი ინსტრუმენტებისა და სტანდარტების შესაბამისად გაქდურებულ ზოგად მოთხოვნებს.⁴

³ საქართველოს სისხლის სამართლის საპროცესო კოდექსის 34-ე მუხლის პირველი ნაწილი.

⁴ ფავლენიშვილი ლ., თუმანიშვილი გ. და სხვები, საქართველოს სისხლის სამართლის საპროცესო კომენტარი (2015 წლის 1 ოქტომბრის მდგომარეობით), თბ., 2015, 428-429.

მოქმედი საკანონმდებლო ცვლილების იურიდიულ საკითხთა კომიტეტის დასკვნის მიხედვით, ფარული საგამოძიებო მოქმედების ჩატარების ვადის განსაზღვრის საკითხთან დაკავშირებით აუცილებელია ადამიანის უფლებათა ევროპული სასამართლოს მიერ დადგენილი პრაქტიკის გათვალისწინება. მის თანახმად, აღნიშნული საკითხი სახელმწიფოს დისკრეციულ უფლებამოსილებას განეკუთვნება. ფარული საგამოძიებო მოქმედების ჩატარების ვადის გახანგრძლივება კი ლეგიტიმური მიზნის მისაღწევად, მათ შორის, საზოგადოებრივი წესრიგის დასაცავად და დანაშაულის წინააღმდეგ ეფექტიანი ბრძოლის საწარმოებლად, შესაძლებელია იმდენჯერ, რამდენჯერაც ამის საჭიროება იარსებებს, შესაბამისი კონტროლით და სათანადო საპროცესო გარანტიების პირობებში.⁵

ნებისმიერი ლეგიტიმური მიზნით ჩატარებული ფარული საგამოძიებო მოქმედება იმავდროულად სისხლის სამართლის საქმისთვის მნიშვნელობის მქონე მტკიცებულების მოპოვებას ისახავს მიზნად. თუმცა, მხოლოდ ის ფაქტი, რომ ფარული საგამოძიებო მოქმედების ჩატარების გზით საქმისათვის მნიშვნელობის მქონე მტკიცებულების მოპოვება უნდა მოხდეს, ან თავიდან იქნეს აცილებული დანაშაული, ვერ გამოდგება სასამართლოს მხრიდან ამგვარი მოქმედების ჩატარებაზე ნებართვის გაცემის საკმარის საფუძვლად. მხარემ დამატებით უნდა დაადასტუროს ისიც, რომ სხვა საშუალებით, ანუ სხვა საგამოძიებო/საპროცესო მოქმედების ჩატარების გზით ამგვარი მტკიცებულების მოპოვება და ამგვარი მიზნის მიღწევა შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს.⁶

ზემოხსენებული სტანდარტების დაცვის მტკიცების ტვირთი რა თქმა უნდა სახელმწიფო ბრალმდებელზეა, სწორედ პროკურორი შუამდგომლობს სასამართლოში ფარული საგამოძიებო მოქმედების განხორციელების შესახებ, კერძოდ პროკურორის შუამდგომლობა განიხილება არაუგვიანეს 24 საათში. განხილვის შემდგომ მოსამართლე იღებს განჩინებას ნებართვის გაცემაზე ან უარის თქმის შესახებ.

მოსამართლის განჩინება დგება 4 ეგზემპლარად, რომელთაგან ორი გადაეცემა შუამდგომლობის წარმდგენ პროკურორს, ერთი რჩება სასამართლოში, ხოლო ერთი განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, დაუყოვნებლივ, მაგრამ არაუგვიანეს 48 საათისა, მიეწოდება პერსონალურ მონაცემთა დაცვის სამსახურს მატერიალური სახით.

ფარული საგამოძიებო მოქმედება ასევე ტარდება გადაუდებელი აუცილებლობის ფარგლებშიც, რა დროსაც პროკურორი დადგენილების ერთი ეგზემპლარი ეგზავნება პერსონალურ მონაცემთა დაცვის სამსახურს.

⁵ იურიდიულ საკითხთა კომიტეტის დასკვნა „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“ საქართველოს კანონზე (№1614-VIIIმს-Xმპ, 7/06/2022) საქართველოს პრეზიდენტის მოტივირებული შენიშვნების თაობაზე (№07-1/14, 23/06/2022).

⁶ *ფაფიაშვილი ლ., თუმანიშვილი გ. და სხვები*, საქართველოს სისხლის სამართლის საპროცესო კომენტარი (2015 წლის 1 ოქტომბრის მდგომარეობით), თბ., 2015, 429.

3. კონტროლი ფარულ საგამოძიებო მოქმედებებსა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობებზე

3.1. პერსონალურ მონაცემთა დაცვის სამსახურის მანდატი

საქართველოში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი სათავეს 2013 წლიდან იღებს. ხოლო 2014 წელს განხორციელებული საკანონმდებლო ცვლილებებით „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი გავრცელდა დანაშაულის თავიდან აცილებისა და გამოძიების, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისათვის სახელმწიფო საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ავტომატურ დამუშავებაზე და პერსონალურ მონაცემთა დაცვის ინსპექტორს მიენიჭა ფარული საგამოძიებო მოქმედებების და ფარული საგამოძიებო მოქმედებების და უფლებამოსილი ორგანოს მონაცემთა ბანკებში განხორციელებული აქტივობების კონტროლის უფლებამოსილება. 2015 წლის 31 მარტიდან ძალაში შესული საკანონმდებლო ცვლილებების თანახმად, პერსონალურ მონაცემთა დაცვის ინსპექტორს განესაზღვრა საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-138 მუხლებითა და 143¹ მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ საგამოძიებო მოქმედებებზე ზედამხედველობის უფლებამოსილება.⁷

ხოლო 2019 წლიდან 2022 წლამდე მისი უფლებამონაცვლე სახელმწიფო ინსპექტორის სამსახური ახორციელებდა ზემოხსენებულ უფლებამოსილებას.

2022 წლის პირველი მარტიდან აღნიშნული მანდატი პერსონალურ მონაცემთა დაცვის სამსახურს მიენიჭა, რომლის ერთ-ერთი ძირითადი ფუნქცია საქართველოში პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულებაზე ზედამხედველობა და მონაცემთა დამუშავების კანონიერების კონტროლია.

ნებისმიერი დემოკრატიული სახელმწიფოსათვის მნიშვნელოვანია სამართალდამცავი ორგანოების მიერ ფარული საგამოძიებო მოქმედებების განხორციელების კანონიერების კონტროლი პერსონალურ მონაცემთა დამუშავებისას და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე წვდომის პროცესში.

3.2. კონტროლის მექანიზმი

როგორც უკვე აღინიშნა სამსახურის ერთ-ერთი ფუნქციაა ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი, რაც უზურპაციის წინააღმდეგ მიმართულ მექანიზმად შეიძლება იწოდოს, ვინაიდან ფარული საგამოძიებო მოქმედებები, არსობრივად საკმაოდ სენსიტიურ საკითხს წარმოადგენს, რაც შესაძლოა გახდეს იმ ფუნდამენტურ უფლებებში უხეში ჩარევის ინსტრუმენტი, რომელთა დაცვას სახელმწიფო თავად უნდა უზრუნველყოფდეს.

სამსახური ზედამხედველობას უწევს საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143¹-ე მუხლის პირველი ნაწილით განსაზღვრულ ფარულ

⁷ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის 2015 წლის ანგარიში, 34.

საგამოძიებო მოქმედებებს, ასევე, ამავე კოდექსის XVI¹ თავით გათვალისწინებული ნორმების დაცვის ფარგლებში. ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლის მიზნით, სამსახურს 24-საათიან რეჟიმში მიეწოდება სასამართლოს განჩინებების რეკვიზიტები და სარეზოლუციო ნაწილი ასეთი მოქმედებების ჩატარების ნებართვის გაცემის შესახებ, გადაუდებელი აუცილებლობის შემთხვევაში ასევე, პროკურორის დადგენილებების რეკვიზიტები და სარეზოლუციო ნაწილი ფარული საგამოძიებო მოქმედების ჩატარებაზე და სამართალდამცავი ორგანოების მიერ ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით შედგენილი ოქმები.

სამსახური აგრეთვე, იღებს შეტყობინებებს, რომლებიც ასახავს ელექტრონული კომუნიკაციის კომპანიების მიერ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა გადაცემას სამართალდამცავი ორგანოებისთვის. სამსახური ამოწმებს მიღებულ დოკუმენტებს, ადარებს ელექტრონულ სისტემებში ასახულ ინფორმაციას, დოკუმენტაციაში ასახული მონაცემები შეაქვს ფარული საგამოძიებო მოქმედებების აღრიცხვის შიდა ელექტრონულ სისტემაში და აანალიზებს მათ. ზემოაღნიშნული მექანიზმების გარდა, ფარული საგამოძიებო მოქმედების — სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის მონიტორინგისთვის, სამსახური იყენებს კონტროლის ელექტრონულ და სპეციალურ ელექტრონულ სისტემებს, ხოლო ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლისათვის გამოიყენება ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემა.⁸

გარდა ამისა, პერსონალურ მონაცემთა დაცვის სამსახური აკონტროლებს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობებს კონტროლის სისტემით და მონაცემთა დამუშავების/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით ანუ ინსპექტირებით.⁹

3.3. სტატისტიკა

საინტერესოა ის ფაქტი, რომ პერსონალურ მონაცემთა დაცვის სამსახურში სტატისტიკის წარმოების ერთიანი მდგომარეობის დამკვიდრებისა და შესაბამისი სტანდარტების დანერგვის მიზნით, შეიმუშავეს მეთოდოლოგია, რომლითაც ხორციელდება სამსახურის საქმიანობის შესახებ სტატისტიკური მონაცემების დაჯამება და ანალიზი.¹⁰

მაგალითისათვის განხილულ იქნა პერსონალურ მონაცემთა დაცვის სამსახურის გასული წლის სტატისტიკა, რომლის თანახმადაც სამსახურმა სატელეფონო კომუნიკაციის ფარული მიყურადება-ჩაწერის შეჩერების მექანიზმი (კონტროლის

⁸ პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 12 თვის საქმიანობის სტატისტიკა (იანვარი-დეკემბერი), 7.

⁹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, 49-ე მუხლის „გ“ ქვეპუნქტი.

¹⁰ პერსონალურ მონაცემთა დაცვის მდგომარეობის, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლის შესახებ წლიური სტატისტიკის წარმოების მეთოდოლოგია, 2024.

