პერსონალურ მონაცემთა
დაცვის სამსახური

არასრულწლოვანთა პერსონალურ მონაცემთა დაცვა-

თეორია და პრაქტიკა

პერსონალურ მონაცემთა
დაცვის სამსახური

არასრულწლოვანთა პერსონალურ მონაცემთა დაცვა - თეორია და პრაქტიკა

გამოცემა შემუშავებულია პერსონალურ მონაცემთა დაცვის სამსახურის გეგმური ინსპექტირების დეპარტამენტისა და საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის მიერ.

სარჩევი

გაეროს „ბავშვთა უფლებების კონვენციის თანახმად“, სხვა ფუნდამენტურ უფლებებთან ერთად, ბავშვს აქვს პირადი ცხოვრების ხელშეუხებლობის უფლება. სახელმწიფო ვალდებულია, მიიღოს ყველა აუცილებელი საკანონმდებლო, ადმინისტრაციული და სხვაგვარი ზომა, რათა შექმნას პირობები ბავშვთა უფლებების განხორციელების და დაცვისათვის.

ბავშვთა და მოზარდთა პერსონალური მონაცემები განსაკუთრებულ დაცვას საჭიროებს. „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მე-7 მუხლი არასრულწლოვნის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესსა და პირობებს განიხილავს[1], შესაბამისად, კანონი აღიარებს და პატივს სცემს ბავშვისა და მოზარდის ძირითად უფლებებსა და მათ საუკეთესო ინტერესებს.

ოცდამეერთე საუკუნეში ციფრული გარემოს საფრთხეები, რომლებსაც შეუძლიათ, გავლენა მოახდინონ არასრულწლოვნების განვითარებაზე, დღითიდღე იზრდება. ციფრულ ეპოქაში ბავშვების კონფიდენციალურობის უფლება მაღალი სტანდარტით დაცვას საჭიროებს. კომუნიკაციის ახალი ფორმების განვითარების თანმდევად, მნიშვნელოვანია, გაუმჯობესდეს ძირითად უფლებათა დაცვის სტანდარტი. ამასთან, რისკების შესახებ ინფორმირებულობა მონაცემთა უკანონო დამუშავების პრევენციისა და ამ კუთხით ცნობიერების ამაღლების ერთ-ერთი მნიშვნელოვანი მიმართულებაა. ამ მიზნით, პერსონალურ მონაცემთა დაცვის სამსახურმა შეიმუშავა არასრულწლოვანთა პერსონალურ მონაცემთა დაცვის გზამკვლევი (მისი პრაქტიკული და თეორიული ასპექტები).

გზამკვლევში განხილულია არასრულწლოვნის პერსონალური მონაცემების დამუშავების ცალკეული საკითხები: კერძოდ, მონაცემთა დამუშავების საფუძვლები; მონაცემთა დამუშავების პრინციპები; არასრულწლოვნის, როგორც მონაცემთა სუბიექტის უფლებები და მათი განხორციელება — ინფორმაციის მიღების უფლება, ინფორმაციის მოთხოვნის, მონაცემთა გასწორების, განახლების, დამატების მოთხოვნის, მონაცემთა დაბლოკვის, წაშლისა და განადგურების, თანხმობის გამოხმობის, მონაცემთა გადატანის უფლება და სხვა; ცალკეულ საკითხებზე პერსონალურ მონაცემთა დაცვის სამსახურის გამოცდილება, საერთაშორისო და ეროვნული საკანონმდებლო ჩარჩო — არასრულწლოვანთა მონაცემების დამუშავების საერთაშორისო სამართლებრივი ინსტრუმენტები და პრაქტიკა, კერძოდ, არასრულწლოვანთა პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვა

[1] კანონი ამოქმედდება 2024 წლის პირველი მარტიდან, ხოლო დებულებები მონაცემთა დაცვაზე ზეგავლენის შეფასების (მუხლი 31), მონაცემთა დაცვის ოფიცრის შესახებ (მუხლი 32), 2024 წლის პირველი ივნისიდან.

გაერთიანებული ერების სამართლებრივ სისტემაში, ევროპის საბჭოს სამართლებრივი ჩარჩო არასრულწლოვანთა პერსონალური მონაცემების დაცვის შესახებ, ადამიანის უფლებათა ევროპული სასამართლოს სტანდარტი და ა. შ.

გაწეული შრომისთვის განსაკუთრებული მადლობა მინდა გადავუხადო პერსონალურ მონაცემთა დაცვის სამსახურის გეგმური ინსპექტირების დეპარტამენტის უფროსს - სოფიო შამუგიას და საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული დეპარტამენტის უფროსს - ანა თოხაძეს, აღნიშნული დეპარტამენტების თითოეულ თანამშრომელს.

ვფიქრობ, გზამკვლევი ხელს შეუწყობს პერსონალურ მონაცემთა ქართული სამართლისა და მონაცემთა დაცვის კულტურის განვითარებას, რაც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს საქმიანობის ერთ-ერთ მთავარ მიმართულებას წარმოადგენს.

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი,

ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი,

ბარსელონის ავტონომიური უნივერსიტეტის მოწვეული პროფესორი,

ლელა ჯანაშვილი

შესავალი

თანამედროვე ციფრულმა ტექნოლოგიებმა მკვეთრად შეცვალა მსოფლიო. არასრულწლოვნები სულ უფრო აქტიურად იყენებენ ციფრულ სივრცეს, რომელიც მათი ცხოვრების განუყოფელი ნაწილი ხდება, რაც წარმოშობს გარკვეულ რისკებს ბავშვების პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის თვალსაზრისით. პერსონალურ მონაცემთა დაცვის სფეროში საქართველოში მოქმედი სამართლებრივი ჩარჩო პირდაპირ არ ითვალისწინებს ციფრულ გარემოში ბავშვების პერსონალურ მონაცემთა დაცვის პროცედურებს. აქედან გამომდინარე, შესაბამისი გარანტიების შექმნისთვის მნიშვნელოვანია საერთაშორისო სტანდარტების გათვალისწინება.

ნაშრომის მიზანია ციფრულ გარემოში, და არამხოლოდ, არასრულწლოვანთა უფლებებთან დაკავშირებით საუკეთესო საერთაშორისო სტანდარტების შესწავლა და ეროვნულ კანონმდებლობასთან მისადაგება. ნაშრომში ყურადღება გამახვილებულია მონაცემთა დამუშავების პრინციპებსა და საფუძვლებზე, ბავშვის პერსონალურ მონაცემთა დაცვის უფლებებზე, „ბავშვის საუკეთესო ინტერესის“ ცნებასთან დაკავშირებულ ცალკეულ მახასიათებლებზე. პერსონალურ მონაცემთა დაცვის სამსახურის პრიორიტეტულ მიმართულებას არასრულწლოვანთა პერსონალური მონაცემების დამუშავების კანონიერების შესწავლა და გამოვლენილი გამოწვევების საპასუხოდ, შესაბამისი ღონისძიებების განხორციელება წარმოადგენს. ამდენად, აღსანიშნავია, რომ როგორც 2022 წლის, ასევე 2023 წლის „პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) გეგმის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2022 წლის 7 აპრილის №01/23 და 2023 წლის 31 იანვრის №01/20 ბრძანებების მიხედვით, სხვა მიზნობრივ ჯგუფებთან ერთად, განისაზღვრნენ არასრულწლოვნებიც. სამსახური მუდმივად ცდილობს ბავშვის უფლებათა დაცვის საუკეთესო საერთაშორისო პრაქტიკის გაზიარებასა და ეფექტიანი სტანდარტების დამკვიდრებას, რაც განსაკუთრებით აქტუალურია „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის იმპლემენტაციის პროცესში. წინამდებარე სახელმძღვანელოც არის ერთგვარი აკადემიური კონტრიბუცია, რომელიც ასახავს არასრულწლოვანთა მონაცემთა დამუშავების ფუნდამენტურ ასპექტებს და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მიღებულ მნიშვნელოვან გადაწყვეტილებებს.

დოკუმენტი სარეკომენდაციო ხასიათისაა, შესაბამისად, პერსონალურ მონაცემთა დაცვის სამსახური იტოვებს შესაძლებლობას, რომ, ცალკეულ საქმეთა ინდივიდუალური გარემოებების გათვალისწინებით, საკითხები ნაშრომში წარმოდგენილი მოსაზრებებისგან განსხვავებულად გადაწყვიტოს.

1. არასრულწლოვანი, როგორც მონაცემთა სუბიექტი და ეროვნული სამართლებრივი ჩარჩო

1.1. პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობა

პერსონალური მონაცემების დაცვის სამართალი ტექნოლოგიური პროგრესის კვალდაკვალ სწრაფად ვითარდება, სადაც აქტუალობას იძენს ადამიანის ინფორმაციული თვითგამორკვევის პროცესი. პერსონალური მონაცემების დაცვის შესახებ ინფორმირებულობა პიროვნების თავისუფალი განვითარების ნაწილია და იგი დაფუძნებულია საკუთარი ნების, გადაწყვეტილების, არჩევანის შესაბამისად განვითარების შესაძლებლობაზე. ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით „პერსონალური მონაცემები“ განიმარტება, როგორც იდენტიფიცირებული ან იდენტიფიცირებადი ინფორმაცია ფიზიკური პირის შესახებ, რომლის ვინაობა ცნობილია ან შეიძლება, დადგინდეს დამატებითი ინფორმაციის საფუძველზე.[2] ევროკავშირის კანონმდებლობით, ფიზიკური პირი მონაცემთა დაცვის წესების ერთადერთ ბენეფიციარს წარმოადგენს.[3] პერსონალურ მონაცემთა ცნების ძირითადი ასპექტებია: „ნებისმიერი ინფორმაცია“; „დაკავშირებული“; „იდენტიფიცირებული ან იდენტიფიცირებადი“; „ფიზიკური პირი“.[4] „ნებისმიერი ინფორმაცია“ ხაზს უსვამს კანონმდებლის სურვილს ფართო განმარტება მიეცეს პერსონალური მონაცემის ცნებას. ამასთან დაკავშირებით, გერმანიის საკონსტიტუციო სასამართლომ 1983 წელს განმარტა, რომ „მონაცემთა ავტომატური დამუშავების პირობებში, აღარ არსებობს უმნიშვნელო ინფორმაცია“.[5] ნებისმიერი ინფორმაცია, რომელიც დაკავშირებულია ინდივიდთან შესაძლოა, იყოს განსაკუთრებული კატეგორიის.[6] აქედან გამომდინარე, პერსონალური მონაცემები მოიცავს ნებისმიერ მონაცემს, იმისგან დამოუკიდებლად იგი შეეხება პიროვნების პირად ცხოვრებას, სამუშაო, ეკონომიკურ თუ სოციალურ გარემოსა თუ მის შესაძლებლობებს.[7] ინფორმაცია შესაძლოა იყოს, როგორც „ობიექტური“, როგორიცაა მონაცემთა სუბიექტის უცვლელი მახასიათებლები, ასევე „სუბიექტური“, რომელიც აერთიანებს

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1-88 art. 4 (1) (შემდგომში - “GDPR”); 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).

[3] GDPR, Article 1.

[4] ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 96.

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

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

[7] WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007, 6.

მოსაზრებებსა და შეფასებებს.[8] არ არის აუცილებელი, რომ იგი იყოს ჭეშმარიტი, დადასტურებული ან სრული.[9] მნიშვნელოვანია, რომ ინფორმაცია უკავშირდებოდეს კონკრეტულ ინდივიდს. „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”)[10] წინამორბედი 29-ე მუხლის სამუშაო ჯგუფის[11] მოსაზრების თანახმად, „ინფორმაცია, მისი შინაარსის, მიზნის ან ეფექტის გამო, დაკავშირებული უნდა იყოს კონკრეტულ პირთან“[12]. 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.[13] აღსანიშნავია, რომ ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-8 მუხლის თანახმად,[14] მონაცემთა დაცვა საყოველთაო უფლებას წარმოადგენს და არ შემოიფარგლება ცალკეული ქვეყნის მოქალაქეებით[15].

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ პრეამბულა ითვალისწინებს არასრულწლოვანთა მონაცემების დამუშავების სპეციალურ მოწესრიგებას. არასრულწლოვნები სარგებლობენ პერსონალური მონაცემების დაცვის განსაკუთრებული უფლებით, რადგან მათთვის შეიძლება ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, სამართლებრივი დაცვის მექანიზმები და მათი უფლებები, რომლებიც უკავშირდება პერსონალური მონაცემების დამუშავებას.[16] განსაკუთრებული დაცვა უნდა შეეხოს არასრულწლოვნების პერსონალური მონაცემების გამოყენებას მარკეტინგის მიზნებისთვის, პიროვნების ან მომხმარებლის პროფილის შექმნასა და არასრულწლოვნებთან დაკავშირებული პერსონალური მონაცემების შეგროვებას ისეთი მომსახურების გამოყენების დროს, რომლის შეთავაზებაც არასრულწლოვნისთვის პირდაპირ ხდება. აღსანიშნავია, რომ მშობლის ან არასრულწლოვნის კანონიერი წარმომადგენლის თანხმობა არ არის საჭირო

[8] იქვე, “especially the latter type of information constitutes a significant part of the processing in sectors such as banking, insurances or employment”.

[9] იქვე.

[10] The European Data Protection Board (EDPB) is established under Article 68 of the GDPR as an independent EU body which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU’s data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

[11] WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007, 10 ff <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>, [18.08.2023].

[12] CJEU, Nowak, 20 December 2017, margin number 35.

[13] General Data Protection Regulation, GDPR, Recital 14 sentence 1.

[14] კონვენცია ბავშვის უფლებების შესახებ, საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება, 1948, მუხლი 8.

[15] General Data Protection Regulation, GDPR, Recital 14.

[16] General Data Protection Regulation, GDPR, Recital 38.

არასრულწლოვნებისთვის პრევენციული ან საკონსულტაციო მომსახურების პირდაპირ შეთავაზების შემთხვევაში.[17] არასრულწლოვნები წარმოადგენენ მოწყვლად ჯგუფს, სადაც მიზანშეწონილია დადგინდეს მათი უფლებების დაცვის კიდევ უფრო მაღალი სტანდარტი. გარდა ამისა, „მონაცემთა დაცვის ძირითადი რეგულაციის“ მიხედვით, არასრულწლოვანთა განსაკუთრებული დაცვის საჭიროებიდან გამომდინარე, ნებისმიერი ინფორმაცია, რომელიც მისთვის არის განკუთვნილი, უნდა იყოს ნათლად, მარტივად და გასაგებად გადმოცემული, რაც უკავშირდება სამართლიანობისა და კანონიერების პრინციპს იმდენად, რამდენადაც მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად[18]. ამასთან დაკავშირებით, აღსანიშნავია, რომ 2013 წელს, „ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ“ (“OECD”) დაამტკიცა პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, რომელშიც ასევე, ხაზგასმულია, რომ ბავშვების სპეციალური და განსაკუთრებული მდგომარეობიდან გამომდინარე, სახელმწიფოების როლი, მიაწოდონ მათ ამომწურავი ინფორმაცია, რათა დაცულები იყვნენ ონლაინ სივრცეში და ინტერნეტი გამოიყენონ სარგებლის მისაღებად, განსაკუთრებით მნიშვნელოვანია.[19]

პერსონალურ მონაცემთა დაცვის ეროვნული საკანონმდებლო მოწესრიგება იზიარებს პერსონალურ მონაცემთა ცნების საერთაშორისოსამართლებრივ დეფინიციას. პერსონალურ მონაცემთა დაცვის ქართული მოდელი ევროპული ანალოგის მსგავსია, სადაც შიდასახელმწიფოებრივი და საერთაშორისო რეგულაციები ითვალისწინებენ ყველა სექტორზე - კერძო, საჯარო სექტორებსა და სამართალდამცავი ორგანოების მიმართ კანონის ფუნქციონირებას. საქართველოში პერსონალურ მონაცემთა დაცვა წესრიგდება ერთიანი საკანონმდებლო სამართლებრივი აქტით — „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, რომელიც 2011 წლის 28 დეკემბერს იქნა მიღებული (პირველი რედაქცია).[20] პერსონალურ მონაცემთა დაცვის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოების, საქართველოს მიერ საერთაშორისო ვალდებულებების შესრულებისა და საერთაშორისოდ აღიარებული პრინციპების დამკვიდრების, აგრეთვე, საჯარო და კერძო დაწესებულებებსა და სამართალდამცავ ორგანოებში არსებული გამოწვევების საპასუხოდ, 2023 წლის 14 ივნისს მიღებულ იქნა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი,[21] რომელიც ახლებურად განსაზღვრავს პერსონალური

[17] იქვე.

[18] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მე-4 მუხლის „ა“ ქვეპუნქტი, <https://matsne.gov.ge/ka/document/view/1561437?publication=31>, [10.08.2023].

[19] OECD Privacy Framework, 2013, 31.

[20] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011.

[21] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, <https://matsne.gov.ge/document/view/1561437?publication=30>, [10.08.2023].

მონაცემების დაცვის სამართლებრივ გარანტიებს, წესებს და სხვა საკითხებთან ერთად, არასრულწლოვანთა პერსონალური მონაცემების დამუშავების საკითხებს.[22]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თავდაპირველი რედაქცია არ ითვალისწინებდა კონკრეტულ ჩანაწერებს არასრულწლოვანთა პერსონალური მონაცემების დამუშავებასთან მიმართებით. საგულისხმოა, რომ კანონის ახალი რედაქციის თანახმად, იზრდება მონაცემთა სუბიექტის უფლებები და ფართოვდება მათი დაცვის გარანტიები. იგი ითვალისწინებს სპეციალურ მოწესრიგებას არასრულწლოვანთა პერსონალური მონაცემების დამუშავებასთან დაკავშირებით. კერძოდ, მე-7 მუხლში წარმოდგენილია არასრულწლოვნის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესი და პირობები. არასრულწლოვნის შესახებ მონაცემთა დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაითვალისწინოს და დაიცვას არასრულწლოვნის საუკეთესო ინტერესები.[23] აგრეთვე, ვიდეომონიტორინგის განხორციელების დასაშვებობის ერთ-ერთი საფუძველია არასრულწლოვნის დაცვა (მათ შორის, მავნე ზეგავლენისგან).[24] ახალი კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირის მიერ მოთხოვნის შემთხვევაში მონაცემთა დამუშავების დაბლოკვის ვალდებულებისგან ერთ-ერთ გამონაკლისს არასრულწლოვნის უფლებების დაცვის აღმატებული ინტერესი წარმოადგენს.[25] საკანონმდებლო სიახლე ის რომ დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს, განსაკუთრებით თუკი მონაცემთა სუბიექტი არასრულწლოვანია, მიაწოდოს ინფორმაცია მარტივ და მისთვის გასაგებ ენაზე.[26] არასრულწლოვანი პირის მიერ ადმინისტრაციული სამართალდარღვევის ჩადენა პასუხისმგებლობის ერთ-ერთ შემამსუბუქებელ გარემოებად მიიჩნევა,[27] ხოლო არასრულწლოვნის მონაცემების დამუშავება კანონის მოთხოვნათა დარღვევით, პასუხისმგებლობის დამამძიმებელი გარემოებაა.[28]

1.2. დარგობრივი ეროვნული კანონმდებლობის მიმოხილვა

საქართველოში ბავშვის უფლებათა დაცვის მომწესრიგებელი საკანონმდებლო აქტის — „ბავშვის უფლებათა კოდექსის“ მიზანს წარმოადგენს ბავშვის კეთილდღეობის უზრუნველყოფა საქართველოს კონსტიტუციის, ბავშვის უფლებათა კონვენციის, მისი დამატებითი ოქმებისა და სახელმწიფოს მიერ აღიარებული სხვა საერთაშორისო

[22] პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის საქმიანობის ანგარიში, 2022, 197-202.
[23] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 7.
[24] იქვე, მუხლი 10.
[25] იქვე, მე-17 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტი.
[26] იქვე, 24-ე მუხლის მე-5 პუნქტი.
[27] იქვე, 61-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი.
[28] იქვე, 62-ე მუხლის „გ“ ქვეპუნქტი.

სამართლებრივი აქტების ეფექტიანი იმპლემენტაციის ხელშეწყობით.[29] კოდექსი განსაზღვრავს ბავშვის ძირითად უფლებებსა და თავისუფლებებს, ქმნის ბავშვის ძირითადი უფლებებისა და თავისუფლებების დაცვისა და მხარდაჭერის სისტემის ფუნქციონირების სამართლებრივ საფუძვლებს.[30] კოდექსის მიზნებისთვის, ბავშვი არის 18 წლამდე პირი, რომელშიც მოიაზრება ყველა არასრულწლოვანი, განურჩევლად სხვადასხვა მახასიათებლისა, რაც პირდაპირ არის დაკავშირებული თანასწორობის უფლებასთან.[31]

ბავშვის უფლებათა კოდექსის მე-9 მუხლით გათვალისწინებულია ბავშვის პირადი და ოჯახური ცხოვრების უფლება, რომლის ფარგლებშიც აღნიშნულია, 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.[32] კოდექსი არ კრძალავს ბავშვის პერსონალური მონაცემების დამუშავებას ისეთი მიზნებისთვის, როგორიცაა: ჯანმრთელობის დაცვა, განათლების და სოციალური დაცვის მიმართულება. თუმცა, უნდა განხორციელდეს ბავშვის საუკეთესო ინტერესებიდან გამომდინარე და მხოლოდ საქართველოს კანონმდებლობის შესაბამისად.[33] ბავშვის საუკეთესო ინტერესის შესახებ მოცემული დეფინიცია არ მოიცავს ამომწურავ განმარტებას და ტოვებს სუბიექტური შეფასების შესაძლებლობას.[34] თანამედროვე ტექნოლოგიების განვითარების პირობებში, ბავშვის უფლებათა კოდექსის შესაბამისად, არასრულწლოვანთა პერსონალური მონაცემების დამუშავების კონტექსტში, ასევე რელევანტურია: ბავშვის სიცოცხლისა და პიროვნული განვითარების უფლება,[35] ბავშვის განათლების უფლება,[36] ბავშვის აზრის, ინფორმაციის, მასობრივი ინფორმაციის საშუალებებითა და ინტერნეტით სარგებლობის თავისუფლების უფლებები.[37]

არასრულწლოვნებთან მიმართებით, პერსონალურ მონაცემთა დაცვის საკითხის განხილვისას, აღსანიშნავია „არასრულწლოვანთა მართლმსაჯულების კოდექსი“, რომელიც ადგენს „არასრულწლოვნის ადმინისტრაციული და სისხლისსამართლებრივი პასუხისმგებლობის, არასრულწლოვნის მონაწილეობით ადმინისტრაციული სამართალდარღვევის საქმის წარმოების და სისხლის სამართლის პროცესის თავისებურებებს, სასჯელისა და სხვა ზომების აღსრულების სპეციალურ

[29] საქართველოს კანონი, ბავშვის უფლებათა კოდექსი, 20/09/2020, მუხლი 1, <https://matsne.gov.ge/document/view/4613854?publication=4>, [10.08.2023].
[30] იქვე, მე-2 მუხლის პირველი ნაწილი.
[31] კილაძე ს., ტურავა პ., ბავშვის უფლებათა კოდექსის სახელმძღვანელო კომენტარები, 2021, 47.
[32] ბავშვის უფლებათა კოდექსი, მუხლი 9.
[33] კილაძე ს., ტურავა პ., ბავშვის უფლებათა კოდექსის სახელმძღვანელო კომენტარები, 2021, 278.
[34] იქვე, 43.
[35] ბავშვის უფლებათა კოდექსი, მუხლი 6.
[36] იქვე, მუხლი 10.
[37] იქვე, მუხლი 14.

წესებს".[38] კოდექსის მიზანია „მართლმსაჯულების პროცესში არასრულწლოვნის საუკეთესო ინტერესების დაცვა, კანონთან კონფლიქტში მყოფი არასრულწლოვნის რესოციალიზაცია-რეაბილიტაცია, არასრულწლოვანი დაზარალებულისა და არასრულწლოვანი მოწმის უფლებათა დაცვა, არასრულწლოვანი დაზარალებულისა და არასრულწლოვანი მოწმის მეორეული ვიქტიმიზაციისა და არასრულწლოვანი დაზარალებულის ხელახალი ვიქტიმიზაციის თავიდან აცილება, ახალი დანაშაულის თავიდან აცილება და მართლწესრიგის დაცვა."[39]

კოდექსის მე-13 მუხლით გარანტირებულია არასრულწლოვნის პირადი ცხოვრების დაცულობის უფლება. ამავე მუხლის თანახმად, „არასრულწლოვნის პირადი ცხოვრების დაცულობა უზრუნველყოფილია არასრულწლოვანთა მართლმსაჯულების ნებისმიერ სტადიაზე. არასრულწლოვნის ნასამართლობისა და ადმინისტრაციული პასუხისმგებლობის შესახებ ინფორმაცია საჯარო არ არის. დაუშვებელია არასრულწლოვნის პერსონალური მონაცემების გამჟღავნება და გამოქვეყნება, გარდა „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით გათვალისწინებული შემთხვევებისა."[40] არასრულწლოვანთა მართლმსაჯულების კონტექსტში პირადი ცხოვრების ხელშეუხებლობის საკითხი შედგება შემდეგი ორი მნიშვნელოვანი კომპონენტისგან: ა) სახელმწიფომ არ დაუშვას კანონთან კონფლიქტში მყოფი ბავშვის შესახებ იმ ინფორმაციის გავრცელება, რომლითაც შესაძლებელი გახდება მისი იდენტიფიცირება; ბ) სატელევიზიო რეპორტაჟების დროს, არ უნდა იყოს შესაძლებელი მოზარდის გარეგნული იდენტიფიცირება, რათა მომავალში „დამნაშავედ იდენტიფიცირებულ" მოზარდს არ გაუჭირდეს საზოგადოებაში ინტეგრაცია და რესოციალიზაცია. პირადი ცხოვრების ხელშეუხებლობის უფლება მჭიდრო კავშირშია ისეთ უფლებებთან, როგორიცაა: იდენტობის შენარჩუნება, უდანაშაულობის პრეზუმფცია, ბავშვის ჭეშმარიტი ინტერესის ან ბავშვის ღირსებისა და ხელშეუვალობის დაცვა. ყოველივე აღნიშნული წარმოადგენს ბავშვის ჯანმრთელი ემოციური, სულიერი და ფიზიკური განვითარების ძირითად ელემენტებს.[41]

1.3. არასრულწლოვნის მონაცემთა დამუშავების ცალკეული ელემენტები

არასრულწლოვნები სწრაფად ითვისებენ ახალ შესაძლებლობებს და ციფრული ტექნოლოგიების დამოუკიდებელ მომხმარებლებად გვევლინებიან.[42] აქიდან გამომდინარე, რომ არასრულწლოვნები საზოგადოების მოწყვლად ჯგუფებს წარმოადგენენ, მათი მონაცემების დამუშავებისას განსაკუთრებული გულისხმიერება

[38] არასრულწლოვანთა მართლმსაჯულების კოდექსი, პირველი მუხლის პირველი ნაწილი.
[39] იქვე, პირველი მუხლის მე-2 ნაწილი.
[40] იქვე, მუხლი 13.
[41] შალიკაშვილი მ., მიქანაძე გ., არასრულწლოვანთა მართლმსაჯულება (სახელმძღვანელო), 2016, 86-87.
[42] ICO, Children's Data and Privacy Online, 4.