ელექტრონული სისტემის საშუალებით) 76 შემთხვევაში გამოიყენა, რაც გამოწვეული იყო სასამართლოს განჩინების დაგვიანებით წარმოდგენით (74 შემთხვევა), სასამართლოს მიერ გადაუდებელი აუცილებლობიდან გამომდინარე პროკურორის დადგენილების საფუძველზე დაწყებული ფარული საგამოძიებო მოქმედების უკანონოდ ცნობით (1 შემთხვევა) და ფარული საგამოძიებო მოქმედების შეწყვეტით (1 შემთხვევა).

- სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის შესახებ სასამართლომ განიხილა 859 შუამდგომლობა, რომელთა 87% (744) სრულად დაკმაყოფილდა, 9% (80) არ დაკმაყოფილდა, ხოლო 4% (35) ნაწილობრივ დაკმაყოფილდა.
- სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ვადის გაგრძელების შესახებ სასამართლომ განიხილა 228 შუამდგომლობა, რომელთაგან დაკმაყოფილდა 87% (199), ნაწილობრივ დაკმაყოფილდა 9% (21), არ დაკმაყოფილდა 4% (8).
- ფარული ვიდეოჩაწერის ან/და აუდიოჩაწერის, ფოტოგადაღების შესახებ სასამართლომ განიხილა 1024 შუამდგომლობა, რომელთაგან 93% (952) სრულად დაკმაყოფილდა, 6.6% (68) არ დაკმაყოფილდა, ხოლო 0.4% (4) ნაწილობრივ დაკმაყოფილდა.
- ფარული ვიდეოჩაწერის ან/და აუდიოჩაწერის, ფოტოგადაღების ვადის გაგრძელების შესახებ სასამართლომ განიხილა 120 შუამდგომლობა, რომელთა 87% (105) დაკმაყოფილდა, 11% (13) არ დაკმაყოფილდა, ხოლო 2% (2) ნაწილობრივ დაკმაყოფილდა.
- სასამართლომ განიხილა 3 შუამდგომლობა ფარული საგამოძიებო მოქმედების კავშირგაბმულობის არსებიდან, კომპიუტერული სისტემიდან ინფორმაციის მოხსნისა და ფიქსაციის თაობაზე, რომელთაგან 1 დაკმაყოფილდა, ხოლო 2 არ დაკმაყოფილდა.
- სასამართლომ განიხილა 1 შუამდგომლობა ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების თაობაზე, რომელიც დაკმაყოფილდა.
- სამსახურს წარედგინა გადაუდებელი აუცილებლობით ფარული საგამოძიებო მოქმედებების ჩატარების შესახებ პროკურორის 92 დადგენილება, რომელთაგან 83% (76) შეეხებოდა ფარულ ვიდეოჩაწერას ან/და აუდიოჩაწერას, ფოტოგადაღებას, 17% (16) შეეხებოდა სატელეფონო კომუნიკაციის ფარულ მიყურადებასა და ჩაწერას. პერსონალურ მონაცემთა დაცვის სამსახურს წარედგინა სასამართლოს განჩინებები და გადაუდებელი აუცილებლობიდან გამომდინარე პროკურორის დადგენილებები სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული საგამოძიებო მოქმედების, დოკუმენტის ან ინფორმაციის გამოთხოვის შესახებ. კოდექსის 136-ე მუხლთან დაკავშირებით წარდგენილი დოკუმენტებიდან პროკურორების დადგენილებებმა შეადგინა 2%, ხოლო სასამართლოს განჩინებებმა 98%. სამსახურს წარედგინა სასამართლოს 1490 განჩინება. დამატებით, სამსახურმა მიიღო პროკურორის 34 დადგენილება გადაუდებელი აუცილებლობით საგამოძიებო მოქმედებების ჩატარების თაობაზე კოდექსის 136-ე მუხლის შესაბამისად.
- სსიპ „საქართველოს ოპერატიულ-ტექნიკურ სააგენტოს“ სასამართლოს მიერ სატელეფონო კომუნიკაციის ფარულ მიყურადება-ჩაწერაზე გაცემულ

ნებართვებში არსებულ ბუნდოვანება-უზუსტობაზე (კონტროლის ელექტრონული სისტემის საშუალებით) ეცნობა 6-ჯერ.

- კონტროლის ელექტრონული სისტემის საშუალებით სატელეფონო კომუნიკაციის ფარული მიყურადება-ჩაწერის პროცესში ინციდენტი არ გამოვლენილა.
- ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემით სამსახურისთვის მოწოდებული ინფორმაციის საფუძველზე, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკიდან სსიპ „ოპერატიულ-ტექნიკური სააგენტოს“ მიერ მონაცემები სასამართლოს შესაბამისი გადაწყვეტილებების საფუძველზე გაიცა 71-ჯერ.
- ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობათა კონტროლის შედეგად რაიმე ხარვეზი ან ინციდენტი არ გამოვლენილა.¹¹

აღნიშნული სტატისტიკა წარსულში არსებულ მარეგულირებლებთან შედარებით გაზრდილია, რაც პერსონალურ მონაცემთა დაცვის სამსახურის მაღალ ეფექტიანობას და მანდატის გაძლიერებისკენაა მიმართული, ეს ყოველივე დადებით მოვლენად უნდა ჩაითვალოს, რადგანაც ერთ დროს სრულიად კანონის კონტროლს გარეთ არსებული სფერო, ზედამხედველობის არეალში მოექცა, აღნიშნულს ცხადყოფს პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2016 წლის ანგარიშიც, რომელშიც ნახსენებია ფაქტი იმის შესახებ, რომ ექვს შემთხვევაში, დადგენილების ეგზემპლარი არ წარუდგენიათ საზედამხედველო ორგანოსთვის. მიზეზად მთავარმა პროკურატურამ განმარტა, რომ პროკურორის დადგენილების წარმოუდგენლობა განპირობებული იყო დროის სიმწირითა და მრავალი გადაუდებელი აუცილებლობით ჩატარებული საგამოძიებო მოქმედებების რიცხვით. ასევე, ამავე წელს დადგინდა დადგენილების დაგვიანებით წარმოდგენის 3 ფაქტი.¹²

3.4. ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურება

ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებულ ინფორმაციას ანადგურებს შესაბამისი საქმის გამოძიებაზე საპროცესო ზედამხედველობის განმახორციელებელი ან სახელმწიფო ბრალდების მხარდამჭერი ან მათი ზემდგომი პროკურორი, იმ მოსამართლის ან სასამართლოს მოსამართლის თანდასწრებით, რომელმაც ან რომლის მოსამართლემაც მიიღო გადაწყვეტილება აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების შესახებ ან გადაუდებელი აუცილებლობისას, მოსამართლის განჩინების გარეშე ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად ან უკანონოდ ცნობის შესახებ. ფარული

¹¹ პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 12 თვის საქმიანობის სტატისტიკა (იანვარი-დეკემბერი), 9.

¹² პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2016 წლის ანგარიში, <<https://old.pdps.ge/ka/download/2870>> [05.08.2024].

საგამოძიებო მოქმედების შედეგად მოპოვებული მასალის განადგურების შესახებ შესაბამისი პროკურორისა და მოსამართლის ხელმოწერებით დადასტურებული ოქმი გადაეცემა პერსონალურ მონაცემთა დაცვის სამსახურს და აისახება ფარული საგამოძიებო მოქმედებების სასამართლო რეესტრში.¹³

საინტერესოა LED-ის მიდგომა ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებული ინფორმაციის განადგურებასთან დაკავშირებით, რომლის თანახმადაც, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ პერსონალურ მონაცემთა წაშლის სათანადო ვადების განსაზღვრა და პერსონალური მონაცემების შენახვის საჭიროების პერიოდული გადასინჯვა. პროცედურული ზომებით უზრუნველყოფილი უნდა იყოს ამ ვადების სათანადოდ დაცვა, რაც შესაძლოა ჩაითვალოს ქართულ მოდელთან ახლოს მყოფ მიდგომასთან.

4. საერთაშორისო სტანდარტები

4.1. მარეგულირებელი ორგანოები

ფარული საგამოძიებო მოქმედებების ჩატარების დროს მოქმედებების ობიექტს მხოლოდ ფარული საგამოძიებო მოქმედების დასრულების შემდეგ ეძლევა შესაძლებლობა სრულფასოვნად დაიცვას საკუთარი უფლებები და შესაბამისად, განსაკუთრებით მნიშვნელოვანია, აღნიშნული მოქმედებების დროს ქმედების განმახორციელებელი ორგანოს კონტროლი. აღნიშნული კონტროლის სათანადოდ განხორციელება, მოქმედებების ობიექტისთვის შეტყობინებამდე არის ერთადერთი სამართლებრივი გარანტია, რომელიც ფარული საგამოძიებო მოქმედებების ობიექტსა და მესამე პირებს იცავს თვითნებობისგან.

ფარულ მიყურადებას და სხვა ფარულ ღონისძიებებს, უმეტეს შემთხვევაში, შესაბამისი ქვეყნების უსაფრთხოების სამსახურები ახორციელებენ. მაგალითად, საქართველოს ოპერატიულ-ტექნიკური სააგენტო სახელმწიფო უსაფრთხოების სამსახურის დაქვემდებარებაშია. უსაფრთხოების სამსახურების საქმიანობაზე საზედამხედველო ორგანოები კი ყველა ქვეყანაში განსხვავებულია. საზედამხედველო ორგანოების შექმნის, საქმიანობის, საუკეთესო პრაქტიკის შესახებ არსებობს როგორც გაეროს, ისე ევროსაბჭოს და ვენეციის კომისიის კვლევითი დოკუმენტები, რომლებიც მნიშვნელოვან რეკომენდაციებს იძლევა ეფექტიანი საზედამხედველო ინსტიტუტების შექმნისა და ფუნქციონირებისთვის. ევროსაბჭოს 2015 წლის კვლევითი ანგარიშის თანახმად, ევროსაბჭოს წევრი არც ერთი ქვეყნის საზედამხედველო სისტემა სრულად არ შეესაბამება აღიარებულ საერთაშორისო სტანდარტებსა და პრინციპებს, ასევე, არ არსებობს ზედამხედველობის ერთი საუკეთესო მოდელი. თუმცა, არსებობს გარკვეული პრაქტიკა და მიდგომები, რომლებიც საყურადღებოა ადამიანის უფლებათა დაცვის პერსპექტივიდან.¹⁴ ევროსაბჭოს ხსენებული დოკუმენტის თანახმად, ევროსაბჭოს წევრ ქვეყნებში უსაფრთხოების სამსახურების ზედამხედველი ორგანოები არიან: საპარლამენტო კომიტეტები, დამოუკიდებელი ზედამხედველობის ინსტიტუტები, სასამართლოები, კვაზი-სასამართლო ორგანოები.

¹³ აქუბარდია ი., კონტროლის მექანიზმები ფარულ საგამოძიებო მოქმედებებზე, სტატიათა კრებული - რევაზ გომელაძე 65, თბ., 2022, 228.

¹⁴ Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services, 2015, 8, <<https://rm.coe.int/1680487770>> [31.07.2024].

4.2. ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა

ა. Roman Zakharov and Others v. Russia¹⁵

განმცხადებელმა, რომელიც იყო საგამომცემლო კომპანიის მთავარი რედაქტორი, დაიწყო სამართალწარმოება სამი მობილური ქსელის ოპერატორის წინააღმდეგ, აცხადებდა რა, რომ ხდებოდა მისი სატელეფონო კომუნიკაციების დაცულობის უფლებაში ჩარევა. იგი ამტკიცებდა, რომ შესაბამისი ეროვნული კანონმდებლობის თანახმად, მობილური ქსელის ოპერატორებმა დაამონტაჟეს სისტემა/აპარატურა, რომელიც ფედერალური უშიშროების სამსახურს (FSB) აძლევდა საშუალებას, განეხორციელებინა სატელეფონო კომუნიკაციაზე მონიტორინგი წინასწარი სასამართლო ნებართვის გარეშე. მან იშუამდგომლა სისტემის/აპარატურის მოხსნაზე და უზრუნველყოფილიყო ტელეკომუნიკაციებზე წვდომა მხოლოდ უფლებამოსილ პირთათვის.

ეროვნულმა სასამართლოებმა არ დააკმაყოფილეს განმცხადებლის მოთხოვნა, მიიჩნიეს რა, რომ მან ვერ დაამტკიცა, რომ ხდებოდა მისი სატელეფონო საუბრების მიყურადება, ან რომ მობილური ქსელის ოპერატორებმა გადასცეს ინფორმაცია არაუფლებამოსილ პირებს. ხოლო სისტემის/აპარატურის მონტაჟი, თავისთავად არ არღვევდა მისი კომუნიკაციების დაცულობას.

ევროპული სასამართლოს წინაშე განმცხადებელი ამტკიცებდა, რომ რუსეთში მობილური ტელეფონების კომუნიკაციების ფარული მიყურადების სისტემა არ შეესაბამებოდა კონვენციის მე-8 მუხლით დადგენილ მოთხოვნებს. 2014 წლის 11 მარტს სასამართლოს პალატამ იურისდიქციაზე უარი თქვა დიდი პალატის სასარგებლოდ.

წინამდებარე საქმეში, გასაჩივრებული კანონმდებლობა პირდაპირ ზემოქმედებდა მობილური სატელეფონო სერვისის ყველა მომხმარებელზე, რადგან მან საფუძველი ჩაუყარა ფარული მიყურადების სისტემას, რომლის ფარგლებშიც ეროვნული პროვაიდერის მობილური სატელეფონო სერვისით მოსარგებლე ნებისმიერი პირის კომუნიკაცია შესაძლოა დაექვემდებაროს მიყურადებას ისე, რომ პირი ფარული საგამოძიებო მოქმედების შესახებ ვერასდროს შეიტყობს. ამასთანავე, ეროვნული კანონმდებლობა არ სთავაზობდა ეფექტიანი დაცვის საშუალებას იმ პირებს, რომლებსაც ეჭვი ჰქონდათ, რომ ექვემდებარებოდნენ ფარულ მიყურადებას. შესაბამისი კანონმდებლობის *in abstracto* შეფასება, შესაბამისად გამართლებული იყო. განმცხადებელს არ სჭირებოდა ემტკიცებინა, რომ მისი პირადი ვითარების გამო იგი იმყოფებოდა ფარული მიყურადების საფრთხის წინაშე. შესაბამისად, მას ჰქონდა კონვენციის დარღვევის მსხვერპლის სტატუსის მოთხოვნის უფლება.

აღნიშნულ გადაწყვეტილებაში მნიშვნელოვანია ზედამხედველობის საკითხი, სადაც გაირკვა რომ - ეროვნული კანონმდებლობით დაწესებული აკრძალვა მიყურადების რეგისტრირებისა და ჩაწერის შესახებ შეუძლებელს ხდის საზედამხედველო ორგანოებისათვის დაადგინონ ის შემთხვევები, როცა მიყურადება განხორციელდა სასამართლო ნებართვის გარეშე. იმასთან ერთად, რომ ხელისუფლების სათანადო ორგანოებს აქვთ ტექნიკური საშუალება, პირდაპირ მიაყურადონ, ამ დებულებამ აზრი დაუკარგა სახელმწიფოში ნებისმიერ საზედამხედველო მექანიზმს და წაართვა მიყურადების კანონიერების შემოწმების

¹⁵ *Case of Roman Zakharov v. Russia*, (Application no. 47143/06), <hudoc.echr.coe> [31.07.2024].

საშუალება, შესაბამისად, ეს მექანიზმი არაეფექტიანია. მართალია, საკანონმდებლო ბაზა თეორიულად ადგენდა გარკვეულ საპროკურორო ზედამხედველობას, მაგრამ პრაქტიკაში კანონმდებლობამ ვერ შეძლო ადეკვატური და ეფექტური გარანტიების დადგენა თვითნებობის წინააღმდეგ.

ბ. Podchasov v. Russia¹⁶

2024 წლის 13 თებერვალს, ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეზე Podchasov v. Russia გადაწყვეტილება მიიღო, რომელიც სამართალდამცავი ორგანოების მიერ ელექტრონულ საკომუნიკაციო სისტემებზე განუსაზღვრელი ფარგლებითა და ვადით წვდომის საკითხს შეეხება, კერძოდ, მიმოწერათა „სუსტი დაშიფვრის სისტემისა“ (“Encryption Mechanism”) და მათ შინაარსზე ხელმისაწვდომობის საკითხს.

რუსეთის ფედერაციის სისხლის სამართლის საპროცესო კოდექსისა და ოპერატიულ-სამძებრო საქმიანობის აქტის საფუძველზე, ელექტრონული კომუნიკაციის კომპანიებს დაევალებათ საკომუნიკაციო მონაცემების ერთი წლის ვადით, ხოლო მათი შინაარსის — ექვსი თვის განმავლობაში შენახვა. აღნიშნული მონაცემი, მათ შორის ნებისმიერი ისეთი ინფორმაცია, რომელიც სამართალდამცავ ორგანოებს კომუნიკაციების გამიფვრაში დაეხმარებოდათ, ელექტრონული კომუნიკაციის კომპანიებს მოთხოვნისთანავე უნდა წარედგინათ.

საქმის ფაქტობრივი გარემოებების თანახმად, რუსეთის სახელმწიფო უსაფრთხოების ფედერალურმა სამსახურმა ელექტრონული კომუნიკაციის კომპანია “Telegram”-ს მოსთხოვა, წარედგინა სისტემური ინფორმაცია, რომელიც სამსახურს ექვსი მობილური ნომრის კომუნიკაციის გამიფვრაში დაეხმარებოდა. აღსანიშნავია, რომ მობილური ნომრების მომხმარებლები, შეტყობინებათა დაშიფვრის მიზნით, პლატფორმა “Telegram”-ის „საიდუმლო მიმოწერის“ ფუნქციას იყენებდნენ.

მომჩივანი აცხადებდა, რომ სამართალდამცავი ორგანოების მიერ ელექტრონულ საკომუნიკაციო სისტემაზე განუსაზღვრელი ფარგლებითა და ვადით წვდომა ეწინააღმდეგებოდა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლს.

ევროპულმა სასამართლომ ყურადღება გაამახვილა ციფრულ ეპოქაში ელექტრონული კომუნიკაციების კონფიდენციალობის უზრუნველყოფის მექანიზმებზე, მათ შორის, მიმოწერის დაშიფვრის ღონისძიებებზე, რაც ხელს უწყობს სხვა ძირითადი უფლებით სარგებლობას. კომუნიკაციის დაშიფვრა მომხმარებლებს საშუალებას აძლევს, დაიცვან საკუთარი მონაცემები და აირიდონ კონფიდენციალური ინფორმაციის გამჟღავნება. სტრასბურგის სასამართლომ დაადგინა, რომ ელექტრონულ საკომუნიკაციო სისტემაში დაცული მონაცემების გამიფვრის მოთხოვნა იყო არაპროპორციული, რამდენადაც ეროვნული კანონმდებლობა არ ითვალისწინებდა შესაბამისი და სათანადო დასაბუთების ვალდებულებას.

სასამართლომ აღნიშნა, რომ პერსონალური მონაცემების დაცვას არსებითი მნიშვნელობა აქვს ინდივიდის პირადი და ოჯახური ცხოვრების პატივისცემის უფლებით სარგებლობისთვის. ეროვნული კანონმდებლობით უზრუნველყოფილი უნდა იყოს შესაბამისი გარანტიები, რათა თავიდან იქნეს არიდებული პერსონალური

¹⁶ ადამიანის უფლებათა ევროპულმა სასამართლომ სამართალდამცავი ორგანოების მიერ ელექტრონულ საკომუნიკაციო სისტემაზე უსაფუძვლო და განუსაზღვრელი წვდომის დაუშვებლობის შესახებ გადაწყვეტილება მიიღო, იხ. <pdps.ge/ka> [31.07.2024], მითითებულია: *Case of Podchasov v. Russia*, Application no. 33696/19, 13 February 2024.

მონაცემების კონვენციის მე-8 მუხლთან შეუსაბამოდ დამუშავება. ამგვარ ღონისძიებათა არსებობა მნიშვნელოვანია პერსონალური მონაცემების ავტომატური დამუშავების პროცესში — განსაკუთრებით კი მაშინ, როდესაც მონაცემები სამართალდამცავი მიზნებისთვის გამოიყენება. სასამართლომ განმარტა, რომ თანამედროვე ტექნოლოგიების დაბალანსებული გამოყენების გარეშე სამართალდამცავი მიზნებისათვის კონვენციის მე-8 მუხლით დაცულ სფეროში ჩარევა, არაპროპორციულ ზომას წარმოადგენს. შესაბამისად, პერსონალური მონაცემების დამუშავების კონტექსტში აუცილებელია, არსებობდეს მკაფიო და დეტალური წესები მონაცემთა შენახვის, გამოყენებისა და მათზე წვდომის შესახებ. ხოლო მონაცემთა შენახვის ვადა უნდა განისაზღვროს შეგროვების კანონიერი მიზნის პროპორციულად.