უნდა იყოს გამოჩენილი. მონაცემთა დამუშავება მოიაზრებს ნებისმიერ ქმედებას ან ქმედებათა ერთობლიობას პერსონალურ მონაცემთან ან მონაცემთა ერთობლიობასთან მიმართებით, რომელიც ხორციელდება ავტომატური თუ სხვა საშუალებებით.[43] არასრულწლოვნების მონაცემების დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია შეიმუშაოს სპეციალური სისტემები და დაიცვას მონაცემთა დაცვის პრინციპებთან შესაბამისობა. განსაკუთრებით მნიშვნელოვანია, დამუშავების კანონიერი საფუძვლების არსებობა.[44] მონაცემთა დამუშავება კანონიერად მიიჩნევა, თუკი კანონის შესაბამისია, გააჩნია ლეგიტიმური მიზანი, აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში[45]. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ თანახმად, არასრულწლოვნის პერსონალური მონაცემების დამუშავება კანონიერად მიიჩნევა, თუკი იგი სულ მცირე 16 წლისაა; 16 წელს მიუღწეველი პირის მონაცემთა დამუშავება კანონიერი იქნება მხოლოდ იმ შემთხვევაში, თუ თანხმობა გაცემულია ან დამუშავება ნებადართულია მშობლის ან კანონიერი წარმომადგენლის მიერ. ამ მიზნით წევრი სახელმწიფო უფლებამოსილია კანონმდებლობით დააწესოს უფრო დაბალი ასაკობრივი ცენზი, თუმცა არანაკლებ 13 წლისა.[46] ასაკობრივი ცენზის განსაზღვრა მნიშვნელოვანია და განპირობებულია სხვადასხვა ფაქტორით. პირველ რიგში, აღნიშნული უკავშირდება ბავშვის შესაძლებლობას გაცნობიერებულად შეეძლოს საკუთარი უფლებების აღქმა, თუმცა იმ შემთხვევაში, როდესაც აშკარაა, რომ ის მოქმედებს საკუთარი საუკეთესო ინტერესების საწინააღმდეგოდ, მაშინ იგი არ მიიჩნევა კომპეტენტურად.[47] ეროვნული საკანონმდებლო რეფორმის პროცესში გათვალისწინებულ იქნა არასრულწლოვნის მიერ თანხმობის სახით ნების დამოუკიდებლად გამოხატვის უფლება, რაც, მსგავსად ევროპული მოწესრიგებისა, უკავშირდება ასაკობრივ ცენზს, რომელიც ასევე 16 წელია.[48] ასევე, გაეროს კომიტეტის ზოგად კომენტარში ხაზგასმულია ბავშვის აზრის მოსმენის უფლება, რომლის თანახმად, სახელმწიფოებმა უნდა უზრუნველყონ საკუთარი შეხედულებების ჩამოყალიბების უნარის მქონე ბავშვების მიერ შეხედულების თავისუფლად გამოხატვა მათთან დაკავშირებულ ყველა საკითხზე.[49]

---

[43] ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 113-116.

[44] ICO, Children and the GDPR, 2018, 1.

[45] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 314.

[46] GDPR, ART. 8.1.

[47] იხ., გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ოფიციალური ვებგვერდი: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/>, [10.08.2023].

[48] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 7.

[49] General Comment No. 12 (2009) The Right of the Child to be Heard, §§20-21.

1.4. ბავშვის საუკეთესო ინტერესი

ბავშვთა საუკეთესო ინტერესის დაცვის პრინციპი აღიარებული და განმტკიცებულია არაერთი სამართლებრივი აქტით, როგორც ეროვნულ,[50] ასევე საერთაშორისო დონეზე.[51] პერსონალური მონაცემების დაცვის კონტექსტში, არასრულწლოვნის საუკეთესო ინტერესის დაცვას უზრუნველყოფს „ბავშვის უფლებების შესახებ“ 1989 წლის კონვენცია (“CRC”), რომლის მიხედვითაც ბავშვებთან დაკავშირებით ნებისმიერი მოქმედების განხორციელებისას საჯარო ან კერძო სოციალური კეთილდღეობის დაწესებულებების, სასამართლოების, ადმინისტრაციული თუ საკანონმდებლო ორგანოების მიერ, უპირველეს ყოვლისა, გათვალისწინებული უნდა იყოს ბავშვის საუკეთესო ინტერესები.[52] ბავშვის საუკეთესო ინტერესების დეფინიცია დინამიკური და მოქნილია, იმისათვის, რომ ადეკვატურად პასუხობდეს ბავშვთან დაკავშირებულ ყველა შესაძლო შემთხვევასა თუ გამოწვევას.[53] ბავშვის საუკეთესო ინტერესის განსაზღვრისას, პირველ რიგში, უნდა დადგინდეს კონკრეტული გარემოებები, რაც განსაკუთრებულს ხდის მას, ხოლო საუკეთესო ინტერესების შეფასებისას, შემდეგი ელემენტები უნდა იქნას მხედველობაში მიღებული: ბავშვის მოსაზრება; ბავშვის იდენტურობა; ოჯახური გარემოს უზრუნველყოფა და ურთიერთობის შენარჩუნება; ბავშვზე ზრუნვა, მისი დაცვა და უსაფრთხოების უზრუნველყოფა; მოწყვლადობის გათვალისწინება; ბავშვის ჯანმრთელობის დაცვის უფლება; ბავშვის განათლების მიღების უფლება.[54] არასრულწლოვნის საუკეთესო ინტერესის ცნება გულისხმობს მის მიერ კონვენციით განსაზღვრული ყველა უფლებით სრულ და ეფექტურ სარგებლობას, არასრულწლოვნის სრულფასოვანი განვითარების უზრუნველყოფასა და მისი ღირსების დაცვას. სრულყოფილი განვითარება განმარტებულია, როგორც ფიზიკური, გონებრივი, სულიერი, მორალური, ფსიქოლოგიური და სოციალური განვითარება.[55]

---

[50] ბავშვის უფლებათა კოდექსი, საქართველოს კანონი, 27/09/2019.

[51] კონვენცია ბავშვის უფლებების შესახებ, საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება, 1948.

[52] UN, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, Article 3.1

[53] კილაძე ს., ტურავა პ., ბავშვის უფლებათა კოდექსის კომენტარები, 2021, 44.

[54] Data Protection Commission of Ireland, Children Front and Centre, Fundamentals for Child-Oriented Approach to Data Processing, December 2020, 19.

[55] გაეროს ბავშვის უფლებათა კომიტეტის, N 14 ზოგადი კომენტარი (2013), ბავშვის საუკეთესო ინტერესის უპირატესობის მინიჭების შესახებ, §§4-5.

ბავშვის საუკეთესო ინტერესისთვის უპირატესობის მინიჭების ვალდებულება სამგანზომილებიანია და მოიცავს მატერიალურ უფლებას, ძირითად საკანონმდებლო პრინციპსა და პროცედურულ ნორმას. აღნიშნული გულისხმობს: არასრულწლოვნის უფლებას, მისი საუკეთესო ინტერესები შეფასდეს და იქნეს მიჩნეული უპირატესად, როდესაც ხდება სხვადასხვა ინტერესის განხილვა კონკრეტულ საკითხზე გადაწყვეტილების მისაღებად; არასრულწლოვანთან დაკავშირებული გადაწყვეტილების მიღების პროცესი უნდა მოიცავდეს ამ გადაწყვეტილების შესაბამის ბავშვზე ან ბავშვებზე შესაძლო ზეგავლენის (დადებითი თუ უარყოფითი) შეფასებას.[56] ბავშვის საუკეთესო ინტერესების შეფასება და განსაზღვრა მოითხოვს საპროცესო გარანტიებს.[57]

ბავშვის საუკეთესო ინტერესის ცნება შესწავლილი იქნა „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”)[58] წინამორბედი 29-ე მუხლის სამუშაო ჯგუფის მიერ 2009 წლის მოსაზრებაში,[59] რომელშიც აღინიშნა, რომ ბავშვის საუკეთესო ინტერესები დაცული უნდა იყოს ყველა იმ პირის მიერ, ვინც ბავშვებთან დაკავშირებულ გადაწყვეტილებებს იღებს. აღნიშნული ეფუძნება იმ გარემოებას, რომ ადამიანს, რომელსაც ჯერ არ მიუღწევია ფიზიკური და ფსიქოლოგიური სიმწიფისთვის, სჭირდება მეტი დაცვა, სხვა ასაკობრივ ჯგუფებთან შედარებით. სასამართლო პრაქტიკა ადასტურებს, რომ „მშობლის თვალით“ დანახული ბავშვის საუკეთესო ინტერესი ყოველთვის არ არის თანმხვედრი ბავშვის საუკეთესო ინტერესთან,[60] რაც, თანამედროვე ეპოქაში შესაძლოა, გამოიკვეთოს მშობლებისა და არასრულწლოვანი

[56] Digital Futures Commission, Child Rights Impact Assessment, a Tool to Realize Children's Rights in the Digital Environment, 2021, 8-9.

[57] გაეროს ბავშვის უფლებათა კომიტეტის მე-14 ზოგადი კომენტარი (2013), ბავშვის საუკეთესო ინტერესის უპირატესობის მინიჭების შესახებ, § 6.

[58] The European Data Protection Board (EDPB) is established under Article 68 of the GDPR as an independent EU body which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

[59] Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools).

[60] „2017 წელს, 16 წლის არასრულწლოვანმა მიმართა სასამართლოს, მშობლის მიერ სოციალურ ქსელში მისი ფოტოს თანხმობის გარეშე განთავსების გამო. სასამართლომ მშობელს დაავალა ფოტოს წაშლა, წინააღმდეგ შემთხვევაში სანქციის სახით განუსაზღვრა ჯარიმა 10 000 ევროს ოდენობით. 2016 წელს ავსტრალიელმა თინეიჯერმა სარჩელი შეიტანა მშობლების წინააღმდეგ სასამართლოში, რომლებმაც ბოლო 7 წლის განმავლობაში განათავსეს 500-მდე „სამარცხვინო“ ფოტოები სოციალურ ქსელში, შვილის თანხმობის გარეშე“. შუდრა თ., ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2023, სქ. 10, 109, ციტირება: Goshadze K., Legal Implications of "Shattering", International Journal of Law: "Law and World ", №15, Vol. 6, Issue 2, 2020, 5.

შვილების განსხვავებულ შეხედულებებში, მათ შორის, ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვის კონტექსტში.[61]

2. მონაცემთა დამუშავების პრინციპების ზოგადი მიმოხილვა

ციფრულ გარემოში ბავშვთა პირადი და ოჯახური ცხოვრების დაცულობის უფლება მოიცავს მათი პერსონალური მონაცემების დაცვას, ასევე, კორესპონდენციისა და პირადი კომუნიკაციების კონფიდენციალურობის პატივისცემას.[62] ბავშვების პირადი ცხოვრების დაცულობა დაკავშირებულია მათ ფიზიკურ და გონებრივ მთლიანობასთან, გადაწყვეტილების მიღების ავტონომიასთან, იდენტობასთან, ინფორმაციულ და ფიზიკურ თუ სივრცულ კონფიდენციალურობასთან.[63] ბავშვის პირადი ცხოვრების ხელშეუხებლობის უზრუნველსაყოფად განსაკუთრებით მნიშვნელოვანია, რომ მათი მონაცემების დამუშავებისას დაცულ იქნეს მონაცემთა დამუშავების პრინციპები და მონაცემები მათ სასარგებლოდ, საუკეთესო ინტერესის გათვალისწინებით დამუშავდეს.[64] ეროვნული კანონმდებლობისა და ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ გათვალისწინებით, წინამდებარე თავში განიხილება მონაცემთა დაცვის ექვსი ძირითადი პრინციპი:

- სამართლიანობა, კანონიერება და გამჭვირვალობა;
- კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზანი;
- მონაცემთა მინიმიზაცია;
- ნამდვილობა და სიზუსტე;
- შენახვის ვადის შეზღუდვა;
- მონაცემთა უსაფრთხოება.

---

[61] შუდრა თ., ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2023, 109.

[62] Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7, §26, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [10.08.2023].

[63] The Special Rapporteur on the Right to Privacy, Joseph A. Cannataci, Artificial Intelligence and Privacy, and Children's Privacy, Report, §71, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement>, [10.08.2023].

[64] Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7, §29, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [10.08.2023].

2.1. სამართლიანობის, კანონიერებისა და გამჭვირვალობის პრინციპი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონი ითვალისწინებს კანონიერების, სამართლიანობისა და გამჭვირვალობის პრინციპს, რომლის მიხედვითაც, მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად, მონაცემთა სუბიექტისთვის გამჭვირვალედ და მისი ღირსების შეულახავად.[65]

2.1.1. კანონიერება

პერსონალურ მონაცემთა კანონიერი დამუშავება გულისხმობს, რომ მონაცემები უნდა დამუშავდეს მხოლოდ მაშინ, როდესაც არსებობს შესაბამისი საფუძველი[66] და დაცულია ყველა სამართლებრივი მოთხოვნა,[67] მიუხედავად იმისა, მონაცემი ეკუთვნის ბავშვს თუ ზრდასრულ პირს.[68] დამუშავების ოპერაციები სამართლებრივ მოთხოვნებთან სრულ შესაბამისობაში უნდა იყოს.[69] უპირველეს ყოვლისა, იმისათვის, რომ დამუშავება კანონიერად იქნას მიჩნეული, იგი უნდა შეესაბამებოდეს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლს, რომელიც მოითხოვს, რომ დამუშავების ნებისმიერი ოპერაცია ამომწურავ ჩამონათვალში მოცემული ექვსი სამართლებრივი საფუძვლიდან მინიმუმ ერთს მაინც აკმაყოფილებდეს:[70] ა) მონაცემთა სუბიექტის თანხმობა; ბ) ხელშეკრულების შესრულება ან მის გაფორმებამდე გარკვეული ზომების მიღება; გ) სამართლებრივი ვალდებულების შესრულება; დ) მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვა; ე) საჯარო ინტერესის სფეროში შემავალი ამოცანების შესრულება ან ოფიციალური უფლებამოსილების განხორციელება; ვ) მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ან სხვა მხარის ლეგიტიმური

[65] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-4 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი.

[66] Adv. Prashant Mali, GDPR Articles with Commentary & EU Case Laws, 15.

[67] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[68] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 22 <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>, [10.08.2023].

[69] Sanjay Sharma, PhD with research associate Pranav Menon, 2020, 126.

[70] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [10.08.2023].

ინტერესები (თუ განსახილველ ინტერესებს არ გადაწონის მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები).[71]

აღნიშნულის გათვალისწინებით, პერსონალურ მონაცემთა შეგროვება და დამუშავების ოპერაციების განხორციელება მხოლოდ მაშინ არის შესაძლებელი, როდესაც არსებობს დამუშავების ლეგიტიმური საფუძველი, მაგალითად, თანხმობა. თუ პერსონალური მონაცემების შეგროვება განხორციელდა არაავტორიზებული წვდომის შედეგად, დამუშავება უკანონო იქნება და, შესაბამისად, დაირღვევა კანონიერების პრინციპი.[72] გარდა ამისა, მონაცემთა დამუშავებას უნდა გააჩნდეს ლეგიტიმური მიზანი, უნდა იყოს აუცილებელი და პროპორციული დემოკრატიულ საზოგადოებაში.[73]

2.1.2. სამართლიანობა

სამართლიანობა ყოვლისმომცველი პრინციპია, რომელიც მოითხოვს, რომ პერსონალური მონაცემები მონაცემთა სუბიექტის საზიანოდ, დისკრიმინაციულად არ დამუშავდეს, არ აღმოჩნდეს მოულოდნელი ან შეცდომაში შემყვანი.[74] ამ პრინციპის მიხედვით, მონაცემთა მოპოვება ან სხვაგვარად დამუშავება უსამართლო საშუალებებით, შეცდომაში შეყვანით ან მონაცემთა სუბიექტის ცოდნის გარეშე, დაუშვებელია.[75] სამართლიანობის პრინციპის მიზანი პიროვნების ინტერესების დაცვაა, რაც ბავშვების შემთხვევაში განსაკუთრებით აქტუალურია.[76] მნიშვნელოვანია, რომ მონაცემთა სუბიექტი ინფორმირებული იყოს მისი პერსონალური მონაცემების დამუშავების შესახებ, როგორ მოხდება მონაცემების შეგროვება, შენახვა და გამოყენება. თუმცა, გარკვეულ შემთხვევებში, დამუშავება ნებადართულია კანონით

[71] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 22 <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>, [10.08.2023].

[72] Adv. Prashant Mali, GDPR Articles with Commentary & EU Case Laws, 15.

[73] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[74] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §69, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].

[75] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[76] Information Commissioner's Office (ICO), Children and the GDPR, 2018, 12, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-1-0.pdf>, [18.08.2023].

და სამართლიანად ითვლება, მიუხედავად მონაცემთა სუბიექტის ცოდნისა და სურვილისა.[77]

დამუშავების ოპერაციის სამართლიანობის საკითხი კონტექსტის მიხედვით უნდა გადაწყდეს.[78] „მონაცემთა დაცვის ევროპული საბჭოს“ („EDPB“) ერთ-ერთ სახელმძღვანელოში[79] მოცემულია სამართლიანობის გარკვეული ელემენტების არასრული ჩამონათვალი, რომლებიც პერსონალური მონაცემების დამუშავებისას უნდა იქნას დაცული. სამართლიანობის მნიშვნელოვან ელემენტებად აღიარებულია, მონაცემთა სუბიექტის მოლოდინი,[80] მისი მონაცემების გონივრული გამოყენების შესახებ, ასევე, გარკვეული ფსიქოლოგიური მდგომარეობის გამო დისკრიმინაციისაგან ან ექსპლუატაციისაგან დაცვის უფლება. “EDPB”-ის განმარტების თანახმად, იმისათვის, რომ დამუშავება „სამართლიანი“ იყოს, დაუშვებელია მოტყუებით მონაცემთა დამუშავება და ყოველი არჩევანი ობიექტური და ნეიტრალური გზით უნდა იყოს წარმოდგენილი, შეცდომაში შემყვანი ან მანიპულაციური ენის ან დიზაინის თავიდან აცილების მიზნით.[81] ინფორმაციის ბავშვებისთვის მიწოდებისას განსაკუთრებული ყურადღება უნდა მიექცეს ენის სიცხადეს.[82]

2.1.3. გამჭვირვალობა

მონაცემთა სამართლიანად დამუშავების პრინციპთან მჭიდროდაა დაკავშირებული გამჭვირვალობის პრინციპი. “GDPR”-ის მიღებამდე გამჭვირვალობის მოთხოვნა აღიქმებოდა სამართლიანობის ცნების შემადგენელ ნაწილად.[83] გამჭვირვალობის პრინციპის მიხედვით, ფიზიკური პირებისთვის ნათელი უნდა იყოს, რომ მათთან დაკავშირებული პერსონალური მონაცემების შეგროვება, გამოყენება, გაცნობა ან სხვა

[77] Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells, European Data Protection Law and Practice, Second Edition, 2019, 128.
[78] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[79] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].
[80] იხ. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Convention 108, Children’s Data Protection in Education Systems: Challenges and Possible Remedies, 2019, 12, <https://rm.coe.int/t-pd-2019-06final-eng-report-children/1680a01b47>, [18.08.2023].
[81] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[82] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 315.
[83] იქვე, 314.

სახით დამუშავება ხორციელდება.[84] ამასთანავე, "GDPR"-ის თანახმად, თუ პირებს ორგანიზაციის მიერ გარკვეული ინფორმაცია მიეწოდებათ მათი პერსონალური მონაცემების გამოყენების შესახებ, მისი მიწოდება ლაკონიური, გამჭვირვალე, გასაგები და ადვილად ხელმისაწვდომი ფორმით, მკაფიო და მარტივი ენით უნდა მოხდეს. ინფორმაციის სიცხადე განსაკუთრებით მნიშვნელოვანია, როდესაც იგი ბავშვს მიეწოდება.[85] 29-ე მუხლის სამუშაო ჯგუფის განმარტებების მიხედვით, გამჭვირვალობა დამოუკიდებელი უფლებაა, რომელიც ისევე ეხება ბავშვებს, როგორც ზრდასრულებს.[86] ეს ნიშნავს, რომ ბავშვებს უფლება აქვთ, საკუთარი პერსონალური მონაცემების დამუშავების შესახებ ინფორმაცია მიიღონ,[87] მიუხედავად დამუშავების სამართლებრივი საფუძვლისა, მაშინაც კი, როდესაც მშობელმა ან მეურვემ მათი სახელით თანხმობა განაცხადა მათივე პერსონალური მონაცემების დამუშავებაზე.[88]

მნიშვნელოვანია გამჭვირვალობის შესახებ ინფორმაციის შესაბამის აუდიტორიაზე მორგება.[89] აღნიშნულის გათვალისწინებით, ბავშვებისთვის კომპლექსური, სამართლებრივი, ბუნდოვანი ან ჟარგონული ენით ინფორმაციის მიწოდება არ არის საკმარისი.[90] გამჭვირვალობის პრინციპი მოითხოვს, რომ როდესაც მონაცემთა დამმუშავებლების სამიზნე აუდიტორიას ბავშვები წარმოადგენენ ან მათ პროდუქციას თუ მომსახურებას განსაკუთრებით ისინი იყენებენ, ნებისმიერი ინფორმაცია და კომუნიკაცია უნდა იყოს გადმოცემული მკაფიო და მარტივი ენით[91] ან ადვილად გასაგები საშუალებებით.[92] შესაძლოა გამოყენებულ იქნას ვიზუალური ტექნიკები,

---

[84] GDPR, Recital 39.

[85] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27.

[86] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, §14, <https://ec.europa.eu/newsroom/article29/items/622227/en>, [18.08.2023].

[87] იხ. Information Commissioner's Office (ICO), Children and the GDPR, 2018, 38, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-1-0.pdf>, [18.08.2023].

[88] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>, [18.08.2023].

[89] Morgan A., The Transparency Challenge: Making children aware of their data protection rights and the risks online, Volume 23, No.1, 2018, 3, <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf>, [18.08.2023].

[90] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27.

[91] იხ. იქვე, 29.

[92] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, §§14-15, <https://ec.europa.eu/newsroom/article29/items/622227/en>, [18.08.2023].

როგორიცაა: ანიმაციები, პიქტოგრამები, ინფოგრამები, ფოტოები, ვიდეოები,[93] რაც მეტად მიიპყრობს ბავშვების ინტერესს.[94] შესაბამისი ღონისძიებების შერჩევისას ყურადღება უნდა გამახვილდეს კონკრეტულ სერვისზე, ბავშვის ასაკსა და განვითარების ეტაპებზე. მონაცემთა დამმუშავებლის მიერ მიზანშეწონილია იმავე ფორმატის გამოყენება, რაც ყველაზე მეტად რელევანტურია შეთავაზებულ სერვისთან. მაგალითად, თუ ისინი ოპერირებენ ვიდეოს გაზიარების პლატფორმაზე, მაშინ ბავშვებისთვის ინფორმაციის გადასაცემად ვიდეო უფრო შესაფერისი საშუალება იქნება, ვიდრე სურათი ან ტექსტი.[95]

2.1.4. საერთაშორისო სასამართლო პრაქტიკა

ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ დაადგინა, რომ „ადამიანის უფლებათა ევროპული კონვენციის“ მე-8 მუხლის პირველი პუნქტის მიხედვით, პერსონალური მონაცემების დამუშავება შესაძლებელია კონკრეტულ გარემოებებში მონაცემთა სუბიექტის პირადი ცხოვრების პატივისცემის უფლებაში ჩარევას წარმოადგენდეს.[96] იმისათვის, რომ ამგვარი ჩარევა გამართლებული იყოს, იგი, სხვა საკითხებთან ერთად, უნდა შეესაბამებოდეს კანონს (კონვენციის მე-8 მუხლის მე-2 პუნქტი), რაც შეიძლება უკავშირდებოდეს კანონიერი დამუშავების მოთხოვნას. ამგვარი საკანონმდებლო ჩარჩო უნდა იყოს განჭვრეტადი მისი შედეგების მიხედვით. საქმეში: “*Rotaru v Romania”,*[97] სასამართლომ აღნიშნა, რომ განჭვრეტადობისთვის შიდა კანონმდებლობამ ხელისუფლების უფლებამოსილებებზე შეზღუდვები უნდა დააწესოს: კანონმა უნდა განსაზღვროს ინფორმაციის სახეები, რომლის დამუშავებაც შესაძლებელია; პირთა კატეგორიები, რომლებზეც შეიძლება შეგროვდეს ინფორმაცია; გარემოებები, როდესაც ასეთი

[93] Morgan A., The Transparency Challenge: Making Children aware of their Data Protection Rights and the Risks Online, Volume 23, No.1, 2018, 3, <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf>, [18.08.2023].

[94] Information Commissioner’s Office (ICO), Children and the GDPR, 2018, 38, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-1-0.pdf>, [18.08.2023].

[95] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [18.08.2023].

[96] იხ. Case of S. and Marper v. the United Kingdom, [GC], [2008] ECHR App. Nos. 30562/04 and 30566/04; case of L.B. v. Hungary, [GC], [2023] ECHR App. No. 36345/16.

[97] Case of Rotaru v Romania, [GC], [2000] ECHR App. No. 28341/95.

ზომების მიღებაა შესაძლებელი; პირები, რომლებსაც მონაცემებზე წვდომა შეუძლიათ; და მონაცემთა შენახვის ვადები.[98]

ევროკავშირის მართლმსაჯულების სასამართლომ *"Bara"*-ს[99] საქმეში დაადგინა, რომ პერსონალური მონაცემების სამართლიანი დამუშავების მოთხოვნის თანახმად, საჯარო დაწესებულებამ მონაცემთა სუბიექტებს მათი პერსონალური მონაცემების სხვა მსგავსი ორგანოსთვის გადაცემის შესახებ უნდა აცნობოს.[100]

"*M.S."-ს* საქმეში,[101] სასამართლომ გამჭვირვალობის მოთხოვნასთან დაკავშირებით აღნიშნა, რომ პერსონალურ მონაცემებთან დაკავშირებით განხორციელებული ოპერაციები (როგორიცაა მონაცემთა მესამე მხარისთვის გადაცემა) აუცილებელია, ექცეოდეს მონაცემთა სუბიექტის გონივრული მოლოდინის ფარგლებში. სასამართლომ აღნიშნა, რომ სადავო მონაცემების შემდგომი გამოყენება ემსახურებოდა განსხვავებულ მიზანს, რომელიც მომჩივნის მოლოდინს სცდებოდა და დაასკვნა, რომ განხორციელდა მომჩივნის პირადი ცხოვრების უფლებაში ჩარევა.[102]

2.1.5. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *ერთ-ერთი საჯარო სკოლის პედაგოგი*

არასრულწლოვნებთან დაკავშირებული თითოეული გადაწყვეტილება მიღებული უნდა იყოს ბავშვის საუკეთესო ინტერესების გათვალისწინებით. პირადი ცხოვრების ხელშეუხებლობის უფლების სათანადოდ რეალიზებაში განსაკუთრებული როლი ბავშვზე მზრუნველ პირებს, მათ შორის, მასწავლებლებს აკისრიათ. აღნიშნულის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახურმა მიმართვის საფუძველზე ერთ-ერთი საჯარო სკოლის პედაგოგის მიერ ამავე სკოლის მოსწავლეების ფოტოზე აღბეჭდვისა და მის მიერ შესაბამისი ფოტოსურათ(ებ)ის გამჟღავნების კანონიერება შეისწავლა. სამსახურის მიერ საჯაროდ ხელმისაწვდომ წყაროებზე დაყრდნობით მოძიებული ინფორმაციით გაირკვა, რომ სკოლის პედაგოგის მიერ გაკვეთილის მიმდინარეობისას მუხლებზე დაჩოქილ/ჩაცუცქულ

[98] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.
[99] CJEU, Case C- 201/ 14, Bara [2015], §34.
[100] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.
[101] Case of M.S. v. Sweden, [1997] ECHR App. No. 74/1996/693/885.
[102] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.

მდგომარეობაში მყოფი არასრულწლოვნებისთვის მოხდა ფოტოსურათის გადაღება და მშობლებისათვის გაგზავნა.

სკოლის პედაგოგის მიერ მონაცემთა დამუშავების კანონიერების შესწავლის შედეგად სამსახურმა დაადგინა, რომ საჯარო სკოლის ერთ-ერთმა პედაგოგმა მოსწავლეებს გადაუღო ორი ფოტოსურათი. კერძოდ, ერთ ფოტოსურათზე აღბეჭდილნი იყვნენ მერხებთან მსხდომი ის მოსწავლეები, რომლებიც გაკვეთილზე მომზადებულნი გამოცხადდნენ, ხოლო მეორე ფოტოზე ასახულნი იყვნენ დაფასთან ე. წ. „ჩაცუცქულ“ მდგომარეობაში მყოფი ის მოსწავლეები, რომლებსაც არ ჰქონდათ ნასწავლი გაკვეთილი. საჯარო სკოლის მასწავლებლის მიერ წარმოდგენილი განმარტებით, მოსწავლეთა დასჯის ამსახველი გარემოების ფოტოზე აღბეჭდვა და მშობლებისთვის აღნიშნული ფოტოსურათის გაგზავნა განპირობებული იყო სწავლების მიზნებით. კერძოდ, მას სურდა მშობლების ინფორმირება მათი შვილების აკადემიური მოსწრების თაობაზე, რათა მათაც ეგრძნოთ სათანადო პასუხისმგებლობა. იგი დარწმუნებული იყო, რომ ასეთი ღონისძიება მოსწავლეების უკეთ სწავლისთვის მოტივაციის წყარო გახდებოდა. მასწავლებელმა ასევე აღნიშნა, რომ აღნიშნულმა ღონისძიებამ გაამართლა და მოსწავლეებმა უკეთ დაიწყეს მომზადება. აღსანიშნავია, რომ მედიასაშუალებების მიერ გავრცელებულ ფოტოსურათზე აღბეჭდილი მოსწავლეთა მდგომარეობა ტოვებდა აღქმას, რომ ისინი „დაჩოქილ“ მდგომარეობაში იყვნენ. მიუხედავად იმისა, „ჩაცუცქულ“ თუ „დაჩოქილ“ მდგომარეობაში იყვნენ ბავშვები, ორივე შემთხვევაში მათი ფოტოსურათზე ასახვა, ფოტოსურათის გადაღებისა და მშობლებისთვის გაგზავნის სრული კონტექსტის გათვალისწინებით, ხაზს უსვამდა მათ განსხვავებას გაკვეთილზე მომზადებულად მისულ მოსწავლეებთან შედარებით. ამასთან, იმ ფაქტორის გათვალისწინებით, რომ მოსწავლეთა აღნიშნული მდგომარეობა უკავშირდებოდა მათ არადამაკმაყოფილებელ მოსწრებას, როგორც „ჩაცუცქულ“, ასევე „დაჩოქილ“ მდგომარეობაში ყოფნა აღიქმებოდა ღირსების შელახვად. ამდენად, მასწავლებლის მიერ დასახული სწავლების მიზნების საპირწონე გარემოებად გამოიკვეთა არასრულწლოვნის ღირსების შელახვა, რაც, თავის მხრივ, ბავშვების ჩაგვრის, ე.წ. „ბულინგის“, დისკრიმინაციისა და არასათანადო მოპყრობის მსხვერპლად გახდომის საფრთხეს შეიცავდა. სამსახურმა დაადგინა, რომ გაკვეთილისთვის მოუმზადებელი ბავშვების მონაცემების დამუშავებისას სკოლის პედაგოგმა არ დაიცვა მონაცემთა სუბიექტის ღირსების შეულახავად მონაცემების დამუშავების პრინციპი, რის გამოც სკოლის მასწავლებელს პასუხისმგებლობა დაეკისრა „პერსონალურ მონაცემთა დაცვის

შესახებ“ საქართველოს კანონის 44-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის.

2.2. კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზანი

მიზნის შეზღუდვა მონაცემთა დაცვის ევროპულ სამართალში ერთ-ერთი ფუნდამენტური პრინციპია.[103] დამუშავების ნებისმიერი ოპერაციის მიზნის განსაზღვრა მონაცემთა დაცვის კანონმდებლობის გამოყენებისა და მონაცემთა დაცვის გარანტიების შემუშავებისთვის პირველი ეტაპია. ამასთანავე, მიზნის განსაზღვრა სხვა მოთხოვნების დაწესების წინაპირობას წარმოადგენს. მიზნის შეზღუდვის პრინციპი ადგენს საზღვრებს, რომლის ფარგლებშიც შესაძლებელია მოცემული მიზნისთვის შეგროვებული პერსონალური მონაცემების დამუშავება და შემდგომი გამოყენება.[104] აღნიშნული პრინციპი გულისხმობს, რომ მონაცემები უნდა შეგროვდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის.[105] პერსონალური მონაცემები, რომლებიც შეგროვდა ერთი მიზნით, არ შეიძლება თავისუფლად იქნას გამოყენებული[106] სხვა მიზნით.[107] თუ მონაცემთა შემდგომი დამუშავება იგეგმება, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ჯერ უნდა დარწმუნდეს, რომ აღნიშნულ დამუშავებას თავდაპირველ მიზანთან თავსებადი მიზნები აქვს. შეესაბამება თუ არა ახალი მიზანი საწყის მიზანს, უნდა შეფასდეს “GDPR”-ის მე-6 მუხლის მე-4 პუნქტის კრიტერიუმების მიხედვით.[108]

2.2.1. კონკრეტულობა

[103] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 140, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf>, [18.08.2023].

[104] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 4, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, [18.08.2023].

[105] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 315.

[106] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

[107] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-4 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი.

[108] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2, 2020, §71, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].

მიზნის კონკრეტულობა გულისხმობს, რომ ნებისმიერ შემთხვევაში, წინასწარ, არაუგვიანეს პერსონალურ მონაცემთა შეგროვების დაწყებისა,[109] მიზანი უნდა იყოს ზუსტად და სრულად იდენტიფიცირებადი. აღნიშნული საჭიროა იმის განსასაზღვრად, თუ რა სახის დამუშავებას მოიცავს კონკრეტული მიზანი. ასევე, კონკრეტული მიზანი მისი კანონთან შესაბამისობისა და გამოყენებულ მონაცემთა დაცვის მექანიზმების შეფასების შესაძლებლობას იძლევა.[110] პერსონალური მონაცემები უნდა შეგროვდეს კონკრეტული მიზნებისთვის. სწორედ ამიტომ, მონაცემთა დამუშავებისთვის უფლებამოსილმა პირმა გულდასმით უნდა განიხილოს, რა მიზნით ან მიზნებისთვის იქნება მონაცემი გამოყენებული და არ უნდა დაამუშაოს, თუკი იგი არ არის დასახული მიზნისა თუ მიზნებისთვის აუცილებელი, ადეკვატური ან შესაბამისი.[111]

გასათვალისწინებელია, რომ ზედმეტად ფართო მიზნების განსაზღვრა საფრთხეს უქმნის მიზნის შეზღუდვის პრინციპის დაცულობას. ზოგადი აღწერილობები, როგორიცაა „მომხმარებლის გამოცდილების გაუმჯობესება“, „მარკეტინგი“, „კვლევა“ ან „IT უსაფრთხოება“ საკმარისად კონკრეტული არ არის.[112] მაგალითად, „მონაცემთა დაცვის ევროპულმა საბჭომ“ (“EDPB”)-მ განმარტა,[113] რომ ვიდეომეთვალყურეობის დროს, მონიტორინგის მიზნები უნდა დაკონკრეტდეს ყველა გამოყენებული სათვალთვალო კამერისთვის და ვიდეო მეთვალყურეობა მხოლოდ „უსაფრთხოების“ ან „თქვენი უსაფრთხოების მიზნით“ არ არის საკმარისად კონკრეტული; მიუხედავად იმისა, რომ მიზანი არ უნდა იყოს ძალიან ფართო, არ არსებობს შეზღუდვა იმის შესახებ, თუ რამდენად კონკრეტული შეიძლება იყოს იგი; კონკრეტულობის ზუსტი დონე “GDPR”-ით ობიექტურად განსაზღვრული არ არის, ხშირ შემთხვევაში, შესაძლებელია, ფართო მიზნების დაყოფა მრავალ, უფრო კონკრეტულ მიზნად.[114]

2.2.2. მკაფიოდ განსაზღვრულობა

[109] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 315.

[110] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 39, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, [18.08.2023].

[111] იქვე, 15.

[112] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

[113] EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 2020, §15, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf>, [18.08.2023].

[114] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

მიზნების მკაფიოდ განსაზღვრულობა ნიშნავს, რომ იგი უნდა იყოს ნათლად გამოვლენილი, ახსნილი ან გამოხატული რაიმე ფორმით, რათა ნებისმიერ პირს შეექმნას დამუშავების მიზნების არაორაზროვანი გაგება, კულტურული ან ენობრივი განსხვავებების მიუხედავად.[115] შესაძლოა, არსებობდეს ისეთი მძიმე დარღვევების შემთხვევები, როგორიცაა შემთხვევა, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი დამუშავების მიზნებს საკმარისად დეტალურად ან მკაფიო და ნათელი ენით ვერ აკონკრეტებს, ან მითითებული მიზნები შეცდომაში შემყვანია, ან არ შეესაბამება რეალობას. ნებისმიერ ასეთ სიტუაციაში, ნამდვილი მიზნების დასადგენად ყველა ფაქტი უნდა იყოს გათვალისწინებული, საქმის კონტექსტიდან გამომდინარე მონაცემთა სუბიექტების საერთო გაგებასა და გონივრულ მოლოდინებთან ერთად.[116] ამ მოთხოვნის საბოლოო ამოცანა ბუნდოვანებისა და გაურკვევლობის გარეშე მიზნების დაზუსტებაა. მიზნები იმგვარად უნდა იქნას ფორმულირებული, რომ ერთგვარად იყოს აღქმადი არა მხოლოდ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის და ნებისმიერი სხვა უფლებამოსილი პირის მიერ, არამედ მონაცემთა დაცვის ორგანოებისა და დაინტერესებული მონაცემთა სუბიექტების მიერ. განსაკუთრებული ყურადღება უნდა მიექცეს იმის უზრუნველყოფას, რომ მიზნის ნებისმიერი სპეციფიკაცია საკმარისად მკაფიო იყოს ყველა დაინტერესებული პირისთვის, განურჩევლად მათი განსხვავებული კულტურული თუ ენობრივი წარმოშობის, გაგების დონისა და სპეციალური საჭიროებებისა.[117]

2.2.3. ლეგიტიმურობა

პერსონალური მონაცემები ლეგიტიმური მიზნებით უნდა შეგროვდეს. იმისათვის, რომ მიზნები ლეგიტიმური იყოს, მათი დამუშავება ყველა ეტაპზე და ნებისმიერ დროს უნდა ეფუძნებოდეს მინიმუმ ერთ სამართლებრივ საფუძველს.[118] ლეგიტიმურობა ფართო მოთხოვნაა და არ არის საკმარისი პერსონალურ მონაცემთა დაცვის კანონმდებლობის მხოლოდ რომელიმე მოთხოვნაზე მითითება.[119] იგი მოიცავს წერილობითი და საერთო სამართლის ყველა ფორმას, პირველად და მეორად კანონმდებლობას, მუნიციპალურ დადგენილებებს, სასამართლო პრეცედენტებს,

[115] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 39, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, [18.08.2023].
[116] იქვე.
[117] იქვე, 17.
[118] იქვე, 19.
[119] იქვე, 39.

კონსტიტუციურ პრინციპებს, ფუნდამენტურ უფლებებს, ზოგად სამართლებრივ პრინციპებს და სხვა.[120] იგი ასევე ვრცელდება სამართლის სხვა სფეროებზე და უნდა განიმარტოს პერსონალურ მონაცემთა დამუშავების კონტექსტში.[121]

კონკრეტული მიზნის ლეგიტიმური დადგენისას შესაძლებელია, გაითვალისწინონ ჩვეულებითი წესები, ქცევის კოდექსები, ეთიკის კოდექსები, სახელშეკრულებო შეთანხმებები და საქმის ზოგადი კონტექსტი და ფაქტები; იგი მოიცავს მონაცემთა დამუშავებისთვის უფლებამოსილ პირსა და მონაცემთა სუბიექტებს შორის არსებული ურთიერთობის ბუნებას, იქნება ეს კომერციული თუ სხვა ხასიათის. მოცემული მიზნის ლეგიტიმურობა ასევე შეიძლება შეიცვალოს დროთა განმავლობაში, რაც დამოკიდებულია მეცნიერულ და ტექნოლოგიურ განვითარებაზე, საზოგადოებისა და კულტურული დამოკიდებულებების ცვლილებაზე.[122]

2.2.4. ახალი მიზანი

მიზნის შეზღუდვის პრინციპმა უნდა უზრუნველყოს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა არ მოახდინონ პერსონალური მონაცემების „მეორადი გამოყენება“ („შემდგომი დამუშავება“), როდესაც ასეთი დამუშავება შეუთავსებელია თავდაპირველ მიზნებთან.[123] დამუშავების ნებისმიერ ახალ მიზანს, რომელიც თავდაპირველ მიზანს არ შეესაბამება, უნდა ჰქონდეს სამართლებრივი საფუძველი. კანონიერი დამუშავება შემოიფარგლება მხოლოდ საწყისი მიზნით და ნებისმიერი ახალი მიზანი საჭიროებს ცალკე სამართლებრივ საფუძველს.[124] ეს ნიშნავს, რომ მაგალითად, მონაცემთა დამმუშავებლის მიერ არასრულწლოვნის ასაკის დადასტურების მიზნით მოპოვებული მონაცემების გამოყენება სხვა მიზნით დაუშვებელია.[125]

“GDPR”-ის მიხედვით, პერსონალური მონაცემების გამოყენება სტატისტიკური მიზნებისთვის, საჯარო ინტერესებისთვის, სამეცნიერო ან ისტორიული კვლევის

---

[120] იქვე, 20.
[121] იქვე, 39.
[122] იქვე, 20.
[123] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[124] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 140, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf>, [07.08.2023].
[125] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 48, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [07.08.2023].

მიზნებისთვის ჩაითვლება თავდაპირველ მიზანთან თავსებადად, თუ დამუშავება ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით განსაზღვრულ ფარგლებში განხორციელდება. თუმცა, თუ მონაცემთა მეორადი ან შემდგომი დამუშავება არ უკავშირდება აღნიშნულ მიზნებს, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეაფასონ, შეესაბამება თუ არა შემდგომი დამუშავება თავდაპირველ მიზნებს.[126] იმისათვის, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა შეაფასოს, შეესაბამება თუ არა მონაცემთა მეორადი გამოყენება თავდაპირველ მიზნებს, მან უნდა გაითვალისწინოს:

- მონაცემების შეგროვების თავდაპირველ მიზანსა და შემდგომი დამუშავების მიზანს შორის ნებისმიერი კავშირი;
- მიზეზი, რის საფუძველზეც შეგროვდა პერსონალური მონაცემები;
- პერსონალური მონაცემების შინაარსი/ხასიათი;
- მონაცემთა სუბიექტებისთვის მონაცემთა შემდგომი დამუშავების სავარაუდო შედეგები;
- უსაფრთხოების სათანადო გარანტიების არსებობა.[127]

თუკი დამუშავება თავდაპირველ მიზანთან თავსებადად მიიჩნევა, ზემოაღნიშნული პირობების არსებობის შემთხვევაში, აღარ არის საჭირო სხვა სამართლებრივი საფუძვლის არსებობა, თუმცა, როდესაც დამუშავება არ არის თავსებადი თავდაპირველ მიზანთან, ცალკე სამართლებრივი საფუძვლის არსებობა იქნება საჭირო (მაგალითად, მონაცემთა სუბიექტის თანხმობა მონაცემთა ახალი მიზნით დამუშავების დაწყებამდე).[128]

2.2.5. საერთაშორისო სასამართლო პრაქტიკა

"Schecke"-ს[129] საქმეზე მართლმსაჯულების ევროპულმა სასამართლომ დაადგინა, რომ პერსონალური მონაცემების დამუშავების სამართლებრივი ვალდებულება უნდა იცავდეს პროპორციულობის პრინციპს, რაც ლეგიტიმური მიზნის მოთხოვნის ნაწილია.[130] სასამართლომ პროპორციულობის პრინციპის დაცვის საკითხი რამდენიმე

[126] Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells, European Data Protection Law and Practice, Second Edition, 2019, 131.
[127] GDPR, Article 6(4).
[128] იქვე, 132.
[129] CJEU, Joined Cases C- 92/ 09 and 93/ 09, Schecke [2010].
[130] საქმე ეხებოდა ევროკავშირის სასოფლო-სამეურნეო ფონდების ბენეფიციარების შესახებ პერსონალური მონაცემების გამოქვეყნებას.

საქმეში განიხილა. მათგან ერთ-ერთი ყველაზე ცნობილი *"Digital Rights Ireland"*-ის[131] საქმე იყო, რომლის ფარგლებშიც სასამართლომ დაადგინა აღნიშნული პრინციპის დაუცველობა. მან აღნიშნა, რომ დამუშავების მიზნებთან დაკავშირებით შესაბამისი მონაცემების განსაზღვრისა და მონაცემთა შენახვის ვადების დადგენის თაობაზე საჭიროა, არსებობდეს შესაბამისი კრიტერიუმები.[132]

"Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság"-ის საქმეზე, მართლმსაჯულების ევროპულმა სასამართლომ "GDPR"-ის მე-5 მუხლის პირველი პუნქტის "ხ" ქვეპუნქტით გათვალისწინებული მიზნის შეზღუდვის პრინციპი განმარტა, რომლის თანახმად, აღნიშნული დებულება არ გამორიცხავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ, ტესტირებისა და შეცდომების გასწორების მიზნებისთვის შექმნილ მონაცემთა ბაზაში იმ პერსონალურ მონაცემთა რეგისტრაციასა და შენახვას, რომლის შეგროვება და შენახვაც სხვა მონაცემთა ბაზაში მოხდა, თუკი ამგვარი დამუშავება თავსებადია თავდაპირველ მიზნებთან. გარემოებები უნდა განისაზღვროს "GDPR"-ის მე-6 მუხლის მე-4 პუნქტში მითითებული კრიტერიუმების შესაბამისად.[133]

2.2.6. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

პირის უფლება სხვათა დაკვირვების გარეშე, თავისუფლად ისარგებლოს ჰიგიენური სივრცეებით, მისი პირადი ცხოვრების ხელშეუხებლობის ერთ-ერთი მნიშვნელოვანი გარანტიაა. აღნიშნულ სივრცეებში მონაცემთა სუბიექტის მონიტორინგი ნებისმიერი მიზნით გაუმართლებელია. როდესაც საქმე არასრულწლოვანთა მონაცემების დამუშავებას ეხება, განსაკუთრებული ყურადღება უნდა მიექცეს მათ საუკეთესო ინტერესებს, რადგან მსგავსი ინფორმაციის თუნდაც შემთხვევითმა გამჟღავნებამ, შესაძლოა, მნიშვნელოვანი ზიანი მიაყენოს მას. ამდენად, სკოლებში ბავშვების დიდი მოცულობისა და განსაკუთრებით პრივატული ინფორმაციის დამუშავებასთან დაკავშირებული რისკების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახურმა საკუთარი ინიციატივით შეისწავლა სხვადასხვა საჯარო და კერძო სკოლის მიერ ჰიგიენისთვის განკუთვნილ ადგილებში ვიდეოთვალთვალის განხორციელების შესაძლო ფაქტები.

---

[131] CJEU, Joined Cases C- 293/ 12 and C- 594/ 12, Digital Rights Ireland [2014].

[132] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.

[133] CJEU, Case C-77/21, Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], §63.

სამსახურის მიერ განხორციელებული შემოწმებების ფარგლებში დადგინდა, რომ სკოლები არასრულწლოვანთა უსაფრთხოების დაცვის მიზნით ახორციელებენ ვიდეოთვალთვალს. საჯარო სკოლების შემოწმებებისას გამოიკვეთა, რომ სკოლებში უსაფრთხოების დაცვაზე პასუხისმგებელ უწყებას ასევე, წარმოადგენს სსიპ - საგანმანათლებლო დაწესებულების მანდატურის სამსახური, რომელიც სკოლასთან ერთად, ჩართულია ვიდეოთვალთვალის განხორციელების პროცესში. გამოვლინდა რამდენიმე შემთხვევა, როდესაც სკოლაში განთავსებული ვიდეოსათვალთვალო კამერების ხედვის არეალში ექცეოდა ჰიგიენისთვის განკუთვნილი სივრცე (ხელსაბანი). ზოგიერთ შემთხვევაში კი დადგინდა, რომ საპირფარეშოს შესასვლელი კარის ღიად დატოვების პირობებში, დერეფანში განთავსებული ვიდეოსათვალთვალო კამერების ხედვის არეალში ექცეოდა საპირფარეშო ოთახში არსებული ხელსაბანი სივრცე. მართალია, ჰიგიენისთვის განკუთვნილ სივრცეებს უმეტესად აქვთ კარები, რომლებიც იხურება, თუმცა, ვინაიდან არასრულწლოვნები ნაკლებად აცნობიერებენ თავისი პირადი ცხოვრების ხელშეუხებლობის დარღვევის რისკებს, შესაძლოა, აღნიშნული სივრცით სარგებლობისას, ღია დატოვონ შესასვლელი კარი და ჰიგიენისთვის განკუთვნილ სივრცეში განხორციელებული მათი ქმედებები მოხვდეს ვიდეოსათვალთვალო კამერების ხედვის არეალში. შემოწმებების ფარგლებში გამოვლინდა სამართალდარღვევების ფაქტებიც, ხოლო რიგ შემთხვევებში, ბავშვის საუკეთესო ინტერესების გათვალისწინებითა და არასრულწლოვანთა მონაცემების დარღვევების პრევენციის მიზნით, სკოლებს მიეცათ შესასრულებლად სავალდებულო დავალებები.

2.3. მონაცემთა მინიმიზაცია

2.3.1. პრინციპის არსი

მონაცემთა მინიმიზაციის პრინციპის თანახმად, მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ხორციელდება დამუშავება.[134] "GDPR"-ის მიხედვით, მონაცემთა მინიმიზაციის პრინციპის დაცვისათვის საჭიროა, რომ დამუშავებული მონაცემების მოცულობა იყოს:

[134] „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-4 მუხლის პირველი პუნქტის „გ" ქვეპუნქტი.

- *ადეკვატური:* საკმარისი დასახელებული მიზნის სათანადოდ მიღწევისთვის.[135] პერსონალური მონაცემები „ადეკვატურია“, თუ ასეთი მონაცემების კონკრეტული მიზნისთვის გამოყენება მიზანშეწონილია (მაგალითად, პირის საცხოვრებელი მისამართი არ არის მისი საკრედიტო შეფასებისთვის საჭირო ინფორმაცია);[136]
- *შესაბამისი:* აქვს გონივრული კავშირი დასახულ მიზანთან.[137] პერსონალური მონაცემები „შესაბამისია“, თუ ის იწვევს განსხვავებულ შედეგს მიზანთან დაკავშირებით (მაგალითად, მომხმარებლის მისამართი პროდუქტის მიწოდებისთვის შესაბამის ინფორმაციას წარმოადგენს);[138]
- *შემოფარგლული მხოლოდ იმით, რაც აუცილებელია:* არ დამუშავდეს უფრო მეტი მონაცემი, ვიდრე მიზნის მიღწევისთვის არის საჭირო.[139] ეს კომპონენტი გულისხმობს, რომ მიზნის მიღწევა გონივრულად შეუძლებელია კონკრეტული პერსონალური მონაცემების დამუშავების გარეშე.[140] აუცილებლობის კრიტერიუმი მოითხოვს, რომ პერსონალურ მონაცემთა შენახვის ვადა შეიზღუდოს მკაცრი მინიმუმით.[141]

პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით.[142] ამასთანავე, მონაცემთა მინიმიზაციის პრინციპი მჭიდრო კავშირშია მიზნის შეზღუდვის პრინციპთან და მისი დაცვა შესაძლებელია მხოლოდ იმ შემთხვევაში, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ კონკრეტული მიზნები მკაფიოდაა განსაზღვრული. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა, მიზნის მიღწევის აუცილებლობის დასადგენად, უნდა

---

[135] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> [18.08.2023].

[136] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

[137] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, [18.08.2023].

[138] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

[139] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/ Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, [18.08.2023].

[140] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

[141] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.

[142] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 143, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf, [18.08.2023].

გადახედოს დამუშავების ოპერაციის თითოეულ საფეხურს და მონაცემთა თითოეულ ელემენტს.[143]

მონაცემთა დამუშავებისთვის 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. ამგვარი შემოწმება უნდა განხორციელდეს ნებისმიერი დამუშავების დაწყებამდე, თუმცა მისი ჩატარება ასევე შესაძლებელია დამუშავების ციკლის ნებისმიერ მომენტში.[144]

მინიმიზაცია შეიძლება, ეხებოდეს იდენტიფიკაციის ხარისხს. 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 მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა პერსონალური მონაცემები უნდა წაშალოს ან მისი ანონიმიზირება მოახდინოს, მას შემდეგ რაც იდენტიფიკაციის საჭიროება აღარ იარსებებს. ხოლო, თუ სხვა დამუშავების აქტივობებისთვის მუდმივი იდენტიფიკაციაა საჭირო, მონაცემთა სუბიექტების უფლებების რისკის შესამცირებლად პერსონალური მონაცემების ფსევდონიმიზაცია უნდა განხორციელდეს.[145]

2.3.2. საერთაშორისო სასამართლო პრაქტიკა

მართლმსაჯულების ევროპულმა სასამართლომ *"Tele2"*-ის[146] საქმეში დაადგინა, რომ კანონმდებლობა, რომელიც ითვალისწინებს პერსონალური მონაცემების ზოგადი ხასიათის და განურჩევლად შენახვას, აჭარბებს მკაცრი აუცილებლობის საზღვრებს და არ შეიძლება გამართლებულად იქნას მიჩნეული.[147]

---

[143] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[144] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §74, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].
[145] იქვე, §75.
[146] CJEU, Joined Cases C- 203/ 15 and C- 698/ 15, Tele2 [2016].
[147] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.

"TK v Asociația de Proprietari bloc M5A-ScaraA"-ის[148] საქმეზე მართლმსაჯულების ევროპულმა სასამართლომ გააკეთა განმარტება, თუ როგორ უნდა შეფასდეს, მიიჩნევა თუ არა გარკვეული დამუშავება (ამ შემთხვევაში, ვიდეოთვალთვალის სისტემა) „აუცილებლად" მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესების დაცვის მიზნებისათვის. სასამართლომ დაადგინა, რომ დამუშავების ოპერაციის აუცილებლობა შესწავლილ უნდა იქნას მონაცემთა მინიმიზაციის პრინციპთან ერთად, რომელიც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მხოლოდ ადეკვატურ, შესაბამის და არაგადაჭარბებულ მიზნებთან დაკავშირებით ანიჭებს დამუშავების შესაძლებლობას.[149]

2.3.3. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *ერთ-ერთი საჯარო სკოლის პედაგოგი*

პერსონალურ მონაცემთა დაცვის სამსახურმა, საქართველოს განათლებისა და მეცნიერების სამინისტროს შიდა აუდიტის დეპარტამენტის შეტყობინების საფუძველზე, ერთ-ერთი სკოლის მასწავლებლის მიერ ბავშვების მონაცემების „Messenger"-ის ჯგუფებში გამჟღავნების კანონიერება შეისწავლა.