საქმის ფაქტობრივი გარემოებების შეფასების საფუძველზე, ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ სისტემაში არსებული ყველა მონაცემისა და მეტამონაცემის ხანგრძლივი ვადით შენახვა ზემოქმედებდა ინტერნეტ-კომუნიკაციების ყველა მომხმარებელზე, მიუხედავად იმისა, არსებობდა თუ არა რაიმე ეჭვი დანაშაულებრივ ქმედებებში პირის მონაწილეობის შესახებ. შესაბამისად, სასამართლომ დაადგინა, რომ მონაცემთა შენახვისა და ხელმისაწვდომობის მოთხოვნა არღვევდა მონაცემთა კონფიდენციალობას, აგრეთვე, არ ითვალისწინებდა მონაცემთა სუბიექტის უფლების დაცვის სათანადო გარანტიებს.

ზემოაღნიშნულიდან გამომდინარე, სასამართლომ დაადგინა, რომ ეროვნული კანონმდებლობა, რომელიც ითვალისწინებს ყველა ინტერნეტ-მომხმარებლის კომუნიკაციის შენახვას, ასევე, ელექტრონულ საკომუნიკაციო სისტემაზე უსაფრთხოების სამსახურის პირდაპირ წვდომას, მონაცემთა დაცვის ადეკვატური გარანტიების არსებობის გარეშე, ვერ იქნება მიჩნეული, როგორც აუცილებელი დემოკრატიულ საზოგადოებაში. შესაბამისად, სასამართლომ დაადგინა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევა.

ევროპარლამენტარებმა ხაზი გაუსვეს როგორც *ex ante*, ასევე *ex post* ზედამხედველობის აუცილებლობას; ეს შესაბამეა სასამართლოს მიდგომას.¹⁷

გ. *Ekimdzhiev and Others v. Bulgaria*¹⁸

საქმე ეკიმძიევი და სხვები ბულგარეთის წინააღმდეგ ეხება უკანონობისა და უფლებამოსილების ბოროტად გამოყენებისაგან დაცვის არასათანადო სამართლებრივ გარანტიებს საიდუმლო თვალთვალის შემთხვევაში, აგრეთვე, კომუნიკაციის მოსმენების შედეგად მიღებული მონაცემების შენახვასა და მათთან წვდომას.

საქმის ფაქტობრივი გარემოებები: მოსარჩელებად გვევლინებიან ორი იურისტი და მათთან დაკავშირებული ორი არასამთავრობო ორგანიზაცია. ისინი ამტკიცებენ, რომ არიან ბულგარეთის სახელმწიფოს მხრიდან ფარული მიყურადებისა და კომუნიკაციის მოსმენის საფრთხეში, მათი საქმიანობიდან გამომდინარე, ფარულ მიყურადებასთან დაკავშირებით ბულგარეთის მოქმედი კანონმდებლობის საფუძველზე და მისი პრაქტიკაში გამოყენების შედეგად.

¹⁷ European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI)).

¹⁸ Case of *Ekimdzhiev and Others v. Bulgaria*, (Application no. 70078/12), <[https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-214673%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-214673%22])> [05.08.2024].

მნიშვნელოვანია, რომ მოსარჩელები არ ამტკიცებენ თვალთვალის ფაქტის ან მათი კომუნიკაციის მოსმენის განხორციელებას სახელმწიფო ორგანოების მიერ.

ევროპული სასამართლოს შეფასება

ევროპულმა სასამართლომ განიხილა ფარულ მიყურადებასთან დაკავშირებით ბულგარეთის კანონმდებლობის გამოყენების პრაქტიკა, რომელიც, მისი აღნიშვნით, დიდ წილად გაუმჯობესდა ევროპული სასამართლოს გადაწყვეტილების მიღების შემდეგ საქმეზე ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმივეი ბულგარეთის წინააღმდეგ. თუმცა, სასამართლოს მიხედვით, კანონმდებლობა არ აკმაყოფილებდა უკანონობისა და უფლებამოსილების ბოროტად გამოყენებისაგან დაცვის იმ მინიმალურ სტანდარტებს, რომელთა არსებობას მოითხოვს კონვენციის მე-8 მუხლი.

სტატიის თემატიკიდან გამომდინარე, საინტერესოა ზედამხედველობის საკითხის განხილვა, სადაც ევროპულმა სასამართლომ დაადგინა შემდეგი: ბულგარეთის ეროვნული კანონმდებლობით არ იყო დადგენილი საკომუნიკაციო მონაცემების შენახვის, წვდომის, განხილვის, გამოყენების, კომუნიცირების და მათი განადგურების წესები; ისინი ინახებოდა სისხლის სამართლის საქმეში და მათზე წვდომა გააჩნდა ნებისმიერ პირს. ამდენად, აღნიშნული მონაცემები არასათანადოდ იყო დაცული, რაც პირის პირად ცხოვრებაში ან იურიდიული პირის კორესპონდენციაში არათანაზომიერი შეჭრის მაღალ რისკს წარმოშობდა.

ამასთან, მოქმედ საზედამხედველო სისტემას არ გააჩნდა უნარი, ეფექტიანად შეეფასებინა ჰქონდა თუ არა ადგილი უფლებამოსილების ბოროტად გამოყენებას. მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვის კომისიას გააჩნდა კომუნიკაციის სერვის პროვაიდერების მიერ მონაცემთა მოპოვებასთან დაკავშირებული ღონისძიებების შემოწმების უფლებამოსილება, მას არ შეეძლო იმ სახელმწიფო ორგანოთა ქმედებების შესწავლის შესაძლებლობა, რომლებსაც ასეთ მონაცემებზე ჰქონდათ წვდომა.

შესაბამისად, ევროპული სასამართლოს გადაწყვეტილებით, კომუნიკაციის მოსმენის შედეგად მიღებული მონაცემების შენახვასა და მათთან წვდომასთან დაკავშირებით ბულგარეთის მოქმედი კანონმდებლობა სრულად არ აკმაყოფილებდა „კანონის“ მოთხოვნას, რის გამოც იგი ვერ უზრუნველყოფდა რომ „ჩარევა“ ყოფილიყო „აუცილებელი დემოკრატიულ საზოგადოებაში.“ აღნიშნულიდან გამომდინარე, ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

5. დასკვნა

საქართველოს კონსტიტუციის მე-15 მუხლით დაცული ინდივიდის პირადი ცხოვრების უფლების ხელშეუხებლობის უზრუნველყოფა დემოკრატიული სახელმწიფოს ერთ-ერთი უმთავრესი ამოცანაა, რადგანაც სწორედ ის ქმნის ადამიანური ზრდისა და პიროვნებად ჩამოყალიბების ფუნდამენტს. ხსენებული უფლება არის ფარი, რომლის მეშვეობითაც მოქალაქეებს აქვთ შესაძლებლობა გამოხატონ საკუთარი აზრი, იყვნენ ინდივიდუალური და ჰქონდეთ განსხვავებული მოსაზრებები ნეგატიური შედეგების გარეშე, სწორედ ამიტომ სამართალდამცავი ორგანოების მიერ ჩატარებული საგამოძიებო, კერძოდ კი, ფარული საგამოძიებო მოქმედებები საჭიროებს დეტალურ კონტროლსა თუ სხვადასხვა სახის

საკანონმდებლო ბოჭვას, გამომდინარე აქედან გაძლიერდა და დაუკავშირდა პერსონალურ მონაცემთა დაცვის სამსახურის მანდატი დასავლურ გამოცდილებას.

აღნიშნულს ცხადყოფს, როგორც გამოქვეყნებული წლიური ანგარიშები თუ სტატისტიკები, ასევე, საგულისხმოა სტატიაში მიმოხილული საერთაშორისო ორგანიზაციების მიერ გაცემული რეკომენდაციების შესრულების მაღალი მაჩვენებელი, რაც პერსონალურ მონაცემთა დაცვის სამსახურს ეფექტურ ფარულ საგამოძიებო მოქმედებებზე საზედამხედველო მექანიზმად აქცევს.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 09/10/2009.
3. საპოლიციო სექტორში პერსონალურ მონაცემთა დამუშავების შესახებ ღირეექტივა.
4. იურიდიულ საკითხთა კომიტეტის დასკვნა „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“ საქართველოს კანონზე (№1614-VIIIმს-Хმპ, 7/06/2022) საქართველოს პრეზიდენტის მოტივირებული შენიშვნების თაობაზე (№07-1/14, 23/06/2022).
5. აუბარდია ი., კონტროლის მექანიზმები ფარულ საგამოძიებო მოქმედებებზე, სტატიათა კრებული - რევაზ გოგშელიძე 65, თბ., 2022, 200, 228.
6. ფაფიაშვილი ლ., თუმანიშვილი გ. და სხვები, საქართველოს სისხლის სამართლის საპროცესო კომენტარი (2015 წლის 1 ოქტომბრის მდგომარეობით), თბ., 2015, 428-429.
7. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის 2015 წლის ანგარიში, 34.
8. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 12 თვის საქმიანობის სტატისტიკა (იანვარი-დეკემბერი), 7, 9.
9. Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services, 2015, 8, <<https://rm.coe.int/1680487770>> [31.07.2024].
10. European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI)).
11. *Case of Roman Zakharov v. Russia*, (Application no. 47143/06).
12. *Case of Podchasov v. Russia*, Application no. 33696/19, 13 February 2024.

**პერსონალურ მონაცემთა დაცვა სამომხმარებლო ურთიერთობებში
(საერთაშორისო და ეროვნული სტანდარტების მიმოხილვა)**

თანამედროვე სავაჭრო ურთიერთობის განვითარების კვალდაკვალ აქტუალური ხდება სავაჭრო ურთიერთობის დახვეწის საჭიროება, აღნიშნული კი წარმოუდგენელია მომხმარებლის უფლებების დაცვის მაღალი სტანდარტის დანერგვის გარეშე, რადროსაც მომხმარებლის პერსონალური მონაცემების დამუშავების საჭიროება იკვეთება და რომლის საფუძველზეც ხორციელდება, როგორც მარკეტინგული ღონისძიებები, ასევე, ვლინდება სამომხმარებლო ხელშეკრულებით გათვალისწინებული უფლებები და ვალდებულებები.

სასიხარულოა, რომ სახელმწიფოს ზემოხსენებულ ორივე დარგში აქვს მიღებული ევროდირექტივებთან შესაბამისი ორი ახალი სპეციალური კანონი, ერთი მხრივ, 2022 წლის 1 ივნისის „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონი და მეორე მხრივ, 2023 წლის 14 ივნისის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.

სტატიამი განხილული იქნება სამომხმარებლო ურთიერთობების სამართლებრივი გარანტიები, რომელსაც ადგენს „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონი და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ასევე ის დირექტივები, რომელთა საფუძველზეც იმპლემენტირებულია აღნიშნული აქტები.