შემოწმების შედეგად გამოირკვა, რომ გაკვეთილის მიმდინარეობისას დამრიგებლის მხრიდან შშმ პირთა შესახებ გამოთქმულ შეხედულებას ერთ-ერთი მოსწავლის მძაფრი რეაქცია მოჰყვა, ვინაიდან მას და ჰყავდა შშმ პირი, რომელიც იმავე სკოლაში სწავლობდა. ინციდენტის მოგვარებაში ჩაერთო არასრულწლოვნის მშობელი, რომელმაც საქმის კურსში ჩააყენა სკოლის დირექტორი. მომხდარი ფაქტის გარშემო დაინტერესება კლასის სხვა მოსწავლეების მშობლებმაც გამოხატეს და შემთხვევა შეხვედრის ფარგლებში განიხილეს, ხოლო მოგვიანებით, არასრულწლოვნის დედამ განცხადებით სკოლის დისციპლინურ კომიტეტს მიმართა. აღნიშნული საქმისწარმოება კი დამრიგებლისთვის საყვედურის გამოცხადებით დასრულდა. ამასთან, კომიტეტის მიერ გადაწყვეტილების მიღებამდე, დამრიგებელმა Messenger-ის ორ სხვადასხვა ჯგუფში მშობლის განცხადებაზე თავისი წერილობითი პასუხის ამსახველი ფოტოები განათავსა.

შესწავლის ფარგლებში ყურადღება გამახვილდა მითითებული ჯგუფების შექმნის მიზნობრიობაზე და დადგინდა რომ ერთ-ერთში გაწევრიანებული იყო კლასის

[148] CJEU, Case C-708/18, TK v Asociația de Proprietari bloc M5A-ScaraA, [2019].
[149] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

მოსწავლეების 30-მდე მშობელი, საორგანიზაციო საკითხებზე და სასწავლო პროცესის შესახებ დამრიგებელსა და მშობლებს შორის ინფორმაციის მყისიერად გასაცვლელად. მეორე ჯგუფი კი სკოლის 30-ზე მეტი თანამშრომლისგან შედგებოდა და შექმნილი იყო დისტანციური სწავლების დროს სკოლის ადმინისტრაციასა და მასწავლებლებს შორის კომუნიკაციისთვის. დამრიგებლის მიერ ჯგუფებში გამჟღავნებული მასალა შეიცავდა მოსწავლის მშობლის განცხადების ტექსტიდან ამონარიდებს და მათზე მასწავლებლის კომენტარებს, ასევე, არაერთი პირის საუბრის შინაარსს, გაკვეთილის მიმდინარეობისას და შემდეგ გამოთქმულ მოსაზრებებს, არასრულწლოვნებისა და მათთან დაკავშირებული პირების საიდენტიფიკაციო მონაცემებს, მომხდარი ფაქტის გამო მიმდინარე დისციპლინური საქმისწარმოების ფარგლებში გამოკვლეულ და შეფასებულ კონფიდენციალურ გარემოებებს, როგორც შემთხვევასთან უშუალოდ დაკავშირებული, ისე სხვა მოსწავლის სახელსა და გვარს, მათთან კომუნიკაციის შინაარსს, მოსწავლეების დამოკიდებულებებს კონკრეტული ფაქტების მიმართ და ა.შ. პედაგოგმა განმარტა, რომ მან საკუთარი სიმართლისა და რეპუტაციის დაცვის მიზნით გაამჟღავნა აღნიშნული ინფორმაცია, რადგან განვითარებული მოვლენები თავისი პედაგოგიური მოღვაწეობისთვის დამაზიანებლად მიიჩნია.

საკითხის შეფასებისას სამსახურმა განმარტა, რომ პედაგოგიური საქმიანობის ფარგლებში მოპოვებული მონაცემები ბავშვების საუკეთესო ინტერესების პრიორიტეტულობის გათვალისწინებით უნდა დამუშავდეს. ასევე, ყურადღება გამახვილდა არასრულწლოვნების პირადი და ოჯახური ცხოვრების, ღირსების, კეთილდღეობის, პიროვნების თავისუფალი განვითარების, უსაფრთხოებისა და სხვა უფლებების დაცვაში ბავშვზე მზრუნველი პირების (მათ შორის, პედაგოგების) განსაკუთრებულ როლზე. განიმარტა, რომ თითოეულ მონაცემთა დამმუშავებელს შესაძლოა ჰქონდეს საკუთარი პროფესიული რეპუტაციის დაცვის ლეგიტიმური ინტერესი, მით უმეტეს, იმ პირობებში, როდესაც მის სამსახურებრივ ქმედებებთან დაკავშირებით დისციპლინური წარმოება მიმდინარეობს და პროფესიული საზოგადოება ამაზე ინფორმირებულია, თუმცა, ლეგიტიმური ინტერესის არსებობის პირობებშიც კი, აუცილებელია განსაკუთრებული სიფრთხილის გამოჩენა მონაცემების იმ მოცულობის შესარჩევად, რომლითაც პირი თავისი კანონიერი მიზნის მიღწევას შეძლებს, არასრულწლოვნების პირადი ცხოვრების უფლებაში ნაკლები ჩარევის სანაცვლოდ. მონაცემების გამჟღავნების კანონიერების შეფასებისას ასევე მიეთითა მართლმსაჯულების ევროპული სასამართლოს განმარტებაზე (იხ. საქმე: Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], C-131/12, 13 May 2014), რომლის თანახმად, მონაცემთა დასაცავად ფუნდამენტურად მნიშვნელოვანია, მონაცემების გამოქვეყნება არ

სცდებოდეს საჭიროების ფარგლებს (მაგ., საზოგადოების ინფორმირება). დადგინდა, რომ პედაგოგს შეეძლო პროფესიული რეპუტაციის დაცვა ნაკლები მოცულობის მონაცემების დამუშავების გზით, „Messenger“-ის ჯგუფებში მხოლოდ საკუთარი ზოგადი პოზიციის დაფიქსირებით, პერსონალურ მონაცემთა გამჟღავნებისა და გარემოებათა ზედმეტი დეტალიზების გარეშე.

სამსახურის გადაწყვეტილებით პედაგოგი ცნობილ იქნა პერსონალური მონაცემების დამუშავების მინიმიზების პრინციპის დამრღვევად, რის გამოც მას შეეფარდა ადმინისტრაციული სახდელი და დაევალა უკანონოდ გამჟღავნებული მიმართვისა და ფოტოების წაშლა. აღნიშნული მან გადაწყვეტილების ჩაბარებიდან უმოკლეს ვადაში შეასრულა.

- *ერთ-ერთი კერძო საავადმყოფო*

ჯანმრთელობასთან დაკავშირებული მონაცემები მოიცავს განსაკუთრებით მნიშვნელოვან დეტალებს ინდივიდის პირადი ცხოვრების, მისი ფსიქიკური და ფიზიკური მდგომარეობის შესახებ. პირის შესახებ მსგავსი ხასიათის მონაცემების უკანონო მოპოვება, გამჟღავნება ან სხვაგვარი დამუშავება კი შესაძლოა, გახდეს არა მხოლოდ პირადი ცხოვრების ხელშეუხებლობის დარღვევის, არამედ ღირსების შელახვის, სტიგმატიზაციის ან დისკრიმინაციის მიზეზი. ამდენად, პირის ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების კონფიდენციალურობა განსაკუთრებულ დაცვას საჭიროებს. სწორედ ამიტომ, საერთაშორისო და საქართველოს კანონმდებლობა ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დაცვის მაღალ სტანდარტს და გარანტიებს აწესებს. მოქალაქის განცხადების საფუძველზე, პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა ერთ-ერთი საავადმყოფოს დირექტორის მიერ ტელეკომპანიისთვის სატელეფონო კომენტარში გამჟღავნებული ინფორმაციის კანონიერება, რომელიც განმცხადებლის გარდაცვლილი შვილის ჯანმრთელობის მდგომარეობას შეეხებოდა (მათ შორის, თანდაყოლილ დაავადებებს, ჩატარებულ სამედიცინო პროცედურებს და ა. შ.). განმცხადებლის განმარტებით, საავადმყოფოს დირექტორის მიერ ჩამოთვლილი და საჯაროდ გახმაურებული ჯანმრთელობის პრობლემები მის გარდაცვლილ არასრულწლოვან შვილს დაძლეული ჰქონდა სატელეფონო კომენტარის გაკეთებამდე წელიწადნახევრით ადრე და სრულად იყო რეაბილიტირებული. მის მიერ ჩამოთვლილ ოპერაციებსა და ჯანმრთელობის სხვა თანდაყოლილ პრობლემებს კავშირი არ ჰქონდა განმცხადებლის შვილის მდგომარეობასთან და მის გარდაცვალებასთან.

საავადმყოფოს მიერ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში წარმოდგენილი ინფორმაციის თანახმად, სატელეფონო კომენტარის გაკეთება ემსახურებოდა საავადმყოფოს ინტერესების დაცვას, რადგან ბავშვის მშობლებისა და ოჯახის წევრების მხრიდან ხდებოდა მედიასაშუალებების მეშვეობით არაზუსტი ინფორმაციის გაჟღერება; პაციენტს კი დაბადებიდან ჰქონდა თანმხლები დაავადებები, რომლებმაც ერთობლიობაში გამოიწვიეს არასრულწლოვნის გარდაცვალება. ამდენად, საავადმყოფოს სახელით სამედიცინო დირექტორის მიერ სატელეფონო კომენტარში მითითებული ინფორმაციის გამჟღავნების მიზანი იყო საავადმყოფოს რეპუტაციის დაცვა და საზოგადოებისთვის საკითხთან დაკავშირებით სწორი ინფორმაციის მიწოდება. განცხადების განხილვის ფარგლებში სამსახურმა დაადგინა, რომ საავადმყოფოს არ ჰქონდა იმ მოცულობის მონაცემების გამჟღავნების საჭიროება, რა მოცულობითაც აღნიშნული საავადმყოფოს სამედიცინო დირექტორის მიერ სატელეფონო კომენტარში განხორციელდა. შესწავლის ფარგლებში ვერც საავადმყოფომ დაასაბუთა, რატომ იყო საჭირო დეტალური ინფორმაციის გამჟღავნება და ზოგადი მითითება ბავშვის ჯანმრთელობის მდგომარეობაზე, რატომ არ იქნებოდა საკმარისი საავადმყოფოს მიერ დასახელებული მიზნის მისაღწევად. საავადმყოფოს დირექტორის მიერ გასაჯაროებული მონაცემები არ იქნა მიჩნეული ადეკვატურად და პროპორციულად. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის გადაწყვეტილებით, საავადმყოფოს დაეკისრა პასუხისმგებლობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 44-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის (მონაცემთა დამუშავების პრინციპების დარღვევა).

2.4. ნამდვილობა და სიზუსტე

2.4.1. პრინციპის არსი

მონაცემთა სიზუსტის პრინციპი გულისხმობს, რომ მონაცემები უნდა იყოს ნამდვილი, ზუსტი და საჭიროების შემთხვევაში — განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე.[150] “GDPR” არ იძლევა „სიზუსტის“ დეფინიციას, თუმცა, პრაქტიკაში „არაზუსტი“ მონაცემი განიმარტება, როგორც არასწორი ან შეცდომაში შემყვანი ნებისმიერი სახის ფაქტი. პიროვნების

[150] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-4 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტი.

შესახებ ობიექტური ფაქტები (სახელი, დაბადების თარიღი ან საცხოვრებელი მისამართი) შეიძლება იყოს „არაზუსტი“ და შესაბამისად, ექცევა რეგულაციის მე-5 მუხლის პირველი პუნქტის “d” ქვეპუნქტის ფარგლებში. გარდა ამისა, სიზუსტის პრინციპი ვრცელდება არა მხოლოდ პიროვნების შესახებ ფაქტებზე, არამედ პროგნოზებსა და ვარაუდებზეც, რაც განსაკუთრებით აქტუალურია ავტომატური პროფილირების თანამედროვე ფორმების, ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავებისა თუ სხვა თანამედროვე სისტემებისთვის. პროგნოზები შესაძლებელია ობიექტურად არაზუსტი იყოს, თუ ისინი ეფუძნება მცდარ ფაქტებს, არასწორ დასკვნებს ან მეთოდოლოგიებს. ამ შემთხვევაში, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები და მონაცემთა დამუშავებაზე უფლებამოსილი პირები სიზუსტის პრინციპს გვერდს ვერ აუვლიან. მტკიცებულებებზე დაფუძნებული პროგნოზებისა და ვარაუდებისგან განსხვავებით, ღირებულებითი განსჯა „არაზუსტი“ არ შეიძლება იყოს, რადგან ისინი თავისი ბუნებით არ არის ობიექტურად სწორი.[151] პრაქტიკაში, მონაცემთა სიზუსტის პრინციპი ნიშნავს, რომ:

- მიღებულ უნდა იქნეს გონივრული ზომები ნებისმიერი პერსონალური მონაცემების სისწორის უზრუნველსაყოფად;
- პერსონალურ მონაცემთა წყარო უნდა იყოს ნათელი;
- მონაცემთა სიზუსტესთან დაკავშირებული ნებისმიერი გამოწვევა ყურადღებით უნდა გაანალიზდეს;
- უნდა შეფასდეს ინფორმაციის პერიოდულად განახლების საჭიროება.[152]

მონაცემთა სიზუსტის მოთხოვნების შეფასება მონაცემთა კონკრეტული გამოყენების რისკებთან და შედეგებთან მიმართებით უნდა განხორციელდეს. არაზუსტმა პერსონალურმა მონაცემებმა შეიძლება საფრთხე შეუქმნას მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს, მაგალითად, პიროვნების არასწორმა სურათმა შეიძლება გამოიწვიოს გადაწყვეტილებების შეუსაბამო საფუძველზე მიღება არაავტომატურად, ავტომატურად თუ ხელოვნური ინტელექტის მეშვეობით.[153]

[151] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[152] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/Accuracy, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>, [18.08.2023].
[153] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §78, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].

ამიტომ, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სიზუსტის პრინციპი დანერგოს დამუშავების ყველა ოპერაციაში.[154]

მონაცემთა სიზუსტე განსაკუთრებით მნიშვნელოვანია ასაკის ვერიფიკაციის, იგივე შემოწმების[155] კონტექსტში, შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა აკონტროლონ და ყურადღებით განიხილონ ნებისმიერი გამოწვევა, რომელიც დაკავშირებულია მონაცემთა სიზუსტესთან. ბავშვი, რომელსაც შეუძლია წვდომა ჰქონდეს შედარებით უფროსი ასაკის არასრულწლოვნებისა და სრულწლოვანებისთვის განკუთვნილ სერვისებზე, შეიძლება, მაგალითად, უნებლიედ დაეთანხმოს მონაცემთა დამუშავებას, რაც იწვევს არასათანადო პროფილირებას.[156] შესაბამისად, მნიშვნელოვანია, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა, რომლებიც ახორციელებენ ასაკის შემოწმებას, გაითვალისწინონ ასაკობრივ შემოწმებაზე გვერდის ავლის რისკი და სავარაუდო ზიანი.[157]

2.4.2. საზღვარგარეთის პრაქტიკა

გერმანიის ფედერალურმა ადმინისტრაციულმა სასამართლომ[158] მონაცემთა სუბიექტის მიერ მონაცემთა გასწორების უფლების[159] მოთხოვნასთან დაკავშირებულ

---

[154] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 145, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf>, [18.08.2023].

[155] მაგალითად, ასაკობრივი შეზღუდვის მქონე ფილმებზე, ფილმებზე წვდომის მიზნით, პირს შესაძლოა მოეთხოვოს ასაკის თაობაზე ინფორმაციის ელექტრონულად შევსება.

[156] "GDPR"-ის მიხედვით, პროფილირება ნიშნავს პერსონალური მონაცემების ნებისმიერი ავტომატური ფორმით დამუშავებას, რომელიც მოიცავს პერსონალური მონაცემების გამოყენებას ფიზიკურ პირთან დაკავშირებული გარკვეული პიროვნული მახასიათებლების შესაფასებლად. პროფილირება წარმოადგენს სფეროს, რომელშიც არასრულწლოვნის პერსონალური მონაცემები ექვემდებარება განსაკუთრებულ დაცვას. პროფილირება შეიძლება გამოყენებულ იქნას მიზნების ფართო სპექტრისთვის. ის შეიძლება ფართოდ იქნას გამოყენებული ონლაინ კონტექსტში, რათა მომხმარებელს შინაარსი შესთავაზოს ან მიაწოდოს. მისი გამოყენება ასევე შეიძლება მომხმარებლის ასაკის დასადგენად ან შესაფასებლად, ბავშვების დაცვის, ან დანაშაულის პრევენციის მიზნით. პროფილები ჩვეულებრივ ეფუძნება მომხმარებლის წარსულ ონლაინ აქტივობას ან დათვალიერების ისტორიას. იხ.: General Data Protection Regulation, GDPR, Article 4 (4), Recital 38; ICO, Age appropriate design: a code of practice for online services, Profiling, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/12-profiling/>, [18.08.2023].

[157] ICO, Information Commissioner's opinion: Age Assurance for the Children's Code, 2021, 26-27, <https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf>, [18.08.2023].

[158] BVerwG (Germany), 6 C 7.20, [2022], <https://gdprhub.eu/index.php?title=BVerwG_-_6_C_7.20>, [18.08.2023].

[159] GDPR, Art. 16.

საქმეზე დაადგინა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს არ შეიძლება მოეთხოვოს ისეთი მონაცემების შეყვანა და შემდგომი დამუშავება, რომელთა სიზუსტის საკმარისი სარწმუნოობით დადგენა შეუძლებელია. ასეთ შემთხვევაში, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი დაარღვევს "GDPR"-ის მე-5 მუხლის პირველი პუნქტის "d" ქვეპუნქტსა და ამავე მუხლის მე-2 პუნქტს. შესაბამისად, გასაახლებელი მონაცემების სიზუსტესთან დაკავშირებით მტკიცების ტვირთი მონაცემთა სუბიექტს ეკისრება. ვინაიდან, მოცემული საქმის მიხედვით, მონაცემთა სუბიექტმა ვერ შეძლო მისი დაბადების თარიღის დადასტურება, სასამართლომ საკითხი მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის სასარგებლოდ გადაწყვიტა.[160]

2.4.3. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *სსიპ - განათლების მართვის საინფორმაციო სისტემის შემოწმება*

პერსონალურ მონაცემთა დაცვის სამსახურმა საკუთარი ინიციატივით შეისწავლა სსიპ - განათლების მართვის საინფორმაციო სისტემის მიერ ზოგადი განათლების მართვის საინფორმაციო სისტემის საშუალებით სსიპ - თბილისის კლასიკური გიმნაზიის მოსწავლეების პერსონალური მონაცემების დამუშავების კანონიერება.

აღსანიშნავია, რომ ზოგადი განათლების მართვის საინფორმაციო სისტემაში (შემდგომში - eSchool) აისახება საქართველოს ტერიტორიაზე მოქმედი საჯარო და კერძო ზოგადსაგანმანათლებლო დაწესებულების თითოეული მოსწავლის მნიშვნელოვანი მოცულობის პერსონალური, მათ შორის, განსაკუთრებული კატეგორიის მონაცემები (მაგ.: სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, მოქალაქეობა, მისამართი, კლასი, სსსმ მოსწავლის, სოციალურად დაუცველი პირის, შშმ პირის, დევნილის, ლტოლვილის, ჰუმანიტარული, თავშესაფრის მაძიებლის სტატუსები და სხვა). ამასთან, კანონმდებლობით დადგენილი წესით, eSchool-ში, ზოგადსაგანმანათლებლო დაწესებულების მონაწილეობით და სსიპ - განათლების მართვის საინფორმაციო სისტემის (შემდგომში - საინფორმაციო სისტემა) ტექნიკური მხარდაჭერით, ელექტრონულად მიმდინარეობს სხვადასხვა პროცესები: საგანმანათლებლო დაწესებულებაში მოსწავლის ჩარიცხვა, ამორიცხვა, სტატუსის შეჩერება და აღდგენა, კლასის დაძლევა, მობილობა, საგაკვეთილო ცხრილის შექმნა. აქვე უნდა აღინიშნოს, რომ სსიპ - თბილისის კლასიკური გიმნაზია (შემდგომში -

[160] GDPRhub, GDPR Decision Database, <https://gdprhub.eu/index.php?title=BVerwG_-_6_C_7.20>, [18.08.2023].

გიმნაზია) არის ქალაქ თბილისის მუნიციპალიტეტში მოქმედი ერთ-ერთი მრავალრიცხოვანი ზოგადსაგანმანათლებლო დაწესებულება (შემოწმების დროისათვის გიმნაზიაში სწავლობდა 2181 მოსწავლე).

შემოწმების ფარგლებში გამოიკვეთა, რომ საინფორმაციო სისტემა eSchool-ში კანონის მე-4 მუხლის „გ“ ქვეპუნქტის დარღვევით, მონაცემთა დამუშავების კანონიერი მიზნის არაპროპორციული მოცულობით, სათანადო საჭიროებისა და ლეგიტიმური მიზნის გარეშე ამუშავებდა, მოსწავლეების ფოტოსურათებს, რომლებიც საინფორმაციო სისტემას გადაეცემოდა სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ბაზიდან. აქვე ნიშანდობლივია, რომ „ზოგადი განათლების მართვის საინფორმაციო სისტემის შექმნის და ადმინისტრირების წესისა და პირობების დამტკიცების შესახებ“ საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის მინისტრის 2021 წლის 9 თებერვლის №08/ნ ბრძანების მე-2 მუხლის მე-4 პუნქტი ამომწურავად განსაზღვრავს სსიპ – სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ელექტრონულ ბაზაში დაცულ მონაცემთა იმ ჩამონათვალს, რომელიც eSchool-ში ასახულ ფიზიკურ პირთა იდენტიფიცირების/ვერიფიკაციის ან/და მათი მოქალაქეობრივი მდგომარეობის დადგენის/გადამოწმების მიზნით, საინფორმაციო სისტემამ შეიძლება მიიღოს და დაამუშაოს, თუმცა ხსენებულ ჩამონათვალში არ არის შეტანილი ფოტოსურათი.

შემოწმების ფარგლებში გამოიკვეთა, რომ eSchool-ში გიმნაზიის მოსწავლეების სოციალურად დაუცველი პირის, იძულებით ადგილნაცვალი პირის და შშმ პირის სტატუსების შესახებ ინფორმაცია აისახებოდა შემდეგი წესით: არასრულწლოვნის გიმნაზიაში ჩარიცხვის მოთხოვნით მშობლის მიერ განცხადების წარდგენისას, მას განემარტებოდა, რომ სურვილის შემთხვევაში გააჩნდა შესაძლებლობა eSchool-ში ინფორმაციის შეტანის მიზნებისთვის გიმნაზიისთვის წარედგინა შესაბამისი სტატუსების დამადასტურებელი დოკუმენტები, რის საფუძველზეც გიმნაზია არასრულწლოვნის შესაბამის სტატუს(ებ)ს აღრიცხავდა eSchool-ში. ამასთან, მშობლებს ხსენებული მონაცემების წარდგენის შესახებ ინფორმაცია მიეწოდებოდათ მხოლოდ ზემოთ დასახელებული განცხადების წარდგენისას და შემდეგ მათთან აღარ ხდებოდა კომუნიკაცია იმის დასადგენად, გარკვეული პერიოდის შემდგომ ხომ არ შეიცვალა სტატუსები.

ნიშანდობლივია, რომ იმდენად, რამდენადაც eSchool-ში სოციალურად დაუცველი პირის, იძულებით ადგილნაცვალი პირის და შშმ პირის თაობაზე ინფორმაცია შეიტანებოდა მხოლოდ გიმნაზიის იმ მოსწავლეებთან დაკავშირებით, რომელთა მშობლებმაც ნებაყოფლობით წარადგინეს ხსენებული სტატუსის დამადასტურებელი

დოკუმენტები, არსებობს მნიშვნელოვანი ალბათობა იმისა, რომ რომელიმე ეს სტატუსი შეიძლება გააჩნდეთ იმ მოსწავლეებსაც, რომელთა eSchool-ის პროფილშიც ხსენებული ველები არ არის მონიშნული. მეორე მხრივ, გიმნაზიის მოსწავლეების შესაბამისი სტატუსის მონიშვნის შემდგომ არ ხდებოდა იმის დადგენა, გარკვეული პერიოდის შემდეგ ხომ არ შეიცვალა დასახელებული სტატუსები და შესაბამისად, არ ახლდებოდა მონაცემები. აღნიშნული კი, ქმნის იმის ალბათობას, რომ მოსწავლეებს, რომლებსაც eSchool-ში მონიშნული აქვთ სოციალურად დაუცველი პირის, იძულებით ადგილნაცვალი პირის და შშმ პირის სტატუსის აღმნიშვნელი ველები, არ გააჩნდეთ ეს სტატუსები. ყოველივე ზემოხსენებულიდან გამომდინარე, გიმნაზიის მოსწავლეების სოციალურად დაუცველი პირის, იძულებით ადგილნაცვალი პირის და შშმ პირის სტატუსის თაობაზე ინფორმაციის აღრიცხვისა და შენახვის მიდგომა არ უზრუნველყოფს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის კანონის მე-4 მუხლის „დ“ ქვეპუნქტის მოთხოვნათა შესაბამისად მოსწავლეების სწორი და განახლებული მონაცემების დამუშავებას.

შემოწმების ფარგლებში დადგინდა, რომ eSchool-ში აღირიცხება გიმნაზიის მოსწავლეების კომპიუტერულ მოწყობილობებსა და ინტერნეტზე ხელმისაწვდომობასთან დაკავშირებით გამოკითხვის შედეგები. საინფორმაციო სისტემის მიერ წარმოდგენილი განმარტებით, აღნიშნული ინფორმაციის დამუშავება ემსახურება დისტანციურ სწავლებაზე გადასვლის საჭიროების დადგომის შემთხვევაში, სათანადო ღონისძიებების დაგეგმვასა და განხორციელებას, თუმცა ვერ იქნა დაზუსტებული, თუ რა მიზნით ხდება მოსწავლის მიერ დისტანციური სწავლების შესაძლებლობასთან დაკავშირებული გამოკითხვის ძველი (წინა წლების) შედეგების შენახვა.

შემოწმების დროისათვის, მოსწავლეების აქტიური სტატუსის შეწყვეტის შემდეგ, eSchool-ში მათი მონაცემების სრული დაარქივება (eSchool-ზე დაშვების მქონე პირთა მხრიდან ამ მონაცემებზე წვდომის შეზღუდვა) არ ხდებოდა და საინფორმაციო სისტემის განმარტებით, აღნიშნული ფუნქციონალის გააქტიურება იგეგმებოდა 2026 წლის თებერვლამდე. ამ პერიოდამდე ასევე იგეგმებოდა საინფორმაციო სისტემის უფროსის იმ ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტის გამოცემაც, რომელიც განსაზღვრავდა დაარქივებულ მონაცემებზე წვდომის უფლებამოსილების მქონე პირებს. ნიშანდობლივია, რომ მონაცემთა დაარქივება ემსახურება სხვადასხვა პირის მხრიდან მონაცემებზე წვდომის მინიმიზაციას, კერძოდ, eSchool-ზე დაშვების მქონე სხვადასხვა დაწესებულებების თანამშრომელთა იმ მონაცემებზე წვდომის შეზღუდვას, რომლებზე წვდომაც მათ შესაძლოა არ ესაჭიროებოდეთ დაკისრებული უფლებამოსილებების შესრულებისთვის. ამდენად,

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მიზანშეწონილად იქნა მიჩნეული საინფორმაციო სისტემამ გაუმართლებელი დაყოვნების გარეშე, შეზღუდულ ვადებში შეაფასოს eSchool-ში დამუშავებული აქტიური სტატუსის არ მქონე მოსწავლეთა მონაცემებზე სისტემის სხვადასხვა სუბიექტების თანამშრომელთა მხრიდან წვდომის საჭიროება და იმ თანამშრომლებს, რომლებსაც არ გააჩნიათ აღნიშნული საჭიროება, შეუზღუდოს დასახელებულ მონაცემებზე დაშვება.

შემოწმების ფარგლებში ასევე დადგინდა, რომ eSchool-ის სისტემის მუშაობისათვის გამოყენებულ მონაცემთა ბაზასთან, მონაცემთა ბაზების მართვის სისტემიდან პირდაპირი წვდომის საშუალებით მონაცემების დამუშავების პროცესში არ აღირიცხებოდა მონაცემების წარმატებული დათვალიერება, რაც არ შეესაბამება კანონის მე-17 მუხლის მოთხოვნებს.