საკვანძო სიტყვები: მომხმარებელი, მოვაჭრე, პერსონალური მონაცემები, სამომხმარებლო ურთიერთობა, პერსონალური მონაცემების დაცვა.

1. შესავალი

თანამედროვე ეპოქაში, სადაც სავაჭრო ურთიერთობების განვითარება მზარდი ტემპით ხასიათდება, მეტად საჭირო ხდება სამართლებრივი რეგულაციების დახვეწა, ვინაიდან სწორედ სამართლებრივი რეგულაციები ქმნის იმის გარანტიას, რომ არსებული და სამომავლო გამოწვევები მყისიერად და შეუფერხებლად იქნეს დაძლეული.

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, სსიპ - საქართველოს კონკურენციისა და მომხმარებლის დაცვის სააგენტოს სასწავლო კვლევითი ცენტრის უფროსი.

სავაჭრო ურთიერთობების მოქნილობას ერთი მხრივ, დიდ წილად უზრუნველყოფს ტექნოლოგიური განვითარებები, ხოლო მეორე მხრივ, სამართლებრივი რეგულაციები, რომლებიც სავაჭრო ურთიერთობების მხარეებს ანიჭებს დაცულობის გარანტიას.

სავაჭრო ურთიერთობა, როგორც კერძოსამართლებრივი ურთიერთობა კომპლექსურობით ხასიათდება, აღნიშნული ურთიერთობის მხარეთა უფლებების დაცვას კი, სამართლის რამდენიმე დარგი უზრუნველყოფს, მათგან აღსანიშნავია, მომხმარებლის უფლებების დაცვა და სამომხმარებლო ურთიერთობაში პერსონალური მონაცემების დაცვის სტანდარტების ურთიერთმიმართება.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი¹ მიიღეს 2011 წელს, ხოლო „მომხმარებელთა უფლებების დაცვის შესახებ“ საქართველოს კანონი² ჯერ კიდევ 1996 წელს, რომელიც უზოგადეს სტანდარტებს აწესებდა. 2014 წლის 18 ივლისს საქართველომ ხელი მოაწერა ევროკავშირთან ასოცირების შეთანხმებას³ (შემდგომში - ასოცირების შეთანხმება), რომელიც სრულად ამოქმედდა 2016 წლის პირველი ივლისიდან, 2014 წლის 1 სექტემბრიდან, დაიწყო შეთანხმების ვაჭრობასთან დაკავშირებული დებულებების, მათ შორის, ევროკავშირთან ღრმა და ყოვლისმომცველი თავისუფალი სავაჭრო სივრცის შესახებ შეთანხმების (შემდგომში - „DCFTA“)⁴ ამოქმედება. საქართველომ აიღო ვალდებულება, რომ შეთანხმებით გათვალისწინებულ ვალდებულებებთან შესაბამისობაში მოეყვანა ეროვნული კანონმდებლობა. სწორედ ამ უწყვეტი პროცესის შედეგად, სამართლის ორივე დარგში ევროპული სტანდარტების სპეციალური კანონების ახალი რედაქციები შემუშავდა, რაც სამართლებრივი ურთიერთობების სუბიექტთა მაღალი დაცულობის მიღწევის მიზნით იყო გამოწვეული.

უდავოა, რომ ქვეყნის განვითარების მნიშვნელოვანი წილი სწორედ თავისუფალ სავაჭრო ურთიერთობებზე დგას, რასაც განამტკიცებს თავის მხრივ „DCFTA“,⁵ თანამედროვე სავაჭრო ურთიერთობები კი ხორციელდება დიდი მოცულობის ინფორმაციის გაცვლის/დამუშავების საფუძველზე, რაც უფრო მოქნილს ხდის ურთიერთობას.

თავის მხრივ, პერსონალური მონაცემების დაცვის კანონმდებლობაც ითვალისწინებს სავაჭრო ურთიერთობების დაცულობის მიზნით მონაცემების დამუშავების გარანტიებს,⁶ რაც ადასტურებს ამ ორი სფეროს გადაჯაჭვულობას.

2. მომხმარებლის უფლებების დაცვის სამართლებრივი გარანტიები

სამომხმარებლო ურთიერთობებს მნიშვნელოვანი დატვირთვა აქვს საზოგადოების ყოველდღიურ ცხოვრებაში, აღნიშნული განპირობებულია იმ საკითხებისა და ურთიერთობების არეალით, რასაც ეს სფერო მოიცავს. ამიტომაც,

¹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №5669-რს, 28/12/2011.

² საქართველოს კანონი „მომხმარებელთა უფლებების დაცვის შესახებ“, №151, 20/03/1996.

³ ასოცირების შესახებ შეთანხმება ერთი მხრივ, საქართველოსა და მეორე მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის <<https://matsne.gov.ge/ka/document/view/2496959?publication=4>> [29.07.2024].

⁴ თავისუფალი ვაჭრობა ევროკავშირთან, <<https://dcfta.gov.ge/ge/agreement>> [29.07.2024].

⁵ იქვე.

⁶ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მე-12 მუხლი.

მომხმარებელთა უფლებების დაცვა მნიშვნელოვანი, აქტუალური და ფუნდამენტურია განვითარებული სახელმწიფოებისთვის.

„მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონი საქართველოს პარლამენტმა 1996 წლის 20 მარტს მიიღო. აღნიშნული კანონი ძალადაკარგულად გამოცხადდა 2012 წლის 8 მაისს, ხოლო დღეს მოქმედი ახალი კანონი „მომხმარებლის უფლებების დაცვის შესახებ“ ძალაში შევიდა 2022 წლის 1 ივნისიდან.⁷

„მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს ახალი კანონი⁸ კი, შეესაბამება მრავალ ევროპულ დირექტივას,⁹ უახლეს დირექტივებთან დაახლოების პროცესი კი უწყვეტად მიმდინარეობს. ახალი კანონი განსაზღვრავს მომხმარებლის უფლებების დაცვის ზოგად პრინციპებს, რომელიც სამართლებრივ ურთიერთობას ამყარებს მოვაჭრესთან მისი საქონლის ან მომსახურების პირადი მოხმარების მიზნით გამოსაყენებლად¹⁰, ამ კანონით დაცული უფლებების და აკრძალული ქმედებებისგან, სტატიის მიზნებისთვის შეფასდება „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონის კანონის 24-ე მუხლი, რომლის თანახმადაც, უსამართლო კომერციული საქმიანობა აკრძალულია. უსამართლოა კომერციული საქმიანობა, რომელიც კეთილსინდისიერების მოთხოვნებს ეწინააღმდეგება და არსებითად უარყოფითად ცვლის ან შესაძლოა შეცვალოს საშუალო მომხმარებლის ეკონომიკური ქცევა იმ საქონელთან ან მომსახურებასთან მიმართებით, რომელიც მას მიაწოდეს ან მისთვის არის განკუთვნილი, ან ახდენს ან შესაძლოა მოახდინოს არსებითი უარყოფითი გავლენა მომხმარებელთა ჯგუფის საშუალო წევრის ეკონომიკურ ქცევაზე, როდესაც კომერციული საქმიანობის ადრესატი მომხმარებელთა განსაზღვრული ჯგუფია. უსამართლო კომერციულ საქმიანობად მიიჩნევა შეცდომაში შემყვანი კომერციული საქმიანობა ან აგრესიული კომერციული საქმიანობა. ამ კანონის 27-ე მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის მიხედვით, „ნებისმიერ შემთხვევაში უსამართლოდ მიიჩნევა და აკრძალულია

⁷ საქართველოს კანონი „მომხმარებლის უფლებების დაცვის შესახებ“, №1455-VIIIმს-Xმპ, 29/03/2022.

⁸ იქვე.

⁹ აღსანიშნავია:

- ევროპარლამენტისა და საბჭოს 2011 წლის 25 ოქტომბრის დირექტივა „მომხმარებლის უფლებების შესახებ“, რომელიც ცვლის საბჭოს 92/13 და ევროპარლამენტის 1999/44 დირექტივებს და ევროპარლამენტისა და საბჭოს 97/7 დირექტივას;
- 1998 წლის 16 თებერვლის ევროპარლამენტისა და საბჭოს 98/6/EC დირექტივა „მომხმარებელთა დაცვის შესახებ მომხმარებელთათვის შეთავაზებულ პროდუქტებზე ფასების მითითებისას“;
- 2005 წლის 11 მაისის ევროპარლამენტისა და საბჭოს 2005/29/EC დირექტივა „შიდა ბაზარზე კომპანიასა და მომხმარებელს შორის უსამართლო სავაჭრო პრაქტიკის შესახებ“ („დირექტივა უსამართლო სავაჭრო პრაქტიკის შესახებ“);
- ევროპარლამენტისა და საბჭოს 1999 წლის 25 მაისის დირექტივა 1999/44/EC „სამომხმარებლო საქონლის რეალიზაციის გარკვეული ასპექტებისა და მათთან დაკავშირებული გარანტიების შესახებ“;
- საბჭოს 1993 წლის 5 აპრილის დირექტივა 93/13/EEC „სამომხმარებლო ხელშეკრულებების უსამართლო პირობების შესახებ“;
- ევროპარლამენტისა და საბჭოს 2009 წლის 23 აპრილის დირექტივა 2009/22/EC „მომხმარებლის ინტერესების დამცავი ღონისძიებების შესახებ“;
- 2004 წლის 27 ოქტომბრის რეგულაცია „მომხმარებლის დაცვის შესახებ კანონების აღსრულებაზე პასუხისმგებელ ეროვნულ ორგანოებს შორის თანამშრომლობის შეახებ (რეგულაცია მომხმარებლის დაცვის სფეროში თანამშრომლობის შესახებ)“, რომელთან მიმართებითაც ეროვნული კანონმდებლობა უნდა დაახლოვდეს შემდეგ მუხლებთან: 3 (c); 4(3) – (7); 13 (3); 13(4).

¹⁰ საქართველოს კანონი „მომხმარებლის უფლებების დაცვის შესახებ“, №1455-VIIIმს-Xმპ, 29/03/2022, მე-2 მუხლის პირველი პუნქტი.

მომხმარებლისთვის სისტემატურად, ტელეფონით ან დისტანციური კომუნიკაციის სხვა საშუალებით არასასურველი შეთავაზებების გაკეთება, გარდა იმ შემთხვევისა, როდესაც ეს აუცილებელია ხელშეკრულებით გათვალისწინებული ვალდებულების შესასრულებლად“.