გიმნაზიის ადგილზე შემოწმების დროისათვის, გიმნაზიის საქმისმწარმოებლები და საინფორმაციო მენეჯერები eSchool-ში სარგებლობდნენ საერთო მომხმარებლის ანგარიშებით. საქმის მასალებში წარმოდგენილი მტკიცებულებებით არ დადასტურდა, გიმნაზიის მიერ საინფორმაციო სისტემისთვის მიმართვა ყველა საქმისმწარმოებლისა და საინფორმაციო მენეჯერისთვის eSchool-ში შექმნილიყო განპიროვნებული ანგარიშები, რაც კანონის მე-17 მუხლის მოთხოვნათა დარღვევას წარმოადგენს.

შემოწმების შედეგად მონაცემთა დამუშავების პრინციპების დარღვევისა და მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრულებლობისთვის საინფორმაციო სისტემა ცნობილ იქნა სამართალდამრღვევად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 44-ე მუხლით და 46-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევების ჩადენაში, ხოლო გიმნაზია მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრულებლობისთვის ცნობილ იქნა ამავე კანონის 46-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში. ამასთან, საინფორმაციო სისტემას დაევალა: eSchool-ში მოსწავლეების ფოტოსურათების დამუშავების შეწყვეტა; მონაცემთა უსაფრთხოების დაცვისთვის იმგვარი ორგანიზაციული და ტექნიკური ზომების მიღება, რომელიც უზრუნველყოფს eSchool-ის მონაცემთა ბაზაში (ბაზაზე პირდაპირი წვდომის დროს) არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვას; eSchool-ში დამუშავებული აქტიური სტატუსის არმქონე მოსწავლეთა მონაცემებზე სხვადასხვა დაწესებულებების თანამშრომელთა მხრიდან წვდომის საჭიროების შეფასება და იმ თანამშრომლებისთვის, რომლებსაც არ გააჩნიათ აღნიშნული საჭიროება, დასახელებულ მონაცემებზე დაშვების შეზღუდვა; შეფასება,

არსებობს თუ არა საჭიროება შენახული იქნას eSchool-ში მოსწავლეთა მიერ დისტანციური სწავლების შესაძლებლობასთან დაკავშირებული გამოკითხვის ძველი (წინა წლების) შედეგები, ასევე, აქტიური სტატუსის არმქონე მოსწავლეების შესახებ ხსენებული ინფორმაცია და შენახვისთვის საჭირო შესაბამისი ვადის ამოწურვის შემდგომ დასახელებული მონაცემების წაშლა, განადგურება ან/და პირის იდენტიფიცირების გამომრიცხავი ფორმით შენახვა. საინფორმაციო სისტემას და გიმნაზიას დაევალათ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „დ“ ქვეპუნქტის მოთხოვნების სრულყოფილად დაცვისთვის, უზრუნველყონ გიმნაზიის მოსწავლეების სოციალურად დაუცველი პირის, შეზღუდული შესაძლებლობების მქონე პირისა და იძულებით ადგილნაცვალი პირის სტატუსების შესახებ ინფორმაციის იმგვარი წესით დამუშავება, რაც უზრუნველყოფს ხსენებულ მონაცემთა ნამდვილობასა და სიზუსტეს.

2.5. შენახვის ვადის შეზღუდვა

2.5.1. პრინციპის არსი

შენახვის ვადის შეზღუდვის პრინციპი გულისხმობს, რომ მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად.[161] მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა წინასწარ უნდა აცნობოს მონაცემთა სუბიექტს შენახვის პერიოდის შესახებ, ასევე, უნდა უზრუნველყოს პრინციპთან შესაბამისობის დემონსტრირება. შესაბამისად, შენახვის ვადები უნდა განისაზღვროს ორგანიზაციის შიგნით, მონაცემთა დამუშავების დაწყებამდე.[162]

პერსონალურ მონაცემთა დამუშავების პროცესში შენახვის ვადის შეზღუდვა მნიშვნელოვანია, ვინაიდან როდესაც მონაცემები ინახება გადაჭარბებული ვადებით, იგი ხდება არასაჭირო, შესაბამისად, აღარ არსებობს მონაცემთა დამუშავების კანონიერი საფუძველი. უფრო პრაქტიკული თვალსაზრისით კი, პერსონალურ მონაცემთა შენახვა იმაზე მეტი ვადით, ვიდრე აუცილებელია, საჭიროებს შენახვასთან

[161] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტი. “GDPR” მე-5 მუხლის პირველი პუნქტის „e“ ქვეპუნქტისა და ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის მე-5 მუხლის მე-4 პუნქტის „e“ ქვეპუნქტის თანახმად, პერსონალური მონაცემები უნდა შეინახოს ისეთი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას არაუმეტეს იმ დროით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნებისთვის.

[162] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

და უსაფრთხოებასთან დაკავშირებულ ზედმეტ ხარჯებს. ამასთანავე, რაც უფრო დიდი ვადით ინახება მონაცემები, მით უფრო მეტი შეიძლება იყოს მათზე მონაცემთა სუბიექტის მიერ მონაცემთა მოთხოვნისა და აღნიშნული ინფორმაციის წაშლის მოთხოვნის განცხადებები.[163]

პერსონალურ მონაცემთა შენახვის ვადების სწორად დადგენა შესაძლებელია შემდეგი ფაქტორების დახმარებით:

- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს გაცხადებული მიზან(ებ)ი. მონაცემთა შენახვა შესაძლებელია მანამ, სანამ ერთ-ერთი მიზნის მისაღწევად მაინც არის იგი საჭირო, თუმცა მონაცემთა შენახვა არ იქნება გამართლებული „ყოველი შემთხვევისთვის“ ან თუ ძალიან მცირე შესაძლებლობა არსებობს, რომ ისინი გამოდგება;
- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განსაზღვროს სჭირდება თუ არა სამართლებრივი ურთიერთობის შესახებ (მაგალითად, არასრულწლოვნისთვის მომსახურების მიწოდება) ჩანაწერების შენახვა მას შემდეგ, რაც სამართლებრივი ურთიერთობა დასრულდება. შესაძლებელია, ყველა მონაცემის წაშლა არ იყოს გამართლებული სამართლებრივი ურთიერთობის დასრულების შემდეგ და ინფორმაცია ან მის შესახებ მცირე დეტალები ინახებოდეს სამართლებრივი ურთიერთობის არსებობის/დასრულების დასადგენად;
- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს სჭირდება თუ არა ინფორმაციის შენახვა შესაძლო სამართლებრივი ინტერესების დასაცავად. მას შეუძლია წაშალოს ინფორმაცია, რომელიც არ არის რელევანტური შესაბამისი სამართლებრივი ინტერესების დასაცავად. თუ მონაცემთა შენახვის სხვა რაიმე მიზეზი არ არსებობს, პერსონალური მონაცემები უნდა წაიშალოს, როდესაც ასეთი სამართლებრივი დაცვის საჭიროება აღარ შეიძლება გაჩნდება;
- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს მის მიმართ მონაცემთა შენახვასთან დაკავშირებული სამართლებრივი მოთხოვნები. არსებობს რეგულაციები და სახელმძღვანელო მითითებები ზოგიერთი კატეგორიის მონაცემთა შენახვის შესახებ, როგორიცაა ინფორმაცია საგანმანათლებლო, საგადასახადო და აუდიტის მიზნებისთვის, ჯანმრთელობისა და უსაფრთხოების შესახებ. თუ ინფორმაციას მონაცემთა

[163] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/The principles/Storage limitation, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/#why_storage_limitation>, [18.08.2023].

დამმუშავებელი ამგვარი მოთხოვნებიდან გამომდინარე ინახავს, ნაკლებად არის შესაძლებელი, რომ მონაცემები ინახება გადაჭარბებული ვადით;

- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს მისი საქმიანობის სფეროს შესაბამისი სტანდარტები და ინსტრუქციები. თუმცა, ასეთი სტანდარტების არსებობა თავისთავად არ ადასტურებს, რომ დაცულია შენახვის ვადის შეზღუდვის პრინციპი და მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მოუწევს მათი მიზანშეწონილობის დასაბუთება;
- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ვადების განსაზღვრისას, უნდა იხელმძღვანელოს პროპორციული მიდგომით, რათა დაბალანსდეს მისი საჭიროებები და შენახვის ვადების გავლენა ბავშვის პირად ცხოვრებასა და მის საუკეთესო ინტერესზე. ასევე, გასათვალისწინებელია, რომ შენახვის ვადები ყოველთვის უნდა იყოს სამართლიანი და კანონიერი.[164]

2.5.2. საერთო სასამართლო პრაქტიკა

ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეზე: "*Aycaguer v. France*" აღნიშნა, რომ იმ დროისათვის ქვეყანაში არ არსებობდა დებულებები, რომლის მიხედვითაც შენახვის ვადები დამოკიდებული იქნებოდა პირის მიერ ჩადენილი დანაშაულის ბუნებასა და სიმძიმეზე. მონაცემთა ბაზაში დნმ-ის პროფილების შენახვასთან დაკავშირებული რეგულაციები მონაცემთა სუბიექტებს არ ანიჭებდა სათანადო დაცვას, მონაცემთა შენახვის ხანგრძლივობის გათვალისწინებით და ასევე იმ ფაქტის გამო, რომ მონაცემები არ შეიძლებოდა წაშლილიყო. შესაბამისად, ევროპულმა სასამართლომ დაადგინა, რომ სახელმწიფოში მოქმედი რეგულაციები ვერ უზრუნველყოფდა დაპირისპირებულ საჯარო და კერძო ინტერესებს შორის სამართლიანი ბალანსის დაცვას.[165]

საქმეზე "*Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság"*, მართლმსაჯულების ევროპულმა სასამართლომ "GDPR"-ის მე-5 მუხლის პირველი პუნქტის "e" ქვეპუნქტით გათვალისწინებული შენახვის ვადის შეზღუდვის პრინციპი განმარტა. კერძოდ, აღნიშნული პრინციპი გამორიცხავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ სხვა მიზნისთვის ადრე შეგროვებული მონაცემების ტესტირებისა და შეცდომების გასწორების მიზნებისთვის შექმნილ მონაცემთა ბაზაში დამუშავებას ტესტირებისა და შეცდომების გასწორებისათვის საჭირო ვადაზე მეტი ვადით.[166]

---

[164] იქვე.

[165] Case of Aycaguer v. France, [2017] ECHR App. No. 8806/12, §§42-43, 45, 47.

[166] CJEU, Case C-77/21, Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], §63.

2.5.3. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა, და ზარალებულთა დახმარების სააგენტოს შემოწმება*

„სოციალური რეაბილიტაციისა და ბავშვზე ზრუნვის 2023 წლის სახელმწიფო პროგრამის დამტკიცების შესახებ“ საქართველოს მთავრობის 2023 წლის 21 თებერვლის №69 დადგენილების საფუძველზე განსახორციელებელ ერთ-ერთ ქვეპროგრამას წარმოადგენს ბავშვთა რეაბილიტაცია/აბილიტაციის ქვეპროგრამა. აღნიშნული ქვეპროგრამის ფარგლებში, შშმ ბავშვებისა და მათი ოჯახების გაძლიერების, ბავშვების ფიზიკური და ინტელექტუალური ფუნქციური პოტენციალის რეალიზების, ზოგადი ჯანმრთელობის, ცხოვრების ხარისხის გაუმჯობესებისა და ინკლუზიური განვითარების პროცესის ხელშეწყობის მიზნით ხორციელდება შესაბამის სპეციალისტთა გუნდის მიერ ბენეფიციარისთვის ინდივიდუალური რეაბილიტაცია/აბილიტაციის გეგმის შედგენა და მისი განხორციელება (მათ შორის, თერაპიული ინტერვენციის და სხვა სახის თერაპიების განხორციელების გზით). ტრეფიკინგის სააგენტო, არასრულწლოვნის კანონიერი წარმომადგენლის მიერ ქვეპროგრამაში ჩართვის მოთხოვნით წარდგენილი განცხადების საფუძველზე ამუშავებს შშმ არასრულწლოვნების დიდი მოცულობით პერსონალურ მონაცემებს (მაგალითად, ჯანმრთელობის მდგომარეობის, შშმ სტატუსის და რეინტეგრაციის შემწეობის თაობაზე ინფორმაციას, სოციალურად დაუცველი პირის სტატუსს, სარეიტინგო ქულას და სხვა). შემოწმება მოიცავდა ტრეფიკინგის სააგენტოს მიერ ზემოხსენებულ ქვეპროგრამაში ჩართვის მოთხოვნით ქალაქ თბილისის საქალაქო ცენტრში წარდგენილი განცხადებების განხილვის მიზნით ელექტრონული სისტემების საშუალებით პერსონალური მონაცემების დამუშავების კანონიერების შესწავლას.

შემოწმების ფარგლებში გამოიკვეთა, რომ ბავშვთა რეაბილიტაცია/აბილიტაციის ქვეპროგრამის განხორციელების ფარგლებში მონაცემები მუშავდება ტრეფიკინგის სააგენტოს საქმისწარმოების ელექტრონული პროგრამისა და სპეციალური ვებ-პორტალის საშუალებით. ამასთან, აღნიშნული სისტემების ადმინისტრირების პროცესში ტრეფიკინგის სააგენტო იყენებს უფლებამოსილი პირის, კერძოდ სსიპ - ინფორმაციული ტექნოლოგიების სააგენტოს მომსახურებას. აღნიშნული სააგენტო, მათ შორის, ახორციელებს სისტემების ტექნიკურ მხარდაჭერას და სააგენტოს დავალებების შესაბამისად, მომხმარებელთა მართვას.

ვებ-პორტალის რეაბილიტაცია/აბილიტაციის მოდულში სხვა სახის ინფორმაციასთან ერთად გათვალისწინებულია ინფორმაციის შევსება ქვეპროგრამის ბენეფიციარის კანონიერი წარმომადგენლის დასაქმების თაობაზე, ასევე ბენეფიციარისთვის სხვა სახის დაფინანსების არსებობის შესახებ. შემოწმების ფარგლებში გამოიკვეთა, რომ ხსენებული მონაცემები არ არის მნიშვნელოვანი და არ გამოიყენება რეაბილიტაცია/აბილიტაციის ქვეპროგრამის განხორციელების ფარგლებში. მიუხედავად იმისა, რომ შემოწმების ფარგლებში აღნიშნული ინფორმაციის პორტალში შენახვის ფაქტი არ გამოვლინდა, სამსახურმა განმარტა, რომ შესაბამისი ველების არსებობის პირობებში, არსებობს საფრთხე განაცხადის რეგისტრაციის განმახორციელებელმა პირებმა სხვადასხვა განმცხადებლებთან მიმართებით შეავსონ ისინი, რის შედეგადაც ადგილი ექნება ქვეპროგრამის განხორციელების მიზნის და საჭიროების შეუსაბამო მოცულობით მონაცემების დამუშავებას. შესაბამისად, სამსახურმა მიზანშეწონილად მიიჩნია ვებ-პორტალის რეაბილიტაცია/აბილიტაციის მოდულიდან ამოღებული იქნას ველები სახელწოდებით - „დასაქმება“ და „სხვა სახის დაფინანსება“.

შემოწმებისას ასევე გამოიკვეთა, რომ ვებ-პორტალში რეაბილიტაცია/აბილიტაციის მოდულში მონაცემები ინახება მუდმივად, თუმცა ტრეფიკინგის სააგენტოს მიერ არ არის შეფასებული მათი შენახვის საჭიროებიდან გამომდინარე შენახვის ვადა. ამდენად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „ე“ ქვეპუნქტით გათვალისწინებული მონაცემთა დამუშავების პრინციპის დაცვის უზრუნველყოფისთვის ტრეფიკინგის სააგენტოს დაევალა მონაცემთა შენახვის საჭიროების/კანონმდებლობით დადგენილი მოთხოვნების გათვალისწინებით, მონაცემთა დამუშავების მიზნის პროპორციულად განსაზღვროს ხსენებული ვადები.

ტრეფიკინგის სააგენტოს მიერ რამდენიმე ეპიზოდში იქნა დარღვეული ვებ-პორტალის და საქმისწარმოების ელექტრონული პროგრამის საშუალებით ქვეპროგრამის ფარგლებში მონაცემების დამუშავებისას უსაფრთხოების დასაცავად საჭირო ორგანიზაციულ-ტექნიკური ზომების მიღების ვალდებულება, კერძოდ:

- ვებ-პორტალში აქტიური ანგარიშის მქონე 143 (ასორმოცდასამი) პირთან დაკავშირებით, ტრეფიკინგის სააგენტომ ვერ დააზუსტა თუ ვინ არიან ისინი და რა უფლებამოსილების ფარგლებში ესაჭიროებათ ქვეპროგრამის ფარგლებში დამუშავებულ ინფორმაციაზე დაშვება. აქვე აღსანიშნავია, რომ ვებ-პორტალზე ამ პირების მხრიდან წვდომა შესაძლებელი იყო ინტერნეტის ღია ქსელიდან, საიდანაც საჭიროების შემთხვევაში მათ ჰქონდათ პაროლის

აღდგენის შესაძლებლობაც. დასახელებულ პორტალზე დაშვება ასევე გააჩნდათ სააგენტოს ყოფილ თანამშრომლებსაც;

- ვებ-პორტალში რეაბილიტაცია/აბილიტაციის მოდულზე დაშვების მქონე სააგენტოს თანამშრომელთა ნაწილს, მათი საქმიანობის ფარგლებში, დაკისრებული ფუნქციების შესასრულებლად არ ესაჭიროებოდა მოდულში დამუშავებულ სრულ ინფორმაციაზე წვდომა;
- საქმისწარმოების ელექტრონულ პროგრამისა და ვებ-პორტალის მონაცემთა ბაზის სერვერებზე პირდაპირი წვდომის შემთხვევაში, ასევე ვებ-პორტალში მონაცემების დამუშავების შესახებ ინფორმაცია არასრულად აღირიცხებოდა. ამასთან, ხსენებულ მონაცემთა ბაზაზე წვდომისთვის უფლებამოსილი თანამშრომლები სარგებლობდნენ საერთო მომხმარებლით;
- საქმისწარმოების ელექტრონულ პროგრამაში პაროლის სირთულე და სიმბოლოების რაოდენობა წინასწარ არ იყო განსაზღვრული და შესაძლებელი იყო ნებისმიერი, მათ შორის, მარტივი პაროლის დაყენება;
- განმცხადებლების ქვეპროგრამაში ჩართვის თაობაზე გადაწყვეტილების მიღების, ასევე მათთვის ქვეპროგრამაში ჩართვაზე უარის განმარტების მიზნებისთვის, სააგენტოს თითოეულ ტერიტორიულ ერთეულს საქმისწარმოების ელექტრონული პროგრამის გამოყენებით ეგზავნებოდა განმცხადებლების ერთიანი სიები. შედეგად ხსენებული სიები ხელმისაწვდომი ხდებოდა სააგენტოს, მათ შორის, ისეთი თანამშრომლისთვისაც რომელსაც არ ჰქონდა მათში მითითებულ სრულ ინფორმაციაზე დაშვების საჭიროება;
- ვებ-პორტალში მომსახურების მიმწოდებელი სამედიცინო დაწესებულებებისთვის შექმნილი სამსახურებრივი ანგარიშები არ იყო განპიროვნებული ამავე ორგანიზაციების თანამშრომლებზე. ტრეფიკინგის სააგენტოს და სსიპ - ინფორმაციული ტექნოლოგიების სააგენტოსთვის არ იყო ცნობილი, იმ თანამშრომელთა ვინაობა, რომლებიც იყენებენ ამ ორგანიზაციებისთვის შექმნილ მომხმარებლებს.

შემოწმების ფარგლებში გამოიკვეთა, რომ ტრეფიკინგის სააგენტოს მიერ სსიპ - ინფორმაციული ტექნოლოგების სააგენტოს ინფორმაცია მიეწოდა რამდენიმე თანამშრომლის გათავისუფლების თაობაზე. აღნიშნული მიმართვებიდან 2 (ორი) შემთხვევაში სპეციალურად იყო მოთხოვნილი თანამშრომლებზე განპიროვნებული მომხმარებლების ვებ-პორტალიდან გამორთვაც, თუმცა უფლებამოსილმა პირმა არ

უზრუნველყო ხსენებული მოთხოვნის შესრულება, რის შედეგადაც შემოწმების დროისათვის ხსენებული მომხმარებლები კვლავ აქტიური იყო.

ზემოხსენებულიდან გამომდინარე, ტრეფიკინგის სააგენტოს პასუხისმგებლობა დაეკისრა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 46-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენისთვის, ხოლო სსიპ - ინფორმაციული ტექნოლოგიების სააგენტოს - ამავე კანონის 52-ე მუხლის პირველი პუნქტით გათვალისწინებული სამართალდარღვევის ჩადენისთვის. მონაცემთა უსაფრთხოების სამომავლოდ უზრუნველყოფის მიზნით ტრეფიკინგის სააგენტოს და სსიპ - ინფორმაციული ტექნოლოგიების სააგენტოს დაევალათ ვებ-პორტალში რეაბილიტაცია/აბილიტაციის მოდულში, ასევე ვებ-პორტალის და საქმისწარმოების ელექტრონული პროგრამის მონაცემთა ბაზებში (ბაზაზე პირდაპირი წვდომის დროს) არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა; იმგვარი ორგანიზაციულ-ტექნიკური ზომების მიღება, რის შედეგადაც ხსენებულ მონაცემთა ბაზებზე უფლებამოსილი პირები მოახდენენ, მხოლოდ მათზე განპიროვნებული სათანადო პაროლით დაცული მომხმარებლების ანგარიშებით; ვებ-პორტალის რეაბილიტაცია/აბილიტაციის მოდულით ქვეპროგრამის ფარგლებში დამუშავებულ მონაცემებზე მხოლოდ იმ პირთა დაშვება, რომელთაც აღნიშნული მონაცემები ესაჭიროებათ მათზე დაკისრებული ფუნქცია-მოვალეობების განსახორციელებლად; ამავე მოდულზე წვდომის საჭიროების მქონე თითოეულ თანამშრომელს დაშვება მხოლოდ კანონმდებლობით მისთვის დაკისრებული უფლებამოსილებების განსახორციელებლად საჭირო ინფორმაციაზე; საქმისწარმოების ელექტრონული პროგრამაზე თანამშრომლების დაშვება მხოლოდ სათანადო სირთულის, კომპლექსური პაროლის გამოყენებით. ტრეფიკინგის სააგენტოს დამატებით დაევალა, მის თითოეულ ტერიტორიულ ერთეულს განმცხადებლების ქვეპროგრამაში ჩართვაზე გადაწყვეტილების მიღების, ასევე მათთვის ქვეპროგრამაში ჩართვაზე უარის განმარტების მიზნებისთვის, საქმისწარმოების ელექტრონული პროგრამის გამოყენებით გადაეგზავნოს მხოლოდ იმ განმცხადებელთა სიები, რომლებთან დაკავშირებით გადაწყვეტილების მიღება/განმცხადებლებისთვის ქვეპროგრამაში ჩართვაზე უარის განმარტება უნდა უზრუნველყოს შესაბამისმა ტერიტორიულმა ერთეულმა.

2.6. მონაცემთა უსაფრთხოება

2.6.1. პრინციპის არსი

მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნას ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ანდა დაზიანებისგან.[167] პერსონალური მონაცემების უსაფრთხოება მოითხოვს შესაბამის ზომებს, რომელთა მიზანია: მონაცემთა უსაფრთხოების დარღვევის — ინციდენტის თავიდან აცილება და მართვა; მონაცემთა დამუშავების ამოცანების სწორად შესრულება და სხვა პრინციპებთან შესაბამისობის უზრუნველყოფა; და პირთა უფლებების ეფექტიანად განხორციელების ხელშეწყობა.[168] უსაფრთხოების ზომები უნდა მოიცავდეს არა მხოლოდ კიბერუსაფრთხოებას, არამედ ფიზიკურ და ორგანიზაციულ უსაფრთხოებასაც. ორგანიზაციებმა რეგულარულად უნდა შეამოწმონ, არის თუ არა მათი უსაფრთხოების ზომები განახლებული და ეფექტიანი.[169] შესაბამისად, მონაცემთა უსაფრთხოების სათანადო ზომების მიღებისას, გათვალისწინებულ უნდა იქნას მონაცემთა უსაფრთხოების თანამედროვე მეთოდები და ტექნოლოგიები,[170] უახლესი მიღწევები, განხორციელების ხარჯები, ასევე, დამუშავების ხასიათი, ფარგლები, კონტექსტი და მიზნები. ასევე, გასათვალისწინებელია, ფიზიკური პირების უფლებებსა და თავისუფლებებზე დამუშავების ოპერაციის გავლენა.[171]

2.6.2. საერთო სასამართლო პრაქტიკა

ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთი გადაწყვეტილება მიიღო მონაცემთა უსაფრთხოების საკითხებზე. *"Z v Finland"*-ის საქმეზე[172] ევროპულმა

---

[167] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-4 მუხლის პირველი პუნქტის „ვ" ქვეპუნქტი.

[168] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §83, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].

[169] Irish DPA, Quick Guide to the Principles of Data Protection, 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf >, [18.08.2023].

[170] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10.X.2018, §63, <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>, [18.08.2023].

[171] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_32_GDPR#cite_note-1>, [18.08.2023].

[172] Case of Z v. Finland, [1997], ECHR, App. No. 22009/93.

სასამართლომ დაადგინა, რომ შიდა კანონმდებლობამ უნდა უზრუნველყოს შესაბამისი უსაფრთხოების ზომები, რათა თავიდან იქნას აცილებული „ადამიანის უფლებათა ევროპული კონვენციის“ მე-8 მუხლის გარანტიებთან შეუსაბამო ნებისმიერი კომუნიკაცია ან ჯანმრთელობის შესახებ მონაცემების გამჟღავნება. კერძოდ, ფინეთმა ვერ უზრუნველყო საჯარო საავადმყოფოში პაციენტის სამედიცინო მონაცემების არასანქცირებული წვდომისგან დაცვის მიზნით ადეკვატური ტექნიკური და ორგანიზაციული ზომების მიღება.[173]

2.6.3. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *მცირე საოჯახო ტიპის სახლების შემოწმება*

საქართველოს მთავრობის დადგენილებით დამტკიცებული ბავშვზე ზრუნვის პროგრამის ფარგლებში განსახორციელებელი ერთ-ერთი ქვეპროგრამაა მძიმე და ღრმა შეზღუდული შესაძლებლობის ან ჯანმრთელობის პრობლემების მქონე ბავშვთა სპეციალიზებული საოჯახო ტიპის მომსახურება. დადგენილებით გათვალისწინებული მომსახურების გაწევის მიზანია მზრუნველობამოკლებული მძიმე და ღრმა შეზღუდული შესაძლებლობის ან ჯანმრთელობის პრობლემების მქონე ბავშვების ოჯახთან მიახლოებულ გარემოში განთავსების გზით ოჯახთან მიახლოებულ პირობებში მოვლისა და აღზრდის უზრუნველყოფა. აღნიშნულის გათვალისწინებით, ვინაიდან ქვეპროგრამით გათვალისწინებული მომსახურების გაწევის პროცესში ორგანიზაცია, რომელიც მართავს მცირე საოჯახო ტიპის სახლს, ამუშავებს არასრულწლოვანი შშმ პირი ბენეფიციარების დიდი მოცულობის, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს, პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით განხორციელდა მომსახურების მიმწოდებელი ორგანიზაციების მიერ მათ მმართველობაში არსებული მცირე საოჯახო ტიპის სახლების (ჯამში 2 მცირე საოჯახო ტიპის სახლი) ბენეფიციარების პერსონალური მონაცემების დამუშავების კანონიერების შესწავლა.