აღსანიშნავია, რომ 24-ე და 27-ე მუხლებით გათვალისწინებული ქმედება, რომ მიჩნეულ იქნეს „მომხმარებლის უფლებების დაცვის შესახებ“ კანონთან შეუსაბამოდ, უნდა არსებობდეს რამდენიმე პირობა, კერძოდ, სადავო ქმედება უნდა წარმოადგენდეს მოვაჭრის ქმედებას, რომელიც აზიანებს მომხმარებელთა ფართო წრის საერთო ინტერესს და ქმედება უნდა იყოს კანონსაწინააღმდეგო.

ზემოაღნიშნული აკრძალვის საფუძველი კი ის გარემოებაა, რომ პირდაპირი მარკეტინგი, რომელიც რეკლამის შინაარს ატარებს და მიზნად ისახავს საქონლის/მომსახურების გაყიდვას ან წახალისებას და ადრესატის ეკონომიკურ ქცევაზე გავლენის მოხდენას, არის ძალისხმევა - მოახდინოს გავლენა მომხმარებელზე, წახალისოს ის თავისი ფინანსური რესურსი მიმართოს საქონლისა თუ მომსახურების შესაძენად.

გასათვალისწინებელია, რომ რეკლამას გააჩნია ორი არსებითი მახასიათებელი: ინფორმაცია უნდა იყოს დაკავშირებული ადრესატის ეკონომიკურ, კომერციულ, ფინანსურ ან პროფესიულ საქმიანობასთან და მიწოდებული ინფორმაციით უნდა ხდებოდეს საქონლის შეძენის ან გამოყენების წახალისება.¹¹ შესაბამისად, ზემოთ ნახსენები დარღვევა საკმაოდ მძიმეა, აღნიშნულს აგრეთვე ითვალისწინებს ევროპარლამენტისა და საბჭოს 2005/29/EC „არაკეთილსინდისიერი კომერციული პრაქტიკის შესახებ“¹² დირექტივა.

ცალსახაა, რომ 27-ე მუხლის პირველი პუნქტის „გ“ ქვეპუნქტით გათვალისწინებულ შეთავაზებას, მოვაჭრე ვერ გააკეთებს, თუკი არ დაამუშავებს მომხმარებელთა პერსონალურ მონაცემებს, რაც დაცულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-12 მუხლით და ითვალისწინებს პირდაპირი მარკეტინგის გზით მონაცემების დამუშავების გარანტიებს.

აღსანიშნავია, რომ ევროკავშირის პრინციპების თანახმად, სახელმწიფომ მომხმარებელი უნდა უზრუნველყოს მისი უფლებების დაცვისთვის მოქნილი და სწრაფი მექანიზმით. მომხმარებლის უფლებების დაცვა ეფექტური საკანონმდებლო მექანიზმის მეშვეობით, ხელს შეუწყობს მოქალაქეთა ეკონომიკური ინტერესების ეფექტიან დაცვას და მომხმარებლის დაინტერესებას, იცოდეს, საკუთარი უფლებები და მოითხოვოს უფლების დაცვა, სწორედ ამ მიზნით განსაზღვრა კანონმდებელმა კანონის ძირითად აღმასრულებელ ორგანოდ სსიპ - საქართველოს კონკურენციისა და მომხმარებლის დაცვის სააგენტო, რომელიც „მომხმარებლის უფლებების დაცვის შესახებ კანონის“ შესაძლო დარღვევის თაობაზე განცხადებას განიხილავს და გადაწყვეტილებას იღებს ერთი თვის ვადაში, საქმის სირთულის შემთხვევაში კი, 3 თვის ვადაში.¹³

¹¹ საქართველოს კონკურენციის ეროვნული სააგენტოს 2023 წლის 22 მარტის №04/141 გადაწყვეტილება, <https://gcca.gov.ge/uploads_script/user_rights/tmp/php8oEZGi.pdf> [29.07.2024].

¹² Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005, Annex 1, 26, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0029-20220528&qid=1673608274813>> [29.07.2024].

¹³ საქართველოს კონკურენციის ეროვნული სააგენტოს თავმჯდომარის №45 ბრძანება „საქმის შესწავლის წესის და პროცედურის დამტკიცების თაობაზე“, 29/09/2022, მე-7 მუხლის პირველი და მე-2 პუნქტები.

3. პერსონალური მონაცემების დაცვის სამართლებრივი გარანტიები

ვინაიდან პერსონალურ მონაცემთა დაცვის საკანონმდებლო ბაზის ჰარმონიზაცია და კონსოლიდაცია წარმოადგენს საქართველოს მიერ ევროპის კავშირთან ასოცირების შეთანხმებითა და ასოცირების დღის წესრიგით ნაკისრ ვალდებულებას, მისი შესრულების მიზნით, 2023 წელს მიიღეს „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი, რომელიც ეყრდნობა ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციას“, ევროპის საბჭოს 108-ე კონვენციას და მის დამატებით ოქმს, ასევე, ევროკავშირის 2008 წლის 27 ნოემბრის 2008/977/JHA ჩარჩო გადაწყვეტილებებს და ევროპის საბჭოს მინისტრთა კომიტეტის 1987 წლის 15 ნოემბრის №R(87)15 რეკომენდაციას. გარდა ამისა, „საქართველოს ევროკავშირში ინტეგრაციის საგზაო რუკის“ თანახმად, მონაცემთა დაცვის შესახებ საქართველოში მოქმედი კანონმდებლობის დაახლოება მონაცემთა დაცვის უახლეს ევროპულ სტანდარტებთან წარმოადგენს ერთ-ერთ მნიშვნელოვან მიმართულებას/სამომავლო გეგმას.¹⁴

„მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონის 24-ე და 27-ე მუხლების საპირწონედ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის წინა რედაქციის¹⁵ მე-8 მუხლი ითვალისწინებდა შემდეგ რეგულაციას: პირდაპირი მარკეტინგის მიზნებისათვის შესაძლებელი იყო დამუშავებულიყო საჯაროდ ხელმისაწვდომი წყაროებიდან მოპოვებული მონაცემები, რომლებიც შეგროვების მიზნის მიუხედავად, შესაძლო იყო მხოლოდ ყოფილიყო სახელი (სახელები), მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, ფაქსის ნომერი, ხოლო მონაცემთა სუბიექტის მიერ ამავე კანონით დადგენილი წესით გაცემული წერილობითი თანხმობის საფუძველზე კი პირდაპირი მარკეტინგის მიზნებისათვის შეიძლებოდა ნებისმიერი მონაცემის დამუშავება.

მონაცემთა სუბიექტს უფლება ჰქონდა, მონაცემთა დამმუშავებლისთვის ნებისმიერ დროს მოეთხოვა მის შესახებ მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის გამოყენების შეწყვეტა. თავის მხრივ, მონაცემთა დამმუშავებელი ვალდებული იყო შეეწყვიტა მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის დამუშავება ან/და უზრუნველყოფოდა უფლებამოსილი პირის მიერ მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის დამუშავების შეწყვეტა მონაცემთა სუბიექტის მოთხოვნის მიღებიდან არაუგვიანეს 10 სამუშაო დღისა.

მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის დამუშავებისას მონაცემთა დამმუშავებელი ვალდებული იყო შეეტყობინებინა მონაცემთა სუბიექტისთვის ზემოაღნიშნული უფლების შესახებ და უზრუნველყო, რომ მონაცემთა სუბიექტს ჰქონოდა შესაძლებლობა მონაცემთა პირდაპირი მარკეტინგული მიზნებისათვის დამუშავების შეწყვეტის მოთხოვნისა იმავე ფორმით, რა ფორმითაც ხორციელდებოდა პირდაპირი მარკეტინგი, ან/და განესაზღვრა ხელმისაწვდომი და ადეკვატური საშუალება მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის დამუშავების შეწყვეტის მოთხოვნისთვის.

ახალი კანონის მე-12 მუხლში კანონმდებელმა პირდაპირი მარკეტინგის მიზნებისთვის პერსონალური მონაცემების დამუშავების უფრო მაღალი სტანდარტი გაითვალისწინა, მიუხედავად მონაცემთა შეგროვების/მოპოვების საფუძვლისა და

¹⁴ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-XXმპ, 14/06/2023.

¹⁵ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №5669-რს, 28/12/2011.

მათი ხელმისაწვდომობისა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება შეიძლება მხოლოდ მონაცემთა სუბიექტის თანხმობით, მონაცემთა სუბიექტის თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა მონაცემთა სუბიექტს ნათლად, მარტივ და მისთვის გასაგებ ენაზე უნდა განუმარტოს მის მიერ თანხმობის ნებისმიერ დროს გამოხმობის უფლება და ამ უფლების განხორციელების მექანიზმი/წესი, ამასთან წინა რეაქციით გათვალისწინებული იყო მონაცემთა სუბიექტის უფლება, განეცხადებინა მონაცემთა დამუშავებისთვის მონაცემთა დამუშავების შეწყვეტის მოთხოვნა და დამუშავებელსაც შეეწყვიტა მონაცემთა დამუშავება არაუმეტეს 10 დღეში შემცირდა არაუმეტეს 7 დღემდე ვადით.¹⁶

4. სავაჭრო ურთიერთობაში პერსონალური მონაცემების დაცვის პრაქტიკული ასპექტები

მიუხედავად მათი განსხვავებული კონსტიტუციური საფუძვლებისა,¹⁷ მომხმარებლის უფლებების დაცვისა და პერსონალური მონაცემების დაცვის სამართალი დაუახლოვდა ერთმანეთს ევროპულ კანონმდებლობასთან ჰარმონიზაციისას.¹⁸ თანამედროვე სავაჭრო ურთიერთობები დიგიტალიზებულია, რაც თავისთავად პერსონალური მონაცემების გაცვლის საფუძველზე ხორციელდება, დისტანციური ვაჭრობის რეგულირება, „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონის დამსახურებაა, ვინაიდან სწორედ აღნიშნული სავაჭრო ურთიერთობა ხდის, ერთი მხრივ, მომხმარებელს მოწყვლადს, მეორე მხრივ კი კომფორტს უქმნის, რომ სავაჭრო ურთიერთობები გახადოს უფრო მობილური, ნაკლები დროის, ადამიანური და ფინანსური რესურსის გარეშე შეიძინოს საქონელი და მომსახურება.

დისტანციური ვაჭრობისას, მომხმარებელი/მონაცემთა სუბიექტი ვალდებულია მოვაჭრეს გადასცეს რიგი ინფორმაცია, მათ შორის ზოგ შემთხვევაში მოვაჭრის ვებგვერდზე გაიაროს რეგისტრაცია, გააზიაროს ელექტრონული ფოსტის, პაროლის, სახელისა და გვარის, საბანკო ბარათის, საცხოვრებელი მისამართის, ტელეფონის ნომრის შესახებ ინფორმაცია, წინააღმდეგ შემთხვევაში მის მიერ შესყიდულ საქონელსა თუ მომსახურებას ვერ მიიღებს. მოვაჭრეს კი, თავის მხრივ შეუძლია ამ ინფორმაციის გარდა დაამუშაოს ასევე მომხმარებლის მიერ ვებგვერდზე გატარებული დროისა და მოძიებული ინფორმაციის შესახებ მონაცემები, რაც შემდგომში მარკეტინგული შეთავაზებების მიზნით გამოყენებაში შეუწყობს ხელს. მონაცემების გაცვლის პროცესამდე კი ყველაზე მნიშვნელოვან ეტაპს წარმოადგენს მონაცემთა სუბიექტის/მომხმარებლის ინფორმირება.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 24-ე და 25-ე მუხლი, განამტკიცებს მონაცემთა სუბიექტის ინფორმირებულობის მექანიზმს, შესაბამისად ხაზს უსვამს მის მნიშვნელობას. 24-ე მუხლი ჩამოთვლის მონაცემთა სუბიექტისთვის დამუშავებისთვის პასუხისმგებელი პირის მიერ მისაწოდებელი

¹⁶ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მე-12 მუხლის პირველი პუნქტი.

¹⁷ EU Charter of Fundamental Rights, Art. 7, <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> [29.07.2024].

¹⁸ *Zuiderveen Borgesius F., Helberger N., Reyna A.*, Common Market Law Review, Volume 54, Issue 5, 2017.

ინფორმაციის ნუსხას, როდესაც მონაცემების დამუშავება უშუალოდ სუბიექტისგან ხდება, ხოლო 25-ე მუხლი - თუ მონაცემების შეგროვება უშუალოდ მისგან არ ხდება,¹⁹ აღნიშნული დებულებები თანხვედრაშია ევროპულ სტანდარტებთან, კერძოდ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“,²⁰ დიდ ყურადღებას უთმობს საკითხს, თუ რა სახით უნდა მოხდეს მომხმარებლების ინფორმირება ისე, რომ მათ შეძლონ ინფორმირებული გადაწყვეტილებების მიღება. ინფორმირებული თანხმობის პრინციპი არის პერსონალური მონაცემების კანონიერი დამუშავების ძირითადი სამართლებრივი საფუძველი. გარდა ამისა, ძირითადი რეგულაცია აწესებს ჩამონათვალს,²¹ რის შესახებაც მონაცემთა სუბიექტები უნდა იყვნენ ინფორმირებული, მათ შორის მონაცემების დამუშავების მიზნები და ყველა სხვა ინფორმაცია, რომელიც აუცილებელია პერსონალური მონაცემების დამუშავების სამართლიანობის უზრუნველსაყოფად. GDPR ასევე აღგენს სტანდარტს²² და პრინციპს ინფორმაციის მიწოდების ფორმასთან დაკავშირებით, კერძოდ, სუბიექტების ინფორმირება უნდა მოხდეს ლაკონიური, ადვილად გასაგები, მკაფიო და მარტივი ენით.

ინფორმირებულობის მაღალ სტანდარტს სავაჭრო/სამომხმარებლო ურთიერთობებში აღგენს „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონის მე-5, მე-6 და მე-10 მუხლებიც, აღნიშნული მუხლები ჩამოთვლის მისაწოდებელი ინფორმაციის ნუსხას, როგორც დისტანციური ვაჭრობისას, აგრეთვე, ადგილზე ვაჭრობისას, აღსანიშნავია, რომ დისტანციური ვაჭრობისას მომხმარებლისთვის ინფორმაციის მიწოდების სტანდარტი, როგორც ზემოთ აღინიშნა, უფრო მაღალია, ვინაიდან მომხმარებელმა საქონლის/მომსახურების შეძენამდე „ინფორმირებული არჩევანის“ ფარგლებში მიიღოს შესყიდვის შესახებ გადაწყვეტილება. საქონლის ან მომსახურების შეძენის შეთავაზების შემთხვევაში არსებით ინფორმაციად მიიჩნევა ინფორმაცია (თუ იგი ისედაც აშკარად არ გამომდინარეობს მისი შინაარსიდან) საქონლის ან მომსახურების არსებითი მახასიათებლების შესახებ, საქონლის ან მომსახურების და ინფორმაციის მატარებლის თავისებურებების გათვალისწინებით.²³

ძირითადი რეგულაციით დადგენილი სტანდარტის მსგავსად, „მომხმარებლის უფლებების დაცვის შესახებ“ კანონის მე-5 მუხლიც აღგენს ინფორმაციის მიწოდების მკაფიოობის სტანდარტს, კერძოდ: „ხელშეკრულების დადებამდე მოვაჭრე ვალდებულია მომხმარებელს საქართველოს სახელმწიფო ენაზე, მკაფიოდ და გასაგებად მიაწოდოს შემდეგი უტყუარი და სრული ინფორმაცია (თუ ეს ინფორმაცია თავისთავად ცხადი არ არის)...“.

აღნიშნული სტანდარტი, რა თქმა უნდა შესაბამისობაშია ევროპარლამენტისა და საბჭოს 2011 წლის 25 ოქტომბრის 2011/83/EC (შემდგომში - 2011/83/EC)²⁴

¹⁹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023.

²⁰ ევროპარლამენტისა და საბჭოს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, 27/04/2016, მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი <<https://gdpr-info.eu/>> [29.07.2024].

²¹ იქვე, მე-14 მუხლი.

²² იქვე.

²³ საქართველოს კონკურენციისა და მომხმარებლის დაცვის სააგენტოს 2024 წლის 11 ივლისის №04/612 გადაწყვეტილება, <https://gcca.gov.ge/uploads_script/user_rights/tmp/phpwMZgnd.pdf> [29.07.2024].

²⁴ მომხმარებელთა უფლებების, საბჭოს დირექტივასა 93/13/EEC და ევროპარლამენტისა და საბჭოს დირექტივაში 1999/44/EC შესწორებების შეტანის და საბჭოს დირექტივისა 85/577/EEC და

დირექტივასთან, რომლის მიზანია მომხმარებელთა დაცვის მაღალი დონის მიღწევის გზით, შიდა ბაზრის გამართულად ფუნქციონირების ხელშეწყობა, მომხმარებლებსა და მოვაჭრეებს შორის დადებულ ხელშეკრულებებთან დაკავშირებული წევრ სახელმწიფოთა კანონმდებლობების, რეგულაციებისა და ადმინისტრაციული დებულებების გარკვეული ასპექტების დაახლოების გზით. 2011/83 დირექტივის მე-3 თავის მე-5 და მე-6 მუხლები შეიცავს ინფორმაციის იმ ჩამონათვალს, რომლის მიწოდებაც ევალება მოვაჭრეს მომხმარებლისთვის ხელშეკრულების დადებამდე. მე-5 მუხლით ძირითადად იმ ინფორმაციის ჩამონათვალია შემოთავაზებული, რომელიც მომხმარებელს უნდა მიეწოდოს ქუჩაში დადებული და დისტანციური ხელშეკრულებების გარდა ყველა სხვა ხელშეკრულების შემთხვევაში. 2011/83 დირექტივის მე-6 მუხლის მე-9 პუნქტის მიხედვით, მომხმარებლისთვის ინფორმაციის მიწოდებასთან დაკავშირებული მტკიცების ტვირთი მთლიანად მოვაჭრეს ეკისრება. შესაბამისად, მხარეთა შორის დაცვის წარმოშობის შემთხვევაში, სწორედ მოვაჭრემ უნდა ამტკიცოს, რომ მან დირექტივით მასზე დაკისრებული ვალდებულება სრულად შეასრულა და მომხმარებლის ინფორმირება სათანადო დონეზე მოახდინა.

სამომხმარებლო ურთიერთობებში პერსონალური მონაცემების დამუშავების კანონიერების მნიშვნელობაზე მსჯელობისას აუცილებელია პრაქტიკული ნიმუშის განხილვაც, რისი მაგალითიცაა საქართველოს კონკურენციის ეროვნული სააგენტოს პრაქტიკა. სააგენტომ ერთ-ერთი საქმის²⁵ შესწავლის ფარგლებში კომპლექსურად იმსჯელა მოვაჭრის მხრიდან „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონის 24-ე და 27-ე მუხლების შესაძლო დარღვევის ფაქტზე, სადაც მომხმარებელი მიუთითებდა, რომ გამუდმებით იღებდა სარეკლამო შინაარსის მოკლე ტექსტურ შეტყობინებებს და შეტყობინებების გამორთვის ყველა მცდელობა იყო უშედეგო. განმცხადებლის განმარტებით, მსგავსი სახის აგრესიული კომერციული საქმიანობა ზიანს აყენებდა არა მხოლოდ მას, არამედ სხვა მომხმარებლების ინტერესსაც.

სააგენტომ აგრეთვე შეისწავლა ევროპარლამენტისა და საბჭოს 2005/29/EC „არაკეთილსინდისიერი კომერციული პრაქტიკის შესახებ“ დირექტივა²⁶, რომლის თანახმადაც, აგრესიულ კომერციულ პრაქტიკად მიჩნეულია ტელეფონით, ფაქსით, ელექტრონული ფოსტით ან სხვა დისტანციური საშუალებით დაჟინებული და არასასურველი რეკლამა, გარდა ეროვნული კანონმდებლობით გათვალისწინებული გარემოებებისა. როგორც კანონის 27-ე მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის თანახმად, ასევე ევროპარლამენტისა და საბჭოს 2005/29/EC „არაკეთილსინდისიერი კომერციული პრაქტიკის შესახებ“ დირექტივის თანახმად, სისტემატურ ხასიათად მიიჩნევა ისეთი სიხშირით მოკლე ტექსტური შეტყობინებების გაგზავნა, რომელიც არის შემაწუხებელი და დამღლელი. გარდა ამისა, სააგენტომ მიიჩნია, რომ გაგზავნილი მარკეტინგული შინაარსის მოკლე ტექსტური შეტყობინება უნდა ყოფილიყო დაკავშირებული ადრესატის ეკონომიკურ, კომერციულ, ფინანსურ ან პროფესიულ საქმიანობასთან და მიწოდებული ინფორმაციით უნდა მომხდარიყო

ევროპარლამენტისა და საბჭოს დირექტივის 97/7/EC გაუქმების შესახებ, <<https://matsne.gov.ge/ka/document/view/4488461?publication=0>> [29.07.2024].

²⁵ საქართველოს კონკურენციის ეროვნული სააგენტოს 2023 წლის 22 მარტის №04/141 გადაწყვეტილება, <https://gcca.gov.ge/uploads_script/user_rights/tmp/php8oEZGi.pdf> [29.07.2024].