შემოწმების ფარგლებში დადგინდა, რომ მცირე საოჯახო ტიპის სახლებში მუშავდება ბენეფიციარების პერსონალური, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების შემცველი დოკუმენტაცია, რომლებსაც მცირე საოჯახო ტიპის სახლი, ერთი მხრივ, მოიპოვებს სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა, დაზარალებულთა დახმარების სააგენტოსგან, ხოლო მეორე მხრივ, უშუალოდ

[173] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 634.

მომსახურების გაწევის პროცესში გამოკვეთილი საჭიროებების გათვალისწინებით სხვადასხვა გზით (მაგალითად, აღმზრდელობითი საქმიანობის განმავლობაში, იმ მკურნალობის ფარგლებში, რომელსაც ორგანიზაცია ზედამხედველობს და სხვა). ამასთან, შემოწმების ფარგლებში, სააგენტოსგან და ორგანიზაციებისგან წარმოდგენილი ინფორმაციის, ასევე ორგანიზაციის საქმიანობის მარეგულირებელი სამართლებრივი აქტების საფუძველზე დადგინდა, რომ კანონმდებლობა ორგანიზაციას ავალდებულებს მომსახურების პროცესში აწარმოოს (მოიპოვოს, შექმნას და შეინახოს) ბენეფიციარებთან დაკავშირებით რეგლამენტით გათვალისწინებული ჟურნალები და ე.წ. „პირადი საქმეები“, სადაც დაცული იქნება ინდივიდუალური განვითარების გეგმის ასლები და მომსახურების ინდივიდუალური გეგმები, ინფორმაცია ბენეფიციარის განათლებასთან, ჯანმრთელობასა და სხვა საკითხებთან დაკავშირებით. ამდენად, შემოწმებების ფარგლებში მოპოვებული მტკიცებულებების საფუძველზე დადგინდა, რომ ორგანიზაცია ბენეფიციარების პერსონალურ, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს ამუშავებს კონკრეტული, მკაფიოდ განსაზღვრული კანონიერი მიზნის მისაღწევად საჭირო მოცულობით.

შემოწმებების ფარგლებში ასევე დადგინდა, რომ მატერიალური ფორმით მონაცემების დამუშავების პარალელურად, ორგანიზაცია ბენეფიციარების მონაცემების დამუშავებისთვის იყენებს ტექნიკურ საშუალებებს - პორტატულ კომპიუტერსა (ე.წ. „ლეპტოპი“) და მონაცემებზე წვდომის უფლების მქონე პირების პირადი ელექტრონული ფოსტის მისამართებს (ბენეფიციარების პერსონალური მონაცემების შემცველი ინფორმაციის/დოკუმენტაციის ურთიერთგაცვლისთვის). შემოწმების ფარგლებში დადგინდა, რომ პორტატული კომპიუტერი, რომლის მეშვეობითაც მუშავდებოდა ბენეფიციარების პერსონალური მონაცემები, წარმოადგენდა მცირე საოჯახო ტიპის სახლის ლიდერის პირად პორტატულ კომპიუტერს. ამასთან, ორივე შემოწმების ფარგლებში დადგინდა, რომ პორტატული კომპიუტერები, რომელიც გამოიყენებოდა მონაცემების დამუშავების მიზნებისთვის, არ იყო დაცული პაროლით, ხოლო ელექტრონული ფოსტის მისამართის პაროლი დამახსოვრებული იყო პორტატულ კომპიუტერებში. აღნიშნული კი ნებისმიერ პირს, რომელსაც ხელი მიუწვდება კომპიუტერებზე, შესაძლებლობას აძლევს წვდომა განახორციელოს ელექტრონულ ფოსტაში დაცულ ბენეფიციარის პერსონალურ, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებზე. ერთ-ერთი შემოწმების ფარგლებში დამატებით დადგინდა, რომ პორტატული კომპიუტერით, რომლის მეშვეობითაც მუშავდება ბენეფიციარების პერსონალური მონაცემები, სარგებლობდა მცირე

საოჯახო ტიპის სახლის რამდენიმე თანამშრომელი, თუმცა, ისინი კომპიუტერის გამოყენებისთვის არ იყენებდნენ ინდივიდუალურ (განპიროვნებულ) მომხმარებელს.

აღსანიშნავია, რომ პირადი ელექტრონული ფოსტის საშუალებით პროფესიულ საქმიანობასთან დაკავშირებული ინფორმაციის ორგანიზაციის თანამშრომლების მიერ მიმოცვლა პრობლემურია, იმდენად რამდენადაც აღნიშნული ელექტრონული სისტემა მონაცემებზე წვდომის შესაძლებლობას დასაქმებულებს აძლევს, მათ შორის, სხვა ელექტრონული მოწყობილობებიდანაც, ხოლო აღნიშნულის გაკონტროლება სრულად ორგანიზაციის ორგანიზაციულ-ტექნიკურ ზომებზე დამოკიდებული ვერ იქნება. ამასთან, მონაცემებზე წვდომის შესაძლებლობა დასაქმებულ პირებს უნარჩუნდებათ მონაცემთა დამმუშავებელთან სამსახურებრივი (შრომითი) კავშირის შეწყვეტის შემდეგაც. ორგანიზაციის შინაგანაწესსა და შრომით ხელშეკრულებაში, ასევე ორგანიზაციის მიერ შედგენილ ცალკე დოკუმენტში (რომელიც არეგულირებს ბენეფიციართა პერსონალური მონაცემების დაცვას) სამსახურებრივი ინფორმაციის კონფიდენციალურობის შესახებ არსებული ჩანაწერი კი ვერ მიიჩნევა იმ რისკების ადეკვატურ ორგანიზაციულ-ტექნიკურ ზომად, რომელსაც შეუძლია უზრუნველყოს ორგანიზაციაში მონაცემთა უსაფრთხოება. აღნიშნული კი განსაკუთრებულ მნიშვნელობას იძენს იმის გათვალისწინებით, რომ ორგანიზაციაში თავს იყრის არასრულწლოვნების დიდი მოცულობის, მათ შორის, განსაკუთრებული კატეგორიის მონაცემები. ამდენად, შემოწმების ფარგლებში დადგინდა, რომ ორგანიზაციას არ ჰქონდა მიღებული მონაცემთა უსაფრთხოებისთვის შესაბამისი ორგანიზაციულ-ტექნიკური ზომები.

ზემოაღნიშნულის გათვალისწინებით, ორგანიზაციებს დაეკისრათ პასუხისმგებლობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 46-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. ამასთან, ორგანიზაციას დაევალა მონაცემების ელექტრონული ფორმით დამუშავების პროცესში გამოიყენოს მხოლოდ სამსახურებრივი მიზნით შექმნილი ელექტრონული ფოსტის მისამართი, ხოლო პორტატული კომპიუტერის მეშვეობით მონაცემების დამუშავებისას გამოიყენოს მხოლოდ სამსახურებრივი მიზნებისთვის შექმნილი ანგარიში, რომელიც სათანადოდ იქნება დაცული პაროლით და გამოიყენება მხოლოდ სამსახურებრივი მიზნებისთვის. ამასთან, ელექტრონული ფორმით ბენეფიციარების მონაცემების დამუშავების პროცესში პორტატულ კომპიუტერზე წვდომის უფლების მქონე თითოეული პირისთვის შექმნას ინდივიდუალური მომხმარებელი, რომელიც სათანადოდ იქნება დაცული პაროლით.

- *ქალაქ რუსთავის მუნიციპალიტეტის მერიის შემოწმება*

მუნიციპალიტეტები ჯანმრთელობის დაცვის პროგრამების/ქვეპროგრამების განხორციელების ფარგლებში, ავტომატური საშუალების გამოყენებითაც ამუშავებენ მოწყვლადი ჯგუფების, მათ შორის, არასრულწლოვნების შესახებ დიდი მოცულობისა და განსაკუთრებული კატეგორიის მონაცემებს. ხსენებულ მონაცემებთან მიმართებაში კი მონაცემთა უსაფრთხოების წესების დაცვა საჭიროებს რისკების ადეკვატურად შეფასებას. შემოწმება განხორციელდა სამსახურის ინიციატივით და მოიცავდა აუტიზმის სპექტრის დარღვევის მქონე ბავშვთა რეაბილიტაციის ქვეპროგრამის განხორციელებისას, ბენეფიციართა პერსონალური მონაცემების დამუშავების კანონიერების შესწავლას.

შემოწმების ფარგლებში დადგინდა, რომ აუტიზმის სპექტრის დარღვევის მქონე ბავშვთა რეაბილიტაციის ქვეპროგრამაში ჩართვის მიზნით, განცხადებასთან ერთად, რუსთავის მერიას წარედგინებოდა ბენეფიციარის თაობაზე მნიშვნელოვანი მოცულობის ინფორმაცია (მათ შორის, ჯანმრთელობის შესახებ ინფორმაცია). მერიას განაცხადი წარედგინებოდა როგორც მატერიალურად, ასევე, რუსთავის მერიის ელექტრონული ფოსტის გაგზავნის ან მოქალაქის ელექტრონული პორტალის მეშვეობით. განცხადებისა და თანდართული დოკუმენტაციის ელექტრონული ასლი კი, პირველ რიგში, იტვირთებოდა საქმისწარმოების ელექტრონულ პროგრამაში, სადაც სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ბაზიდან ბენეფიციარის და მისი კანონიერი წარმომადგენლის თაობაზე ავტომატურად აისახებოდა რიგი მონაცემები (სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, ფოტოსურათი და სხვა). ქვეპროგრამის განხორციელების მიზნებისთვის, ასევე, ხორციელდებოდა “MS Excel”-ის ფორმატის ელექტრონული დოკუმენტების შექმნა, განახლება და გამოყენება, სადაც, აგრეთვე, მითითებული იყო ბენეფიციარის რიგი პერსონალური მონაცემები. საქმისწარმოების ელექტრონული პროგრამისა და მოქალაქის პორტალის ფუნქციონირებას ტექნიკურად უზრუნველყოფდა ა(ა)იპ - მუნიციპალური სერვისების განვითარების სააგენტო.

შემოწმების ფარგლებში დადგინდა, რომ რუსთავის მუნიციპალიტეტის მერიის საქმისწარმოების ელექტრონულ პროგრამაში არსებული ზოგიერთი ძიების ფუნქციონალის გამოყენების შემთხვევაში, შესაძლებელი იყო მუნიციპალიტეტის საქმისწარმოების პროგრამაში ნებისმიერ კორესპონდენციაზე წვდომა. საქმისწარმოების ელექტრონულ პროგრამაში სამსახურებრივი ანგარიშის მქონე

ზოგიერთ თანამშრომელს გააქტიურებული ჰქონდა ფუნქციონალები და დაშვება ჰქონდა აუტიზმის სპექტრის დარღვევის მქონე ბავშვთა რეაბილიტაციის ქვეპროგრამის ფარგლებში დამუშავებულ დიდი მოცულობის მონაცემებზე, თუმცა, შემოწმების ფარგლებში დადგინდა, რომ აღნიშნულ თანამშრომელთა ნაწილს დაკისრებული ფუნქცია-მოვალეობების განხორციელებისას არ ესაჭიროებოდათ ბენეფიციართა მონაცემებზე დაშვება (მაგალითად: შემოწმების დროისათვის აღნიშნული თანამშრომლებისთვის ხელმისაწვდომი იყო საქმისწარმოების პროგრამაში რეგისტრირებული ჯამში 39 277 (ოცდაცხრამეტი ათას ორას სამოცდაჩვიდმეტი) კორესპონდენცია, მათ შორის, აუტისტური სპექტრის მქონე ბენეფიციარებთან დაკავშირებული კორესპონდენციები).

შემოწმების შედეგად ასევე გამოიკვეთა, რომ საერთო საზიარო საქაღალდეს, რომლის გამოყენებითაც მერიის თანამშრომლებს დაშვება გააჩნდათ ბენეფიციართა პერსონალური მონაცემების შემცველ “MS Excel”-ის ფორმატის ელექტრონულ დოკუმენტებზე, არ ჰქონდათ მონაცემთა მიმართ განხორციელებული მოქმედებების აღრიცხვის ელექტრონული ჟურნალი. აღნიშნული კი წარმოშობდა საფრთხეს, რომ მონაცემებზე წვდომის უფლებამოსილების მქონე თანამშრომლების მიერ მონაცემების უკანონო დამუშავების, მათ შორის, გამჟღავნების შემთხვევაში, ვერ დაფიქსირებულიყო შესაბამისი ფაქტი და პასუხისმგებელი პირის იდენტიფიცირება.

შემოწმების ფარგლებში დადგინდა, რომ საქმისწარმოების ელექტრონული პროგრამისა და მოქალაქის პორტალის ფუნქციონირების მიზნებისთვის ხორციელდებოდა მონაცემების სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს ბაზიდან მიღება. თუმცა, აღნიშნულ საკითხთან დაკავშირებით სააგენტოსა და ქალაქ რუსთავის მუნიციპალიტეტს შორის გაფორმებული ხელშეკრულება არ ითვალისწინებდა რუსთავის მერიისთვის ფიზიკურ პირთა ფოტოსურათების მიწოდებას და რუსთავის მერიის მოქალაქის პორტალზე მონაცემების რეალურ დროში მიწოდების საკითხებს.

სამსახურის გადაწყვეტილებით, ქალაქ რუსთავის მუნიციპალიტეტის მერიას მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრულებლობისთვის დაეკისრა პასუხისმგებლობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 46-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. ამასთან, მერიას დაევალა ბენეფიციართა მონაცემების (მათ შორის, საერთო საზიარო საქაღალდეში არსებული მონაცემების) მიმართ

განხორციელებული ყველა მოქმედების აღრიცხვა, ასევე, ქვეპროგრამის ფარგლებში საქმისწარმოების ელექტრონულ პროგრამაში დამუშავებულ მონაცემებზე მესამე პირთათვის კანონის მოთხოვნათა დარღვევით გადაცემის შემთხვევების თავიდან აცილების ღონისძიების დანერგვა და ამ მონაცემებზე მხოლოდ იმ პირთა დაშვება, რომელთაც ხსენებულ მონაცემებზე წვდომა მათზე დაკისრებული ფუნქცია-მოვალეობების განსახორციელებლად ესაჭიროებათ. ქალაქ რუსთავის მუნიციპალიტეტის მერიას და სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს, ასევე, დაევალათ საქმისწარმოების ელექტრონული პროგრამისა და მოქალაქის პორტალის ფუნქციონირების პროცესში ხსენებული სააგენტოსგან პერსონალური მონაცემების რეალურ დროში და დამუშავების მიზნის პროპორციული მოცულობით მიღების საკითხის ხელშეკრულებით სრულყოფილად დარეგულირება.

- *ერთ-ერთი საჯარო სკოლის შემოწმება*

შემოწმება განხორციელდა სამსახურის ინიციატივით, ვინაიდან სკოლებში, არასრულწლოვანთა დისციპლინური გადაცდომების შესახებ მნიშვნელოვანი მოცულობის პერსონალური მონაცემები მუშავდება, მათ შორის, ავტომატური საშუალებითაც. აღნიშნული მონაცემების მიმართ სათანადო ორგანიზაციულ-ტექნიკური ზომების მიუღებლობამ შესაძლოა, გამოიწვიოს მონაცემთა კანონდარღვევით გამჟღავნება ან სხვა ფორმით დამუშავება, რაც, თავის მხრივ, ბავშვის ღირსების შელახვის, მისი სტიგმატიზაციის, ე. წ. „ბულინგის“ და დისკრიმინაციის განმაპირობებელი ფაქტორი შეიძლება გახდეს.

შემოწმების ფარგლებში დადგინდა, რომ სკოლა დისციპლინური გადაცდომების ფარგლებში, მათ შორის, ავტომატური საშუალებების გამოყენებით (ელექტრონული ჟურნალი) ამუშავებდა მოსწავლეთა მონაცემებს. სკოლის დირექტორის მოვალეობის შემსრულებელი და მისი მოადგილე ელექტრონული ჟურნალის დარღვევების აღრიცხვის ველში მანდატურის სამსახურის ელექტრონული საინფორმაციო ბაზიდან პროგრამულად იღებდნენ მოსწავლის მიერ დისციპლინურ გადაცდომასთან დაკავშირებულ მონაცემებს (დარღვევის ჩადენის ადგილის, დროის და მანდატურის მიერ გატარებული ღონისძიების თაობაზე ინფორმაციას). ამასთან, ელექტრონული ჟურნალის დარღვევების ველში ზოგადი განათლების მართვის საინფორმაციო სისტემიდან (“eSchool”) აისახებოდა მოსწავლის სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, სქესი, კლასი და სოციალური სტატუსი. დისციპლინური წარმოების პროცესში სკოლა მოსწავლისგან იღებდა წერილობით ახსნა-განმარტებას სავარაუდო დარღვევასთან დაკავშირებით, მოსწავლის პასუხისმგებლობის ზომას კი

სკოლის დირექტორი განსაზღვრავდა ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტით. ელექტრონული ჟურნალის, მანდატურის სამსახურის ელექტრონული საინფორმაციო ბაზისა და "eSchool"-ის პროგრამულ უზრუნველყოფას ახორციელებდა სსიპ - განათლების მართვის საინფორმაციო სისტემა.

შემოწმების ფარგლებში დადგინდა, რომ ელექტრონულ ჟურნალში განხორციელებული მოქმედებებიდან არ აღირიცხებოდა ძებნა/დათვალიერების მოქმედება. მონაცემთა მიმართ შესრულებული მოქმედებები ასევე არ აღირიცხებოდა ელექტრონულ ჟურნალში არსებული მონაცემების შესანახად გამოყენებულ მონაცემთა ბაზაზე პირდაპირი წვდომის შემთხვევაში. სსიპ - განათლების მართვის საინფორმაციო სისტემის ბაზის ადმინისტრატორები ბაზაზე პირდაპირი წვდომის შემთხვევაში სარგებლობდნენ ერთი და იმავე მომხმარებლებით. აღსანიშნავია, რომ მონაცემთა მიმართ განხორციელებული ქმედებების აღრიცხვის შემთხვევაშიც კი მონაცემებზე საერთო მომხმარებლით წვდომა ართულებს კონკრეტული მოქმედების განმახორციელებელი პირის იდენტიფიცირებას, რაც არ შეესაბამება მონაცემთა უსაფრთხოების დაცვის მოთხოვნებს.

სამსახურის გადაწყვეტილებით, სსიპ - განათლების მართვის საინფორმაციო სისტემა ცნობილ იქნა სამართალდამრღვევად „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 46-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის (მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრულებლობა) ჩადენაში. ამასთან, სისტემას დაევალა ელექტრონულ ჟურნალში, ასევე მონაცემთა ბაზაში (ბაზაზე პირდაპირი წვდომის დროს) არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა. ასევე, იმგვარი ორგანიზაციული და ტექნიკური ზომების მიღება, რომლის მიხედვითაც უფლებამოსილი პირები ელექტრონული ჟურნალის მონაცემთა ბაზაზე პირდაპირ წვდომას შეძლებენ მხოლოდ სათანადო პაროლით დაცული განპიროვნებული მომხმარებლების ანგარიშით.

- *ქ. თბილისის მუნიციპალიტეტის ვაკის რაიონის გამგეობის შემოწმება*

აღსანიშნავია, წვევამდელთა სამხედრო აღრიცხვაზე აყვანა მუნიციპალიტეტის რაიონული გამგეობების მიერ. აღნიშნულ პროცესში არასრულწლოვნების შესახებ დიდი მოცულობისა და სენსიტიური კატეგორიის ინფორმაცია მუშავდება, რომლის პარალელურად იზრდება მათი უკანონოდ დამუშავების საფრთხეც. ამდენად, პერსონალურ მონაცემთა დაცვის სამსახურმა საკუთარი ინიციატივით შეამოწმა ქ.

თბილისის მუნიციპალიტეტის ვაკის რაიონის გამგეობა, რომელიც მოიცავდა გამგეობის მიერ წვევამდელთა სამხედრო აღრიცხვაზე აყვანის მიზნით არასრულწლოვანთა პერსონალური მონაცემების დამუშავების კანონიერების შესწავლას.

პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის შედეგად დადგინდა, რომ ქ. თბილისის მუნიციპალიტეტის ვაკის რაიონის გამგეობა არასრულწლოვანთა პირველად აღრიცხვაზე აყვანის მიზნით, მატერიალურად - მოსწავლეების/მოსწავლეების კანონიერი წარმომადგენლების მიერ შევსებული „ანკეტების“, „საკომუნიკაციო ფორმების“, პირადობისა და დაბადების მოწმობების ასლების, ფოტოსურათების მოპოვების გზით, ასევე, ელექტრონული სისტემის მეშვეობით ამუშავებს არასრულწლოვანთა პერსონალურ მონაცემებს, მათ შორის, აგროვებს, იყენებს და ინახავს მათ. გარდა ამისა, შემოწმების ფარგლებში გამოვლინდა, რომ ელექტრონულ სისტემას, რომლის მეშვეობითაც ხორციელდება არასრულწლოვანთა პირველადი აღრიცხვის, ასევე სამხედრო სავალდებულო სამსახურში გაწვევის მიზნით მონაცემთა დამუშავება, ადმინისტრირებას უწევს ქ. თბილისის მუნიციპალიტეტის მერიის ადმინისტრაციის სტრუქტურული ერთეული — საიდუმლო-სამობილიზაციო სამსახური. შესაბამისად, მის უფლებამოსილ პირებს წვდომა აქვთ აღნიშნულ ელექტრონულ სისტემაში არსებულ მონაცემებზე.

შემოწმების ფარგლებში დადგინდა, რომ „მოქალაქეთა სამხედრო აღრიცხვის შესახებ დებულების დამტკიცების თაობაზე“ საქართველოს მთავრობის 2015 წლის 02 ივნისის №247 დადგენილებით განსაზღვრულია პირველადი სამხედრო აღრიცხვის პროცესი და ამ პროცესში ჩართული თითოეული სუბიექტის (გამგეობის, საგანმანათლებლო დაწესებულების, წვევამდელის) როლი, უფლებამოსილება და წარსადგენი დოკუმენტაცია. დებულებით გამგეობის მიერ დოკუმენტაციის/ინფორმაციის მოპოვების პროცესი მოწესრიგებულია იმგვარად, რომ არასრულწლოვნის შესახებ დოკუმენტაცია და ანკეტაში არსებული მონაცემები გამგეობას უშუალოდ უნდა მიაწოდოს არასრულწლოვანმა ან მისმა კანონიერმა წარმომადგენელმა. ამასთან, ანკეტა, ასევე, შეიცავს წვევამდელის ისეთ პერსონალურ მონაცემებს, რომლის ფლობის უფლებამოსილება და ვალდებულება სკოლას კანონმდებლობით არ გააჩნია. შემოწმების შედეგად დადგინდა, რომ გამგეობა, დებულებით განსაზღვრული წესისგან განსხვავებით, სკოლის გავლით იღებდა წვევამდელის ისეთ პერსონალურ მონაცემებს (მაგალითად: ფოტოსურათს), რომელიც უშუალოდ წვევამდელისგან უნდა მიეღო და არა სკოლისგან. ამდენად, წვევამდელის პერსონალური მონაცემები ხელმისაწვდომი ხდებოდა არაუფლებამოსილი პირებისთვის, რომლებსაც აღნიშნულ

მონაცემებზე წვდომის საჭიროება, კანონიერი საფუძველი და ლეგიტიმური მიზანი არ ჰქონდათ, რაც, თავის მხრივ, ზრდიდა მონაცემების უკანონო დამუშავების რისკებს.

შემოწმების ფარგლებში ასევე დადგინდა, რომ მონაცემების შეგროვება ხორციელდებოდა უშუალოდ მონაცემთა სუბიექტებისგან, მათ შორის, ანკეტებისა და „საკომუნიკაციო ფორმების“ მეშვეობით. თუმცა გამგეობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-15 მუხლით დადგენილი წესის შესაბამისად არ ახდენდა მონაცემთა სუბიექტების ინფორმირებას ანკეტაში სავალდებულო და ნებაყოფლობითი ფორმით მისათითებელი მონაცემების თაობაზე. გარდა ამისა, დადგინდა, რომ ელექტრონული სისტემა შეიცავდა ისეთ შესავსებ ველებს (ფსიქიატრის, ქირურგის, თერაპევტის, ოკულისტის და სხვა დასკვნების შესავსებ ველებს), რომლის საჭიროებაც შემოწმების ფარგლებში ვერ დასაბუთდა. ამასთან, ელექტრონული სისტემა, სრულყოფილად არ აღრიცხავდა ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებულ ყველა მოქმედებას (მაგალითად: სისტემაში შესვლა/გასვლას, მონაცემების მოძიებას/დათვალიერებას, ატვირთული დოკუმენტის გახსნას/დათვალიერებას/გადმოწერას). აღნიშნული, თავის მხრივ, ზრდის მონაცემთა უკანონო მოპოვებისა და გამჟღავნების რისკებს, ვინაიდან შესაბამისი მართლსაწინააღმდეგო შემთხვევის არსებობის პირობებში (მაგალითად: ელექტრონულ სისტემაში ატვირთული დოკუმენტების გამჟღავნებისას) არსებითად მცირდება მონაცემთა უკანონო დამუშავებაზე პასუხისმგებელი პირის იდენტიფიცირების შესაძლებლობა. ამდენად, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის გადაწყვეტილებით როგორც გამგეობას, ასევე ქ. თბილისის მუნიციპალიტეტის მერიას მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრულებლობისთვის დაეკისრათ პასუხისმგებლობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 46-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. ამასთან, გამოვლენილი დარღვევების აღმოფხვრის მიზნით როგორც გამგეობას, ასევე ქ. თბილისის მუნიციპალიტეტის მერიას მიეცათ შესასრულებლად სავალდებულო დავალებები.

3. მონაცემთა დამუშავების საფუძვლების ზოგადი მიმოხილვა

როგორც უკვე აღინიშნა, არასრულწლოვნები სარგებლობენ პერსონალური მონაცემების დაცვის განსაკუთრებული უფლებით, რადგან მათთვის შეიძლება ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, სამართლებრივი დაცვის

მექანიზმები და უფლებები, რომლებიც უკავშირდება მათი პერსონალური მონაცემების დამუშავებას.[174] ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ ადგენს მონაცემთა დამუშავების ექვს საფუძველს, რომლის ჩამონათვალი უნდა იქნას გაგებული, როგორც ამომწურავი და საბოლოო. ასევე, საგულისხმოა, რომ მონაცემთა დამუშავების საფუძვლებს შორის იერარქია არ არსებობს:[175]

- მონაცემთა სუბიექტის თანხმობა;
- ხელშეკრულების ვალდებულების შესრულება ან სახელშეკრულებო აუცილებლობა;
- სამართლებრივი ვალდებულების შესრულება;
- მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დაცვა;
- საზოგადოებრივი ინტერესებიდან გამომდინარე ან საჯარო ფუნქციის შესრულება;
- დამუშავებისთვის პასუხისმგებელი ან დამუშავებაზე უფლებამოსილი პირის ან მესამე პირის ლეგიტიმური ინტერესი (სადაც ინტერესი არ აჭარბებს მონაცემთა სუბიექტის ინტერესებს ან ფუნდამენტურ უფლებას).