²⁶ Directive 2005/29/EC of the European Parliament and of the COUNCIL of 11 May 2005, Annex 1, 26, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0029-20220528&qid=1673608274813>> [29.07.2024].

საქონლის/მომსახურების შეძენის ან გამოყენების წახალისება. განსახილველ შემთხვევაში, მოვაჭრის მიერ გაგზავნილი მოკლე ტექსტური შეტყობინებების პერიოდულობისა და შინაარსის გათვალისწინებით, სააგენტომ მიიჩნია, რომ მათ არ გააჩნდათ სისტემური ხასიათი, ამასთან მოვაჭრის მიერ მოწოდებული მტკიცებულებების თანახმად, მომხმარებელს/მონაცემთა სუბიექტს გაცხადებული ჰქონდა თანხმობა ინფორმაციის მიღებაზე, მასთან მოვაჭრის მიერ გაგზავნილ ყველა მარკეტინგულ შეთავაზებას გააჩნდა შეტყობინების გათიშვის საშუალებაზე მითითება, ხოლო მომხმარებელს აღნიშნული საშუალება გამოყენებული არ ჰქონდა, შესაბამისად, სააგენტომ საქმის შესწავლის შედეგად „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონის დარღვევა არ დაადგინა.

5. დასკვნა

სტატიაში განხილული სამართლებრივი ასპექტების საფუძველზე, შესაძლოა ითქვას, რომ ამ ორი სხვადასხვა დარგის საკანონმდებლო რეგულირება ავსებს ერთმანეთს და უზრუნველყოფს ფიზიკური პირის დაცულობას. „მომხმარებლის უფლებების დაცვის შესახებ“ საქართველოს კანონმა, რომელიც 2 წელია მოქმედებს, წარმატებით დაადგინა მაღალი სტანდარტი სავაჭრო სფეროში და „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალ კანონთან ერთად ქმნის მომხმარებლის/მონაცემთა სუბიექტის უფლებების დაცვის ევროპული სტანდარტის ანალოგს, რომელიც ევროკავშირის წევრი ქვეყნების უმრავლესობაში ათეულობით წელია რაც მოქმედებს.

ბიბლიოგრაფია:

1. ასოცირების შესახებ შეთანხმება ერთი მხრივ, საქართველოსა და მეორე მხრივ, ევროკავშირის და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის, 27/06/2014, <<https://matsne.gov.ge/ka/document/view/2496959?publication=4>> [29.07.2024].
2. ევროპარლამენტისა და საბჭოს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, 27/04/2016, <<https://gdpr-info.eu/>> [29.07.2024].
3. მომხმარებელთა უფლებების, საბჭოს დირექტივასა 93/13/EEC და ევროპარლამენტისა და საბჭოს დირექტივაში 1999/44/EC შესწორებების შეტანის და საბჭოს დირექტივისა 85/577/EEC და ევროპარლამენტისა და საბჭოს დირექტივის 97/7/EC გაუქმების შესახებ, <<https://matsne.gov.ge/ka/document/view/4488461?publication=0>> [29.07.2024].
4. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №5669-რს, 28/12/2011.
5. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023.
6. საქართველოს კანონი „მომხმარებელთა უფლებების დაცვის შესახებ“, №151, 20/03/1996.

7. საქართველოს კანონი „მომხმარებლის უფლებების დაცვის შესახებ“, №1455-VIIIმს-Xმპ, 29/03/2022.
8. საქართველოს კონკურენციის ეროვნული სააგენტოს თავმჯდომარის №45 ბრძანება „საქმის შესწავლის წესის და პროცედურის დამტკიცების თაობაზე“, 29/09/2022.
9. საქართველოს კონკურენციის ეროვნული სააგენტოს 2023 წლის 22 მარტის №04/141 გადაწყვეტილება, <https://gcca.gov.ge/uploads_script/user_rights/tmp/php8oEZGi.pdf> [29.07.2024].
10. საქართველოს კონკურენციისა და მომხმარებლის დაცვის სააგენტოს 2024 წლის 11 ივლისის №04/612 გადაწყვეტილება, <https://gcca.gov.ge/uploads_script/user_rights/tmp/phpwMZgnd.pdf> [29.07.2024].
11. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005, Annex 1, 26, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0029-20220528&qid=1673608274813>> [29.07.2024].
12. EU Charter of Fundamental Rights, <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> [29.07.2024].
13. *Zuiderveen Borgesius F., Helberger N., Reyna A.*, Common Market Law Review, Volume 54, Issue 5, 2017.
14. <<https://dcfta.gov.ge/ge/agreement>> [29.07.2024].

ნორბერტ ბერნსდორფი*

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი საქართველოში - მოკლე მიმოხილვა**

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ („GDPR“) წარმოადგენს მონაცემთა დაცვის მთავარ მარეგულირებელ კანონს ევროპაში, რომელმაც ჩაანაცვლა ადრე მოქმედი მონაცემთა დაცვის დირექტივა (95/46/EC). ამგვარად, „GDPR“ ევროკავშირის თითოეული მოქალაქისთვის ქმნის მონაცემთა დაცვის ერთგვაროვან სტანდარტს.

მიუხედავად იმისა, რომ „GDPR“ ავტომატურად ინტეგრირდება საქართველოს საკანონმდებლო სისტემაში, როდესაც ქვეყანა ევროკავშირის წევრი გახდება, საქართველოს მონაცემთა დაცვის კანონმდებლობა მაინც უნდა შეესაბამებოდეს მას. საქართველოს ევროკავშირში გაწევრიანებისთანავე, „მონაცემთა დაცვის ძირითადი რეგულაციის“ ყველა დებულება ამოქმედდება. იქიდან გამომდინარე, რომ „GDPR“-ის გამოყენება პრიორიტეტულია საქართველოს კანონთან შედარებით, ეს უკანასკნელი გავრცელდება მხოლოდ იმ საკითხებზე, რომლებსაც „GDPR“ არ დაარეგულირებს.

„პერსონალური მონაცემების დაცვის შესახებ“ კანონის მიღებით საქართველოს საკანონმდებლო ორგანო თანამედროვე გამოწვევებს გამოეხმაურა, რომლის ძირითადი ნაწილი 2024 წლიდან შევიდა ძალაში და სრულად ანაცვლებს წინამორბედ კანონს.

ვის ან რას იცავს ახალი კანონი?

უპირველეს ყოვლისა, მონაცემთა დაცვის ახალი კანონი იცავს პერსონალურ მონაცემებს. კანონის მე-3 მუხლის „ა“ ქვეპუნქტის თანახმად, პერსონალური მონაცემები არის ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. ამ თვალსაზრისით, კანონი იცავს პერსონალურ მონაცემებს, რომლებიც იძლევა გარკვეული დასკვნების გაკეთების საშუალებას პირის შესახებ.

როგორია „პერსონალური მონაცემების დაცვის შესახებ კანონის შინაარსი“?

საქართველოს ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ეხება:

- მონაცემთა დამუშავების საფუძვლებს (მე-4 და შემდგომი მუხლები);
- მონაცემთა სუბიექტის უფლებებს (მე-13 და შემდგომი მუხლები);
- დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვალდებულებებს (23-ე და შემდგომი მუხლები);
- პასუხისმგებლობისა და სანქციების საკითხებს (58-ე და შემდგომი მუხლები, 64-ე და შემდგომი მუხლები);
- კანონის მოქმედების სფეროს, ტერმინთა განმარტებას და მონაცემთა დამუშავების პრინციპებს (მე-2 მუხლი, მე-3 და შემდგომი მუხლები);

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, წინამდებარე ჟურნალის სარედაქციო კოლეგიის წევრი.

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

- პერსონალურ მონაცემთა დაცვის ოფიცერს (33-ე მუხლი);
- პერსონალურ მონაცემთა დაცვის სამსახურის სტატუსს და საქმიანობის პრინციპებს (39-ე და შემდგომი მუხლები);
- სამართლებრივი დაცვის საშუალებებს (63-ე მუხლი);
- მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემას (37-ე და 38-ე მუხლი) და ა.შ.

საქართველოს ახალი კანონი „პერსონალურ მონაცემების დაცვის შესახებ“ ცხადყოფს, რომ კანონმდებელმა ინტენსიურად იფიქრა და ყურადღებით გააანალიზა ევროკავშირის მონაცემთა დაცვის კანონმდებლობა, რისთვისაც იმსახურებს გულწრფელ მილოცვას! საქართველომ ახალი კანონის მეშვეობით უკვე დიდწილად შეუსაბამა მონაცემთა დაცვის ეროვნული კანონი “GDPR“-ის სტანდარტებს.

დამატებით უნდა აღინიშნოს:

საქართველოს მონაცემთა დაცვის ახალი კანონის 33-ე მუხლის მოთხოვნები, რომლებიც შეეხება მონაცემთა დაცვის ოფიცერების საქმიანობას, ძალიან ვრცელი და ბევრად უფრო დეტალურია, ვიდრე, მაგალითად, გერმანიის მონაცემთა დაცვის კანონი. მიუხედავად იმისა, რომ კანონით შესაძლებელი იყო სასამართლოების მიერ მონაცემთა დაცვის ოფიცერის დანიშვნის ვალდებულებისგან გათავისუფლება, აღნიშნული გარკვეულწილად უკვე განხორციელდა კანონის მოქმედების შესახებ დებულების მე-2 მუხლის მე-2 პუნქტში.

საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“ მრავლად შეიცავს მესამე ქვეყნებსა და საერთაშორისო ორგანიზაციებში მონაცემთა გადაცემის მოწესრიგებას (37-ე და შემდგომი მუხლები). თუ საქართველო ევროკავშირის წევრი გახდება, “GDPR“-ის 45-ე მუხლი ავტომატურად ამოქმედდება: ევროკომისიამ უნდა დაუშვას მონაცემთა გადაცემა შესაბამისობის გადაწყვეტილების საფუძველზე, თუმცა წევრ სახელმწიფოს შეუძლია გაასაჩივროს ეს გადაწყვეტილება სასამართლოში. აღნიშნულის შესახებ ნათქვამია ევროკავშირის მართლმსაჯულების სასამართლოს 2015 წლის გადაწყვეტილებაში - „უსაფრთხო ნავსადგომი“ (C-362/14). ამის შემდეგ საქართველოს შეეძლება საკითხის დარეგულირება მონაცემთა დაცვის ეროვნული კანონმდებლობით.



პერსონალურ მონაცემთა
დაცვის სამსახური

© პერსონალურ მონაცემთა დაცვის სამსახური, 2024

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის №7, 0105

ბათუმი, ბაქოს ქუჩა, №48, 6010

www.personaldata.ge

ტელ.: (+995 32) 242 1000

E-mail: office@pdps.ge