დამუშავებისთვის პასუხისმგებელ პირებს შეუძლიათ, დაეყრდნონ ნებისმიერ ზემოხსენებულ სამართლებრივ საფუძველს მონაცემთა სუბიექტის პერსონალური მონაცემების დასამუშავებლად. ამასთანავე, მნიშვნელოვანია, რომ დამუშავების გარემოებები ესადაგებოდეს აღნიშნულ სამართლებრივ საფუძვლებს. აღსანიშნავია, რომ ზოგიერთი სამართლებრივი საფუძველი, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ავალდებულებს, რომ დააკმაყოფილონ დამატებითი კრიტერიუმები, ისეთ შემთხვევაში, როდესაც მონაცემთა სუბიექტს არასრულწლოვანი წარმოადგენს.[176]

აღსანიშნავია, რომ ეროვნული კანონმდებლობით განსაზღვრული საფუძვლები შეესაბამება ევროკავშირის სამართლებრივ ჩარჩოს. კერძოდ, ახალი კანონის მე-5 მუხლი აყალიბებს მონაცემთა დამუშავების საფუძვლებს, რომელთაგან ერთ-ერთია დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების დაცვა, თუკი აღნიშნულის საპირწონედ არ იკვეთება არასრულწლოვნის უფლების დაცვის აღმატებული ინტერესი.[177] აღნიშნული კიდევ ერთხელ ცხადყოფს კანონმდებლის ორიენტირს არასრულწლოვანთა მოწყვლადობის

[174] GDPR, Recital, para. 38.

[175] Fundamentals for a Child-Oriented Approach to Data Processing, 22.

[176] იქვე.

[177] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-5 მუხლის პირველი პუნქტის „ი“ ქვეპუნქტი.

გათვალისწინებით, მათი საუკეთესო ინტერესის დაცვაზე, რასაც მოწმობს არაერთი სახელმწიფოს პერსონალურ მონაცემთა დაცვის ეროვნული სამართალი.[178]

3.1. არასრულწლოვნის, როგორც მონაცემთა სუბიექტის თანხმობა

ევროკავშირის საკანონმდებლო ჩარჩო არასრულწლოვანთან მიმართებით ორსაფეხურიანი დაცვის რეჟიმს ადგენს, რაც ვლინდება, ერთი მხრივ, მონაცემთა დამმუშავებლების ვალდებულებების სახით, ხოლო მეორე მხრივ — არასრულწლოვანთან მიმართებით სპეციალური მოწესრიგების არსებობით.[179] ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-6 მუხლის პირველი პუნქტის “a” ქვეპუნქტის თანახმად, პერსონალური მონაცემების დამუშავება კანონიერია, თუ „მონაცემთა სუბიექტი განაცხადებს თანხმობას მისი პერსონალური მონაცემების დამუშავებაზე ერთი ან მეტი კონკრეტული მიზნისათვის“. მონაცემთა დამუშავებაზე თანხმობა უნდა გაიცეს ნათლად გამოხატული მოქმედებით და უნდა დგინდებოდეს მონაცემთა სუბიექტის ნებაყოფლობითი, კონკრეტული, ინფორმირებული და არაბუნდოვანი თანხმობა მის შესახებ მონაცემების დამუშავებაზე, მაგალითად, წერილობითი განცხადებით, მათ შორის, ელექტრონული საშუალებების გამოყენებით, ან ზეპირი განცხადებით.[180] აღსანიშნავია, რომ მონაცემთა სუბიექტის დუმილი, წინასწარ მონიშნული გრაფები ან უმოქმედობა არ წარმოადგენს თანხმობას. ამასთანავე, თანხმობა უნდა შეეხებოდეს დამუშავების ყველა აქტივობას, რომელიც ხორციელდება იმავე მიზნით ან მიზნებით. თუ მონაცემთა სუბიექტმა თანხმობა უნდა გასცეს ელექტრონული საშუალებებით გამოგზავნილი მოთხოვნის პასუხად, აღნიშნული მოთხოვნა უნდა იყოს მოკლე და ნათლად ჩამოყალიბებული და არ უნდა აყენებდეს ზიანს იმ მომსახურებას, რომლის მისაღებადაც იქნა თანხმობა მოთხოვნილი.[181] მნიშვნელოვანია, რომ მონაცემთა სუბიექტს ჰქონდეს თანხმობის გამოთხოვის შესაძლებლობაც.[182]

საინფორმაციო საზოგადოების სერვისებთან (ონლაინ სერვისებთან) მიმართებით, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონი, მსგავსად,

---

[178] Steeves V., Macenaite M., Data Protection and children’s online privacy, in: Research Handbook on Privacy and Data Protection Law, 2022, 364-365.

[179] იქვე, 367.

[180] Fundamentals for a Child-Oriented Approach to Data Processing, 22.

[181] GDPR, Recital, para. 32.

[182] შუდრა თ., ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2023, 127.

“GDPR”-სა, ადგენს ბავშვების თანხმობის ასაკობრივ ცენზს, რომელიც არ უნდა იყოს 16 წელზე ნაკლები.[183] ონლაინ სერვისებთან მიმართებით თანხმობის ასაკობრივი მოთხოვნის დაწესება არ არის ვებგვერდებსა და აპლიკაციებზე წვდომის ხელშემშლელი ღონისძიება; იგი ერთგვარი ინდიკატორია ონლაინ სერვისების მიმწოდებლებისთვის, რათა მათი მომსახურების ბუნება, დიზაინი და მომხმარებლის ასაკისთვის შესაბამისი გახადონ; ამასთანავე, აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის შესაბამისად, 16 წლის ასაკს მიღწეული პირებისაგან ან 16 წლამდე ასაკის არასრულწლოვნების შემთხვევაში, მათი მშობლებისგან ან სხვა კანონიერი წარმომადგენლებისგან მიღებული ციფრული თანხმობა არ უნდა იქნას გამოყენებული იმგვარად, რომ ყველა ასაკის ბავშვის მიმართ იმგვარი მოპყრობა განხორციელდეს, როგორიც ზრდასრულების შემთხვევაში არის მისაღები.[184]

საგულისხმოა, რომ ევროკავშირის წევრ სახელმწიფოებს შიდა საკანონმდებლო დონეზე შეიძლება, ჰქონდეთ დამატებითი მოთხოვნები არასრულწლოვანთა თანხმობისა და მონაცემთა დაცვის შესახებ. ამასთანავე, აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელი პირი, რომელიც უზრუნველყოფს ტრანსსასაზღვრო მომსახურებას, ყოველთვის არ შეიძლება დაეყრდნოს მხოლოდ იმ წევრი სახელმწიფოს კანონმდებლობას, სადაც მას აქვს დაწესებულება, ასევე შეიძლება საჭირო გახდეს თითოეული წევრი სახელმწიფოს შესაბამისი ეროვნული კანონმდებლობის დაცვა, რომელსაც იგი სთავაზობს სერვისებს. აღნიშნული დამოკიდებულია იმაზე, ირჩევს თუ არა წევრი სახელმწიფო დამუშავებისთვის პასუხისმგებელი პირის ძირითადი დაწესებულების ადგილს თავის ეროვნულ კანონმდებლობაში თუ მონაცემთა სუბიექტის რეზიდენციას.

გასათვალისწინებელია, რომ მოქმედი კანონი არ არეგულირებს უშუალოდ არასრულწლოვნის მიერ თანხმობის გაცემის საკითხებს, თუმცა მასზე ვრცელდება მონაცემთა კანონიერი დამუშავების შესახებ დადგენილი საკანონმდებლო სტანდარტები. „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მიხედვით, თანხმობა განიმარტება, როგორც: „მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე ზეპირად, სატელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით

[183] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 7. აქვე აღსანიშნავია, რომ “GDPR”-ი თანხმობის ასაკობრივ ცენზს მხოლოდ ელექტრონული მომსახურების შეთავაზებასთან დაკავშირებით აწესებს, ხოლო „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონი პერსონალურ მონაცემთა დამუშავებას 16 წლის ასაკს მიღწეული არასრულწლოვნის თანხმობის საფუძველზე დასაშვებად მიიჩნევს.

[184] Fundamentals for a Child-Oriented Approach to Data Processing, 41.

გამოხატული ნებაყოფლობითი თანხმობა, რომლითაც შესაძლებელია ნათლად დადგინდეს მონაცემთა სუბიექტის ნება“.[185] ხოლო, წერილობითი თანხმობა გულისხმობს „მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე გამოხატული ნებაყოფლობითი თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან სხვაგვარად აღნიშნა წერილობით ან მასთან გათანაბრებული ფორმით“.[186] ახალი კანონის მე-7 მუხლი ასახავს არასრულწლოვნის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესსა და პირობებს, კერძოდ, არასრულწლოვანი პირის შესახებ მონაცემების დამუშავება მისი თანხმობით დასაშვებია იმ შემთხვევაში, თუ მან მიაღწია 16 წლის ასაკს, ხოლო 16 წლამდე პირის შემთხვევაში, აუცილებელია მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა[187].

ბავშვებისთვის სერვისების მიწოდებისას თანხმობის საფუძველზე, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დაადასტუროს, რომ მომხმარებელი, რომელიც გასცემს თანხმობას, თანხმობის ასაკზე უფროსია და ეს ზომები უნდა იყოს პროპორციული დამუშავების აქტივობების ხასიათისა და რისკების მიმართ. ისეთ შემთხვევებში, როდესაც მომხმარებლები აცხადებენ, რომ ისინი არიან ციფრულ თანხმობის ასაკს მიღწეულნი, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია განახორციელოს შესაბამისი შემოწმება, ამ განაცხადის სინამდვილის დასადასტურებლად. აღსანიშნავია, რომ ასაკის ვერიფიკაციამ, შემოწმებამ არ უნდა გამოიწვიოს მონაცემთა გადაჭარბებული დამუშავება; მექანიზმი, რომელიც შერჩეულია მონაცემთა სუბიექტის ასაკის დასადასტურებლად, უნდა მოიცავდეს შეთავაზებული დამუშავების რისკის შეფასებას.[188] საეჭვოობის შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განიხილოს მათი ასაკის გადამოწმების მექანიზმები კონკრეტულ შემთხვევაში და განიხილოს ალტერნატიული შემოწმების საჭიროებაც.[189]

---

[185] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-2 მუხლის „ზ“ ქვეპუნქტი.

[186] იქვე, „თ“ ქვეპუნქტი.

[187] საინტერესოა საკითხის ემანსიპაციის ინსტიტუტის კონტექსტშიც განხილვა იმდენად, რამდენადაც საქართველოს სამოქალაქო კოდექსი ზოგიერთ შემთხვევაში ითვალისწინებს არასრულწლოვანი პირის სრულ გათანაბრებას — ემანსიპაციას სრულწლოვანი პირების უფლებებთან, მაგალითად, თუკი 16 წლის ასაკს მიღწეული პირს კანონიერი წარმომადგენელი საწარმოს დამოუკიდებლად გაძღოლის უფლებას ანიჭებს, ჭანტურია ლ. (რედ.),სამოქალაქო კოდექსი კომენტარი, წიგნი I, სამოქალაქო კოდექსის ზოგადი დებულებები, 2017, 70, 377.

[188] CNIL, Online age verification: balancing privacy and the protection of minors, 2022, <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>, [20.12.2023]; CIPL, Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable, 2023, <https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable>, [20.12.2023].

[189] Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018.

აღსანიშნავია, რომ ახალი კანონი თანახმად, 16 წლამდე არასრულწლოვნის შესახებ მონაცემთა დამუშავების მიზნით სავალდებულოა მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა, რომელიც თავის მხრივ, არ უნდა ეწინააღმდეგებოდეს ბავშვის საუკეთესო ინტერესს.[190] მეორე მხრივ, კანონი ადგენს მონაცემთა დამმუშავებლის ვალდებულებას, გაითვალისწინოს ყველა გონივრული ღონისძიება, რათა მოხდეს მშობლის ან კანონიერი წარმომადგენლის თანხმობის დადასტურება.[191] ამასთანავე, აღსანიშნავია, რომ თანხმობა უნდა განხორციელდეს თავისუფალი ნების განხორციელების შედეგად. იმისათვის, რომ თანხმობა იყოს ნებაყოფლობითი, ურთიერთობა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის უნდა იყოს „თანასწორუფლებიანი“ — მაგალითად, თანხმობა არ შეიძლება იქნას გამოყენებული სამართლებრივ საფუძვლად მოსწავლეებსა და სკოლასთან მიმართებით მათი არათანაბარი ურთიერთობის გამო.[192] მონაცემთა სუბიექტისთვის თანხმობამდე ინფორმაციის მიწოდება არსებითად მნიშვნელოვანია, რათა მან მიიღოს ინფორმირებული გადაწყვეტილება თანხმობის გაცემის საკითხზე.

3.2. ხელშეკრულების ვალდებულების შესრულება ან სახელშეკრულებო აუცილებლობა

მონაცემთა დამუშავება კანონიერია, როდესაც იგი აუცილებელია იმ ხელშეკრულების შესასრულებლად, რომლის მხარეც მონაცემთა სუბიექტია ან იმისთვის, რომ გადაიდგას შესაბამისი ნაბიჯები მონაცემთა სუბიექტის მოთხოვნილი ხელშეკრულების დადებამდე.[193] აღნიშნული სამართლებრივი საფუძველი გამოიყენება, როდესაც არსებობს ფაქტობრივი ან განზრახ სახელშეკრულებო ურთიერთობა მონაცემთა სუბიექტსა და ორგანიზაციას შორის. ბავშვის პერსონალური მონაცემების დამუშავების კონტექსტში ორგანიზაციებმა უნდა გაითვალისწინონ ასაკობრივი შეზღუდვები და სხვა უნარებთან დაკავშირებული სპეციფიკური წესები, რომლებიც შეიძლება გამოყენებული იქნას ეროვნული კანონმდებლობით ხელშეკრულების დადების შესაძლებლობასთან.[194]

---

[190] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 7.

[191] იქვე, მე-7 მუხლის მე-2 პუნქტი.

[192] Swedish Authority for Privacy Protection, The rights of children and young people on digital platforms, Stakeholder guide, 22.

[193] GDPR, Article 6(1)(b).

[194] Fundamentals for a Child-Oriented Approach to Data Processing, 23.

3.3. სამართლებრივი ვალდებულების შესრულება

მონაცემთა დამუშავება კანონიერია, როდესაც იგი აუცილებელია კანონიერი ვალდებულების შესასრულებლად, რომელსაც ექვემდებარება დამუშავებისთვის პასუხისმგებელი პირი.[195] ორგანიზაციებს შეუძლიათ დაეყრდნონ ზემოაღნიშნულ მუხლს, ისეთ შემთხვევებში, როდესაც ისინი ვალდებულნი არიან დაამუშაონ პერსონალური მონაცემები, რათა შეასრულონ ვალდებულებები, რომლებიც წარმოიშობა როგორც საერთაშორისო, ისევე ადგილობრივი კანონმდებლობიდან გამომდინარე. აღნიშნული საფუძვლით მონაცემთა დამუშავების შემთხვევაში, მნიშვნელოვანია იმგვარ სამართლებრივ ვალდებულებებზე ორიენტირი, რომელიც ბავშვის პერსონალური მონაცემების დამუშავებისას წარმოიშობა.[196] დამუშავების მიზანი უნდა იყოს ვალდებულების შესრულება. აღნიშნული ასევე ვრცელდება იმგვარ შემთხვევებზე, ვალდებულება ასევე განსაზღვრულია საჯაროსამართლებრივი აქტით, მეორადი ან დელეგირებული კანონმდებლობით, კონკრეტულ შემთხვევაში კი საჯარო ორგანოს სავალდებულო გადაწყვეტილებით.[197]

3.4. მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დაცვა

“GDPR”-ის მე-6 მუხლის პირველი პუნქტის “d” ქვეპუნქტის თანახმად, მონაცემთა დამუშავება კანონიერია, როდესაც მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დასაცავად. აღნიშნული საფუძველი მიემართება მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დაცვას, მათ შორის, მაგალითად, ეპიდემიის მონიტორინგის ან/და მისი გავრცელების აღკვეთის, ჰუმანიტარული კრიზისების, ბუნებრივი და ადამიანის მოქმედებით გამოწვეული კატასტროფების მართვას. ამასთანავე, აღსანიშნავია, რომ ბავშვის სასიცოცხლო ინტერესების დაცვა, შეიძლება განსხვავებული იყოს ზრდასრული პირის სასიცოცხლო ინტერესებისგან. ირლანდიის პერსონალურ მონაცემთა საზედამხედველო ორგანოს პრაქტიკიდან გამომდინარე, ბავშვთა დაცვის ღონისძიებები უპირატესია ყველა სხვა მონაცემთა სუბიექტის ინტერესის დაცვასთან შედარებით.[198]

---

[195] GDPR, Article 6(1)(c).

[196] Fundamentals for a Child-Oriented Approach to Data Processing, 23.

[197] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020.

[198] Fundamentals for a Child-Oriented Approach to Data Processing, 24.

3.5. საზოგადოებრივი ინტერესებიდან გამომდინარე ან საჯარო ფუნქციის შესრულება

“GDPR”-ის მე-6 მუხლის პირველი პუნქტის “e” ქვეპუნქტის თანახმად, მონაცემთა დამუშავება კანონიერია, როდესაც „მონაცემთა დამუშავება აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან მონაცემთა დამმუშავებლისათვის მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად“.[199] მონაცემთა დამუშავების აღნიშნული საფუძველი, ძირითად შემთხვევაში, დაცული იქნება მიერ ან ისეთი ორგანიზაციების მიერ, რომლებიც ასრულებენ საჯარო სამართლის ან ნორმატიულ ფუნქციას. ამ კონტექსტში საჯარო სექტორის დაწესებულებს აქვთ კონკრეტული ფუნქციები, რომელიც ითვალისწინებს არასრულწლოვანთა მონაცემების დამუშავებას, მაგალითად: ჯანდაცვის სფეროში, სოციალურ ზრუნვასთან ან საგანმანათლებლო პროცესთან დაკავშირებით. აღსანიშნავია, რომ დამუშავება სრულად უნდა შეესაბამებოდეს სამართლებრივი საფუძვლის მოთხოვნებს, გარდა იმ შემთხვევისა, როდესაც საპირწონედ ბავშვის საჯარო ინტერესი ანდა მისი საუკეთესო ინტერესია დასაცავი. აღსანიშნავია, რომ მტკიცების ტვირთი არასრულწლოვნის მონაცემთა დამუშავებაზე სწორედ დამმუშავებელს აკისრია.[200]

3.6. დამუშავებისთვის პასუხისმგებელი ან დამუშავებაზე უფლებამოსილი პირის ან მესამე პირის ლეგიტიმური ინტერესი

„მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესებს აღემატება იმ მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები, რომელიც მოითხოვს მონაცემთა დაცვას, განსაკუთრებით თუ მონაცემთა სუბიექტი ბავშვია“.[201] აღნიშნულ საფუძველზე დაყრდნობის მთავარი პირობაა ის, რომ კანონიერი ინტერესები, რომლებსაც ახორციელებს დამმუშავებელი, არ აჭარბებდეს მონაცემთა სუბიექტის ინტერესებს, უფლებებს ანდა ფუნდამენტურ თავისუფლებას. აღნიშნული ნიშნავს, რომ ორგანიზაციამ უნდა შეაფასოს ბავშვის პერსონალური მონაცემების დამუშავება, რაც მოიცავს დამუშავებისთვის პასუხისმგებელი პირის ან ორგანიზაციის ლეგიტიმური

[199] GDPR, Article 6, 1(e).
[200] Fundamentals for a Child-Oriented Approach to Data Processing, 24.
[201] GDPR, Article 6, 1(f).

ინტერესების იდენტიფიცირებას, რომელთა მიღწევაც არის გამიზნული; მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ან ორგანიზაციამ შეძლოს დემონსტრირება თუ რატომ და როგორ განხორციელდება მონაცემთა დამუშავება და რამდენად პროპორციული საშუალება იქნება გამოყენებული ლეგიტიმური მიზნის მისაღწევად, ასევე, კანონიერი ინტერესების ბალანსი ბავშვის ინტერესებთან და ფუნდამენტურ უფლებებთან მიმართებით.[202]

საერთაშორისო და ევროკავშირის კანონმდებლობის პრინციპების გათვალისწინებით, ბავშვის საუკეთესო ინტერესები უნდა იყოს უმთავრესი ინდიკატორი ნებისმიერი გადაწყვეტილების მიღებისას, კერძოდ, ბავშვის, როგორც მონაცემთა სუბიექტების ინტერესები ან/და ფუნდამენტური უფლებები და თავისუფლება ყოველთვის უნდა იყოს უპირატესი.[203]

3.7. მოკლედ განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავების თაობაზე

პერსონალურ მონაცემთა კატეგორიზაციის კონტექსტში აღსანიშნავია „განსაკუთრებული კატეგორიის“, სხვა სიტყვებით კი — „სენსიტიური“ პერსონალურ მონაცემი, რომლის მოწესრიგება განსაკუთრებული რეგულირების ქვეშ ექცევა.[204] განსაკუთრებული კატეგორიის მონაცემთა დამუშავების ცალკეული საფუძვლები „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის სპეციალური ნორმით არის განსაზღვრული, რომელიც აყალიბებს კანონიერი დამუშავების წინაპირობებს.[205] პერსონალური მონაცემები, რომლებიც მათი ბუნებიდან გამომდინარე, განსაკუთრებულად სენსიტიურია ფუნდამენტურ უფლებებთან და თავისუფლებებთან მიმართებით, საჭიროებს სამართლებრივი დაცვის განსხვავებულ რეჟიმს,[206] რადგან მათი დამუშავების კონტექსტი შეიძლება მნიშვნელოვანი რისკის ქვეშ აყენებდეს ფუნდამენტურ უფლებებსა და თავისუფლებებს, განსაკუთრებით კი არასრულწლოვანთა მონაცემთა დამუშავების კონტექსტში. განსაკუთრებული კატეგორიის მონაცემის დამუშავება დასაშვებია, თუკი უზრუნველყოფილია

[202] Fundamentals for a Child-Oriented Approach to Data Processing, 24.

[203] იქვე.

[204] Voigt P., Bussche A., The EU General Data Protection Regulation, A Practical Guide, 2017, 110.

[205] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 6.

[206] Swedish Authority for Privacy Protection, Sensitive personal data <https://www.imy.se/en/individuals/data-protection/introduktion-till-gdpr/what-is-actually-meant-by-personal-data/what-is-meant-by-sensitive-personal-data/> [17.08.2023].

მონაცემთა სუბიექტის უფლებებისა და ინტერესების დაცვა და ამავდროულად, არსებობს კანონით განსაზღვრული შესაბამისი საფუძველი.[207]

მნიშვნელოვანია, რომ საკანონმდებლო მოწესრიგება ნათლად განსაზღვრავდეს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების აკრძალვის საგამონაკლისო შემთხვევებს — მონაცემთა სუბიექტის ცალსახა თანხმობა ან ჯანდაცვის მიზნებიდან გამომდინარე, მათ შორის, საზოგადოებრივი ჯანდაცვისა და ჯანდაცვის სერვისების სამართავად ან საჯარო ინტერესით განპირობებული დაარქივების, სამეცნიერო თუ ისტორიული კვლევის ან სტატისტიკური კვლევის მიზნებისთვის.[208] საგულისხმოა, რომ განსაკუთრებული კატეგორიის მონაცემები, შესაძლოა, დამუშავდეს, როდესაც მონაცემთა სუბიექტმა ისინი აშკარად გაასაჯაროვა, გამოყენების აშკარა აკრძალვის დათქმის გარეშე.[209] აღნიშნულ კონტექსტში აქტუალურია არასრულწლოვნის, როგორც მონაცემთა სუბიექტის, ინფორმირებული გადაწყვეტილება მისი განსაკუთრებული კატეგორიის მონაცემების დამუშავებაზე თანხმობის გაცხადების თუ გასაჯაროების შესახებ. 16 წელს მიუღწეველი პირის განსაკუთრებული კატეგორიის მონაცემთა დამუშავების წინაპირობაა არასრულწლოვნის მშობლის ან კანონიერი წარმომადგენლის თანხმობაა, რომელიც, თავის მხრივ, უნდა გამომდინარეობდეს ბავშვის საუკეთესო ინტერესიდან.[210] თანხმობის ნამდვილობის წინაპირობას მისი ფორმაც წარმოადგენს იმდენად, რამდენადაც არასრულწლოვნის განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მშობლის ან სვა კანონიერი წარმომადგენლის წერილობითი თანხმობის საფუძველზე.[211]

3.8. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *სკოლისა და ადვოკატის მიერ არასრულწლოვნის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმება*

პერსონალურ მონაცემთა დაცვის სამსახურს მომართა არასრულწლოვნის კანონიერმა წარმომადგენელმა (დედამ) და მოითხოვა მისი არასრულწლოვანი შვილის პერსონალური მონაცემების ერთ-ერთი საჯარო სკოლისა და ადვოკატის მიერ

[207] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 6.

[208] GDPR, Recital, para. 52.

[209] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-6 მუხლის პირველი პუნქტის „ი“ ქვეპუნქტი.

[210] Steeves V., Macenaite M., Data Protection and children's online privacy, in: Research Handbook on Privacy and Data Protection Law, 2022, 366.

[211] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-7 მუხლის მე-3 პუნქტი.

დამუშავების კანონიერების შესწავლა. კერძოდ, განცხადების თანახმად, ერთ-ერთ რაიონულ სასამართლოში განიხილებოდა უკანონო ხელშეშლის აღკვეთის თაობაზე სამოქალაქო დავა, რომელშიც მოსარჩელე იყო არასრულწლოვანი, ხოლო მოპასუხე მხარეს წარმოადგენდა მოსარჩელის მეზობლად მცხოვრები პირი, რომელსაც მის ეზოში შესაბამისი ნებართვის გარეშე მოწყობილი ჰქონდა საგვარეულო სასაფლაო, რაც ზიანს აყენებდა არასრულწლოვნის ფსიქო-ემოციურ მდგომარეობას. აღნიშნულის გათვალისწინებით არასრულწლოვნის ოჯახს მოუწია საცხოვრებლის შეცვლა და ბავშვის სხვა სკოლაში გადაყვანა.

შემოწმების ფარგლებში დადგინდა, რომ ზემოაღნიშნული სასამართლო წარმოების ფარგლებში, მოსარჩელის მიერ სარჩელში მითითებული ფაქტობრივი გარემოებების გაქარწყლების მიზნით, მოპასუხე მხარის წარმომადგენელმა მტკიცებულების მოპოვებისა და სასამართლოში წარდგენისთვის წერილობითი ფორმით ორჯერ მიმართა სკოლას და მოითხოვა არასრულწლოვნის პერსონალური მონაცემების შემცველი ინფორმაცია. კერძოდ, პირველი კორესპონდენციის მეშვეობით, სკოლისგან გამოთხოვილ იქნა არასრულწლოვნის სკოლაში ჩარიცხვის თარიღის და სწავლების ფორმატის (პირისპირ/დისტანციური) თაობაზე ინფორმაცია. ხოლო, განმეორებითი წერილით მოთხოვნილ იქნა შემდეგი ინფორმაცია - არასრულწლოვნის სკოლაში ჩარიცხვის თარიღი, ასევე როდის და რომელ სკოლაში გადავიდა ის სასწავლებლად. შემოწმების ფარგლებში დადგინდა, რომ სკოლამ მოპასუხის წარმომადგენელს მიაწოდა მის მიერ მოთხოვნილ ინფორმაციაზე მეტი მოცულობის მონაცემები (დამატებით მიაწოდა ინფორმაცია იმის თაობაზე, თუ ვისი განცხადების საფუძველზე მოხდა პირის სკოლიდან ამორიცხვა), რაც მოპასუხის წარმომადგენლის მხრიდან წარდგენილ იქნა სასამართლოში მტკიცებულების სახით.

ზემოაღნიშნულის საფუძველზე სამსახურმა იმსჯელა როგორც ადვოკატის, ასევე სკოლის მიერ არასრულწლოვნის მონაცემების დამუშავების კანონიერებაზე. ადვოკატის მიერ არასრულწლოვნის პერსონალური მონაცემების დამუშავების ნაწილში, სამსახურმა განმარტა, რომ მოპასუხე მხარის ადვოკატმა, თავისი პროფესიული საქმიანობის ფარგლებში, მისი მარწმუნებლის ინტერესების დაცვის მიზნით, შეჯიბრებითობის პრინციპის გათვალისწინებითა და საქართველოს სამოქალაქო საპროცესო კოდექსის მოთხოვნების შესაბამისად, მტკიცებულების მოსაპოვებლად და მათი სასამართლოში წარსადგენად გამოითხოვა სკოლიდან არასრულწლოვნის მონაცემები. აღნიშნულ პროცესში კი მოქმედებდა კანონიერი მიზნით და კონკრეტული საჭიროების ფარგლებში. ამდენად, ადვოკატის მხრიდან

არასრულწლოვნის პერსონალური მონაცემების უკანონო დამუშავების ფაქტი არ დადგინდა.

რაც შეეხება სკოლის მხრიდან არასრულწლოვნის პერსონალური მონაცემების გამჟღავნების კანონიერების საკითხს, სამსახურმა შეაფასა სკოლის მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის „ე“ ქვეპუნქტით გათვალისწინებული საფუძვლით (სკოლა მიუთითებდა აღნიშნულ საფუძველზე) მონაცემების გაცემის კანონიერება და განმარტა, რომ აღნიშნული სამართლებრივი საფუძვლის არსებობის პირობებში სკოლა უნდა დარწმუნებულიყო იმ გარემოებაში, რომ ადვოკატთან მიმართებით არ არსებობდა მოსარჩელე არასრულწლოვნის უფლებებისა და თავისუფლებების დაცვის აღმატებული ინტერესები. ამასთან, იმ პირობებში, როდესაც სკოლამ არასრულწლოვნის მონაცემები გაუმჟღავნა მოდავე მხარეს, საგანმანათლებლო დაწესებულება ვერ იქნებოდა დარწმუნებული აღნიშნული გადაწყვეტილების ბავშვის საუკეთესო ინტერესებთან თავსებადობაში, ვინაიდან მისთვის ვერ იქნებოდა განჭვრეტადი მონაცემთა დამუშავების შემდგომ პროცესში ბავშვის ინტერესების სარგებელი. ამდენად, სამსახურმა დაადგინა, რომ ვინაიდან სკოლას მისი მხრიდან მონაცემების გამჟღავნების თაობაზე არ ჰქონდა მონაცემთა სუბიექტის თანხმობა და არც სასამართლოს დავალება, ამასთან, სკოლამ ვერ დაასაბუთა მონაცემთა დამუშავების სხვა რომელიმე საფუძველი, სკოლის მიერ დაირღვა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლით დადგენილი მოთხოვნები, რაც წარმოადგენს ამავე კანონის 43-ე მუხლით გათვალისწინებული ადმინისტრაციული პასუხისმგებლობის დაკისრების საფუძველს. დამატებით, სამსახურმა განმარტა, რომ ვინაიდან სკოლამ ადვოკატს გაუმჟღავნა იმაზე მეტი მოცულობის მონაცემები, ვიდრე ადვოკატს ჰქონდა მოთხოვნილი, აღნიშნულ პროცესში დამატებით დაირღვა კანონის მე-4 მუხლით გათვალისწინებული მონაცემთა დამუშავების პრინციპებიც.

- *სსიპ — მსჯავრდებულთა პროფესიული მომზადებისა და გადამზადების ცენტრი*

ბავშვების პირადი ცხოვრების ხელშეუხებლობის უფლების უზრუნველსაყოფად მნიშვნელოვანია, რომ არასრულწლოვნების პერსონალური, განსაკუთრებით კი სენსიტიური კატეგორიის მონაცემები, კანონის მოთხოვნათა დაცვით დამუშავდეს. იმ შემთხვევაში კი, როცა საკითხი ბავშვების მონაცემების გამჟღავნებას შეეხება, მხედველობაში უნდა იქნეს მიღებული, თუ როგორ აღიქმება გასაჯაროებული მონაცემები მესამე პირების მხრიდან. არასრულწლოვნების მონაცემების გამჟღავნების

პროცესში განსაკუთრებით საყურადღებოა, რომ შეცდომაში შემყვანი ინფორმაციის გასაჯაროებამ შესაძლოა, საზოგადოებაში ბავშვის სტიგმატიზაციაც კი გამოიწვიოს. სწორედ ამიტომ, პერსონალურ მონაცემთა დაცვის სამსახურმა ერთ-ერთი არასამთავრობო ორგანიზაციის მომართვის საფუძველზე, შეისწავლა ცენტრის მიერ სოციალურ ქსელ „ფეისბუქზე“ ფოტოსურათების გასაჯაროების გზით არასრულწლოვნების პერსონალური მონაცემების დამუშავების კანონიერება. სამსახურში წარმოდგენილი ინფორმაციით, ცენტრის მიერ ე. წ. „ფეისბუქ“ პოსტის სახით გასაჯაროვდა ბერი ანდრიას საქველმოქმედო ფონდის ბენეფიციარებისთვის და ონკოლოგიური სენით დაავადებული სხვა ბავშვებისთვის ბავშვთა დაცვის დღის მილოცვის შესახებ ინფორმაცია, რომელსაც თან ახლდა იდენტიფიცირებადი ფორმით არასრულწლოვანი პირების ამსახველი ფოტოსურათი.

პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის შედეგად დადგინდა, რომ ცენტრის მიერ გასაჯაროებულ ფოტოსურათებში ასახული ბავშვების კანონიერ წარმომადგენლებს და სხვა პირებს გაცხადებული ჰქონდათ თანხმობა მათი მონაცემების დამუშავებასთან დაკავშირებით. ამასთან, ფოტომასალა ფონდის ბენეფიციარების (ონკოლოგიური დაავადების მქონე ბავშვების) გარდა, კონკრეტულ დღეს ფონდში სხვადასხვა მიზეზით მყოფ სხვა ბავშვებს და ფონდის ბენეფიციარების ოჯახის წევრების გამოსახულებას ასახავდა. ამდენად, ცენტრის მიერ ე. წ. „ფეისბუქის“ მეშვეობით გასაჯაროებული ინფორმაცია იყო შეცდომაში შემყვანი, რადგან ე. წ. „პოსტში“ მითითებული ინფორმაციის თანახმად, ცენტრის წარმომადგენლებმა მოინახულეს ფონდის ბენეფიციარები. თუმცა, შემოწმების ფარგლებში დადგინდა, რომ სოციალურ ქსელში ცენტრის მიერ გასაჯაროებულ ინფორმაციასთან ერთად განთავსებული ფოტომასალა, ბენეფიციარების გარდა, სხვა პირთა გამოსახულებას ასახავდა. სამსახურის უფროსის გადაწყვეტილებით, სსიპ - მსჯავრდებულთა პროფესიული მომზადებისა და გადამზადების ცენტრს დაევალა ე. წ. „პოსტში“ ინფორმაციის იმგვარად შეცვლა, რომ მისი მკითხველისთვის ცხადი გამხდარიყო, რომ გამოქვეყნებულ ინფორმაციაში არამხოლოდ ფონდის ბენეფიციარების ფოტოსურათები იყო გასაჯაროებული.

4. არასრულწლოვნის, როგორც მონაცემთა სუბიექტის, უფლებები და მათი განხორციელება

არასრულწლოვანი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამართლით უზრუნველყოფილი უფლებების პირველად სუბიექტს. იგი აღჭურვილია და

სარგებლობს იმავე სამართლებრივი დაცვის საშუალებებითა და მექანიზმებით, რომლითაც სრულწლოვანი პირი. თუმცა აღნიშნული უფლებების განხორციელებისას მიზანშეწონილია ბავშვზე მორგებული მიდგომების გათვალისწინება. აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი ადგენს მოთხოვნებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის, დაადგინონ უფლების დაცვის უფრო მაღალი სტანდარტი ბავშვის პერსონალური მონაცემების დამუშავებისას, მათ შორის, ბავშვსა და მის კანონიერ წარმომადგენელს შორის მონაცემთა დამუშავებასთან დაკავშირებით არსებული აზრთა სხვადასხვაობის არსებობის დროს ბავშვის საუკეთესო ინტერესისთვის უპირატესობის მინიჭებით.[212] ბავშვზე მორგებული მართლმსაჯულების ნათელი მაგალითია ბავშვისთვის ინფორმაციის მიწოდების მისთვის გასაგები ფორმით მიწოდების ვალდებულება.[213] ამასთანავე, ახალი კანონი ბავშვის მიერ მონაცემთა უკანონო დამუშავებას მიიჩნევს შემამსუბუქებელ,[214] ხოლო ბავშვის პერსონალურ მონაცემთა უკანონო დამუშავებას დამამძიმებელ გარემოებად,[215] რაც კიდევ ერთხელ მიუთითებს, ბავშვის, როგორც მონაცემთა სუბიექტი უფლებების დაცვის განსაკუთრებულ ინტერესზე. არასრულწლოვნის უფლების დაცვის განსაკუთრებული გარანტიებით უზრუნველყოფის აუცილებლობა გამომდინარეობს ბავშვის მდგომარეობიდან, რაც გულისხმობს, რომ შესაძლებელია, ბავშვი ნაკლებად აცნობიერებდეს მისი პერსონალური მონაცემების დამუშავებასთან დაკავშირებულ რისკებს, პოტენციურ შედეგებს, მისი უფლებებსა და უფლების დაცვის სამართლებრივ გარანტიებს ასაკის, განვითარების ან განათლების დონიდან გამომდინარე.[216] მეორე მხრივ კი აღსანიშნავია, რომ მონაცემთა სუბიექტის უფლებები არ არის აბსოლუტური ხასიათის და საგამონაკლისო შემთხვევაში, ექვემდებარება გარკვეულ შეზღუდვებს. მონაცემთა სუბიექტის უფლებები უნდა განხორციელდეს ლეგიტიმურ ინტერესებთან თანაფარდობით. ამდენად, მონაცემთა სუბიექტის უფლებების შეიძლება შეიზღუდონ მხოლოდ მაშინ, როდესაც ეს კანონით არის გათვალისწინებული და წარმოადგენს აუცილებელ და პროპორციულ ზომას დემოკრატიულ საზოგადოებაში.[217]

---

[212] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-7 მუხლის, მე-5 პუნქტი.

[213] იქვე, 24-ე მუხლის მე-5 პუნქტი.

[214] იქვე, 61-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი.

[215] იქვე, 62-ე მუხლის „გ“ ქვეპუნქტი.

[216] Hof S., Children and data protection from the perspective of children's rights – Some difficult dilemmas under the General Data Protection Regulation, 2018, 10-11. ICO, Age appropriate design: a code of practice for online services, 2020, 5.

[217] 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 11.

4.1. ინფორმაციის მიღების უფლება

„ინფორმაციული თვითგამორკვევა მოითხოვს ფუნქციონირებადი ქსელების ჩამოყალიბებას სახელმწიფოს, ეკონომიკურ სტრუქტურებს, მეცნიერებასა და სამოქალაქო საზოგადოებას შორის“.[218] მოქმედი კანონის თანახმად, თუ მონაცემთა შეგროვება ხორციელდება უშუალოდ მონაცემთა სუბიექტისაგან, მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს შემდეგი ინფორმაცია: ა) მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) ვინაობა და რეგისტრირებული მისამართი; ბ) მონაცემთა დამუშავების მიზანი; გ) სავალდებულოა თუ ნებაყოფლობითი მონაცემთა მიწოდება; თუ სავალდებულოა — მასზე უარის თქმის სამართლებრივი შედეგები; დ) მონაცემთა სუბიექტის უფლება, მიიღოს ინფორმაცია მის შესახებ დამუშავებულ მონაცემთა თაობაზე, მოითხოვოს მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა და განადგურება; ხოლო თუ მონაცემთა შეგროვება არ ხორციელდება უშუალოდ მონაცემთა სუბიექტისაგან, მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი ვალდებულია მოთხოვნის შემთხვევაში მონაცემთა სუბიექტს მიაწოდოს ზემოთ ჩამოთვლილი ინფორმაცია.[219]

კანონის ახალი რედაქციის თანახმად, მონაცემების უშუალოდ მონაცემთა სუბიექტისგან შეგროვებისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მონაცემთა შეგროვებამდე ან შეგროვების დაწყებისთანავე მონაცემთა სუბიექტს მიაწოდოს სულ მცირე შემდეგი ინფორმაცია:

- დამუშავებისთვის პასუხისმგებელი პირის, მისი წარმომადგენლის ან/და დამუშავებაზე უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;
- მონაცემთა დამუშავების მიზნებისა და სამართლებრივი საფუძვლის შესახებ;
- მონაცემთა მიწოდების სავალდებულოობის შესახებ, ხოლო თუ მონაცემთა მიწოდება სავალდებულოა – მონაცემთა მიწოდებაზე უარის თქმის სამართლებრივი შედეგების თაობაზე, აგრეთვე ინფორმაცია იმის შესახებ, რომ მონაცემთა შეგროვება/მოპოვება გათვალისწინებულია საქართველოს კანონმდებლობით ან აუცილებელი პირობაა ხელშეკრულების დასადებად (ასეთი ინფორმაციის არსებობის შემთხვევაში);

[218] ხუბუა გ., მისასალმებელი წერილი, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2023, 10.

[219] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 15.

- დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების შესახებ;
- პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია;
- მონაცემთა მიმღების ვინაობა ან მონაცემთა მიმღებების კატეგორიები (ასეთის არსებობის შემთხვევაში);
- მონაცემთა დაგეგმილი გადაცემისა და მონაცემთა დაცვის სათანადო გარანტიების არსებობის შესახებ, მათ შორის, მონაცემთა გადაცემაზე ნებართვის თაობაზე (ასეთის არსებობის შემთხვევაში), თუ დამუშავებისთვის პასუხისმგებელი პირი გეგმავს მონაცემთა სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის გადაცემას;
- მონაცემთა შენახვის ვადის შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმების თაობაზე;
- მონაცემთა სუბიექტის უფლებების შესახებ.[220]

თუ მონაცემების შეგროვება უშუალოდ მონაცემთა სუბიექტისგან არ ხორციელდება, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს ზემოთ ჩამოთვლილი ინფორმაცია, აგრეთვე აცნობოს, მის შესახებ რომელი მონაცემები მუშავდება და ამ მონაცემთა მოპოვების წყარო, მათ შორის, მოპოვებულ იქნა თუ არა მონაცემები საჯაროდ ხელმისაწვდომი წყაროდან.[221] ბავშვის ინფორმირებისას, მნიშვნელოვანია, მონაცემთა დამმუშავებელმა ყურადღება გაამახვილოს შემდეგ საკითხებზე: ა) მონაცემთა სუბიექტისთვის დამახასიათებელი თავისებურებების გაცნობა; ბ) ბავშვისთვის ინფორმაციის შესაბამისი ფორმით მიწოდება (მარტივი და ადვილად აღქმადი სახით ინფორმაციის მიწოდება, არაწერილობითი ფორმით ინფორმაციის მიწოდება).[222]

საქართველოს კანონმდებლობა და საერთაშორისო სტანდარტი ადგენს ვალდებულებას, რომ მონაცემთა სუბიექტებს უნდა მიეწოდოთ ძირითადი ინფორმაცია მათი მონაცემების სავარაუდო გამოყენების შესახებ. ინფორმაციის სიცხადე განსაკუთრებით მნიშვნელოვანია ინფორმაციის ბავშვისთვის მიწოდების დროს. ინფორმირების მნიშვნელობაზე ხაზგასმულია საერთაშორისო ორგანიზაციების მიერ შემუშავებულ სახელმძღვანელო დოკუმენტებში. 29-ე მუხლის სამუშაო ჯგუფის განმარტების თანახმად, როდესაც მონაცემთა დამმუშავებლის სამიზნე აუდიტორია ბავშვებია ან მონაცემთა დამმუშავებელმა იცის, ან უნდა იცოდეს, რომ მის პროდუქტს/მომსახურებას განსაკუთრებით იყენებენ არასრულწლოვნები

[220] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 24.
[221] იქვე, მუხლი 25.
[222] იქვე, 24-ე მუხლის მე-5 პუნქტი.

(მათ შორის, გასათვალისწინებელია ისეთი შემთხვევებიც, როდესაც მონაცემთა დამმუშავებელი დამუშავების საფუძვლად ეყრდნობა ბავშვის თანხმობას), მან უნდა უზრუნველყოს, რომ გამოყენებული ლექსიკა, ტონი და ენის სტილი იმგვარად იყოს მორგებული ბავშვთა საჭიროებებზე, რომ ინფორმაციის ადრესატისთვის აღქმადი იქნება, რომ მას მიემართება აღნიშნული შეტყობინება თუ ინფორმაცია.[223] თუმცა, გაურკვევლობის არიდების მიზნით, მცირეწლოვან ან წერა-კითხვის არმცოდნე ბავშვებზე ორიენტირებული პროდუქტის/მომსახურების შეთავაზებისას გამჭვირვალობის ზომები შეიძლება მიმართული იყოს მშობლის/სხვა წარმომადგენლის მიმართ, იმის გათვალისწინებით, რომ ასეთმა ბავშვებმა, უმეტეს შემთხვევაში, ნაკლებად სავარაუდოა, რომ გაიაზრონ თუნდაც ყველაზე ძირითადი წერილობითი ან გრაფიკული შეტყობინებები გამჭვირვალობის შესახებ.[224]

ბავშვის უფლება, იყოს ინფორმირებული მისი პერსონალური მონაცემების დამუშავების შესახებ არ შეიძლება, შეიზღუდოს მხოლოდ იმიტომ, რომ მონაცემთა დამუშავების შესახებ თანხმობა გაცემულია, ნება დართულია მშობლის ან სხვა წარმომადგენლის მიერ. მიუხედავად იმისა, რომ ასეთი თანხმობა, ხშირ შემთხვევაში, ერთჯერადად არის გაცემული ან ავტორიზებული მშობლის ან კანონიერი წარმომადგენლის მიერ, ბავშვს (როგორც მონაცემთა კიდევ ერთ სუბიექტს) აქვს მონაცემთა დამმუშავებლისგან ინფორმაციის მიღების მუდმივი უფლება მონაცემთა დამუშავების მოქმედებების მიმდინარეობისას.[225] აღნიშნული შეესაბამება გაეროს ბავშვთა უფლებების კონვენციის მე-13 მუხლს, რომელიც აცხადებს, რომ ბავშვს აქვს გამოხატვის თავისუფლება, რომელიც მოიცავს უფლებას მოიძიოს, მიიღოს და გაავრცელოს ყველა სახის ინფორმაცია და იდეები.

მონაცემთა დამმუშავებელს აქვს ვალდებულება, უზრუნველყოს ბავშვებისადმი მიმართული გამჭვირვალობის ზომები. აღნიშნული მიდგომა თავსებადია ევროპის საბჭოს მინისტრთა კომიტეტის რეკომენდაციებთან[226], რომელთა თანახმად, სახელმწიფოებმა და სხვა შესაბამისმა დაინტერესებულმა მხარეებმა უნდა მიაწოდონ ბავშვებს ინფორმაცია მათი უფლებების, მათ შორის მონაწილეობის უფლებების

---

[223] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, 14, <https://ec.europa.eu/newsroom/article29/items/622227/en>, [20.12.2023].

[224] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, para. 15.

[225] იქვე, para. 15.

[226] იხ. CoE, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [20.12.2023]. იხ. ასევე, CoE, Recommendation CM/Rec(2012)2 of the Committee of Ministers to member States on the Participation of Children and Young People under the Age of 18, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cb0ca>, [20.12.2023].

შესახებ, მათთვის გასაგებ ენაზე, რომელიც შეესაბამება ბავშვების განვითარების დონესა და არსებულ გარემოებებს. ბავშვებისთვის უნდა შეიქმნას შესაძლებლობები, გამოხატონ საკუთარი თავი საინფორმაციო და საკომუნიკაციო ტექნოლოგიების საშუალებით. ბავშვები უნდა იყვნენ ინფორმირებულნი მექანიზმებისა და სერვისების შესახებ, რომლებიც უზრუნველყოფენ ადეკვატურ მხარდაჭერას და პროცედურებს საჩივრების, უფლების დაცვის საშუალებების ან მათი უფლებების დარღვევის შემთხვევაში. ასეთი ინფორმაცია ასევე ხელმისაწვდომი უნდა იყოს მათი მშობლებისთვის ან კანონიერი წარმომადგენლებისთვის, რათა მათ შეძლონ ბავშვების დახმარება უფლებების განხორციელებაში.[227] გარდა ამისა, ბავშვსა და მის წარმომადგენელს დამატებით უნდა ეცნობოთ მონაცემთა დამუშავების გასაჩივრების უფლების განხორციელების მექანიზმების შესახებ.[228]

4.2. ინფორმაციის მოთხოვნის უფლება

წვდომის უფლების რეალიზაცია ხორციელდება მხოლოდ მონაცემთა სუბიექტს მიკუთვნებულ პერსონალურ მონაცემთან მიმართებით. იგი მოიცავს ორ ეტაპს: დამმუშავებელმა უნდა შეამოწმოს, მუშავდება თუ არა მონაცემთა სუბიექტის პერსონალური მონაცემი და თუკი მუშავდება — უზრუნველყოფილი უნდა იქნას მონაცემთა სუბიექტის წვდომა შემდეგ ინფორმაციაზე: დამუშავების მიზნების შესახებ; დამუშავებული პერსონალური მონაცემების კატეგორიები; მიმღებებს ან მიმღებთა კატეგორიები; შენახვის დაგეგმილი ხანგრძლივობა ან მათი განსაზღვრის კრიტერიუმები; ამასთანავე, მონაცემთა სუბიექტი უნდა იყოს ინფორმირებული მის ისეთ უფლებებზე, როგორიცაა: გასწორება, წაშლა ან დამუშავების შეზღუდვა, გასაჩივრების უფლება. ამასთანავე, მონაცემთა სუბიექტს მიეწოდება ინფორმაცია მონაცემების წყაროს შესახებ, თუ მონაცემი არ არის შეგროვებული თავად მონაცემთა სუბიექტისგან.[229] დამმუშავებელმა უნდა უზრუნველყოს წვდომის უფლების რეალიზაცია და ასევე, სხვათა უფლებებისა და თავისუფლებების ადეკვატური დაცვა.[230]

---

[227] CoE, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, para. 6, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [20.12.2023].

[228] იქვე, para. 33. Committee on the Rights of the Child, General Comment No. 12 (2009) The Right of the Child to be Heard, para 25, <https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf>, [20.12.2023].

[229] GDPR, Intersoft Consulting, Right of Access, <https://gdpr-info.eu/issues/right-of-access/>, , [20.12.2023].

[230] ირლანდიის საზედამხედველო ორგანოს განმარტება უფლების ფარგლებზე, <https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information>, [20.12.2023].

მონაცემთა სუბიექტის წვდომის უფლების შესახებ „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) სახელმძღვანელო რეკომენდაციის პრეამბულის თანახმად, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ განსაზღვრავს,[231] რომ მონაცემთა სუბიექტის უფლება, მიიღოს ასლი მისი პერსონალურ მონაცემის დამუშავების შესახებ (დამუშავების საფუძვლებზე, პერსონალური მონაცემის კატეგორიაზე, და სხვა) უარყოფითად არ უნდა აისახოს სხვათა უფლებებსა და თავისუფლებებზე. „მონაცემთა დაცვის ევროპული საბჭო“ მიიჩნევს, რომ სხვათა უფლებები და თავისუფლებები მხედველობაში უნდა იქნას მიღებული არა მხოლოდ ასლის მიწოდების გზით ინფორმაციის გაზიარების დროს, არამედ სხვა საშუალებებით წვდომის უზრუნველყოფის შემთხვევაშიც. ამასთანავე, მონაცემთა დამმუშავებელს უნდა შეეძლოს იმის შეფასება, რომ ცალკეულ ინდივიდუალურ შემთხვევაში, წვდომის უფლების რეალიზაცია უარყოფითად იმოქმედებს სხვათა უფლებებსა ან თავისუფლებებზე.[232]

„პერსონალურ მონაცემთა დაცვის შესახებ“ მოქმედი კანონის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამმუშავებელთან გაეცნოს მის შესახებ არსებულ პერსონალურ მონაცემებს და უსასყიდლოდ მიიღოს აღნიშნული მონაცემების ასლები.[233] ინფორმაციის მოთხოვნისა და ასლის მიღების უფლების მიზანია მიაწოდოს მონაცემთა სუბიექტებს საკმარისი, გამჭვირვალე და ადვილად ხელმისაწვდომი ინფორმაცია მისი პერსონალური მონაცემების დამუშავების შესახებ, რათა მონაცემთა სუბიექტმა იცოდეს და განსაზღვროს დამუშავების კანონიერება და დამუშავებული მონაცემების სიზუსტე. ინფორმაციის მოთხოვნისა და ასლის მიღების უფლება ამარტივებს სხვა უფლებების განხორციელებას, როგორიცაა წაშლის ან გამოსწორების უფლება. ადამიანის უფლებათა ევროპული სასამართლოს (“ECtHR”) განმარტების თანახმად, სახელმწიფოებს აქვთ პოზიტიური ვალდებულება, უზრუნველყონ პირადი ცხოვრების ხელშეუხებლობის სათანადო პატივისცემა და დანერგონ ეფექტიანი და ხელმისაწვდომი პროცედურები, რომლებიც შესაძლებლობას მისცემს მონაცემთა სუბიექტს მიიღოს ყველა რელევანტური და სათანადო ინფორმაცია.[234] ამასთანავე, აღსანიშნავია, რომ მონაცემთა სუბიექტი არ არის ვალდებული დაასაბუთოს საკუთარი

[231] GDPR, Artcile 15(4): “The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.”, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2599-1-1>, [20.12.2023].

[232] EDPB, Guidelines 01/2022on data subject rights - Right of Access, 18.01.2022, <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf>, [20.12.2023].

[233] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 21, საკითხს ძირითადად ანალოგიურად ახალი კანონი მე-14 მუხლით.

[234] იხ. ECtHR, Roche v. the United Kingdom [GC], 2005, § 162; Haralambie v. Romania, 2009, § 86; Joanna Szulc v. Poland, 2012, §§ 86, 94.

მოთხოვნა.[235] მონაცემთა დამმუშავებელმა აგრეთვე უნდა შეაფასოს, შეეხება თუ არა მოთხოვნა მონაცემთა სუბიექტის შესახებ დამუშავებულ ყველა მონაცემს, თუ მხოლოდ ნაწილს.[236] მონაცემთა სუბიექტს არ მოეთხოვება, გამოიყენოს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ განსაზღვრული საკომუნიკაციო არხები და ამის ნაცვლად შეუძლია გაგზავნოს მოთხოვნა დამმუშავებლის ოფიციალურ მისამართზე.[237] ამასთანავე, მონაცემებზე წვდომის უზრუნველყოფის გზები შეიძლება განსხვავდებოდეს მონაცემთა მოცულობისა და განხორციელებული დამუშავების მოქმედებების სირთულის მიხედვით. თუ მოთხოვნაში სხვაგვარად არ არის მითითებული, მონაცემებზე წვდომის მოთხოვნა გაგებული უნდა იქნეს, როგორც მონაცემთა სუბიექტის შესახებ არსებულ ყველა პერსონალურ მონაცემზე წვდომის უზრუნველყოფა. მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შეუძლია სთხოვოს მონაცემთა სუბიექტს, დააკონკრეტოს მოთხოვნის ფარგლები, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს მონაცემთა დიდ რაოდენობას.[238]

აღსანიშნავია, რომ მონაცემებზე ხელმისაწვდომობის უფლების რეალიზაციის მასშტაბს განსაზღვრავს პერსონალური მონაცემების ცნების ფარგლები. მონაცემი, რომელიც დაექვემდებარა ფსევდონიმიზაციას, დეპერსონალიზებული მონაცემებისგან განსხვავებით, კვლავაც ინარჩუნებს პერსონალური მონაცემების სტატუსს. მონაცემებზე წვდომის უფლება შეეხება მოთხოვნის განმახორციელებელი პირის პერსონალურ მონაცემებს. ამდენად, აღნიშნული არ უნდა განიმარტოს ზედმეტად ვიწროდ და მონაცემებზე წვდომის უფლება შეიძლება გავრცელდეს მონაცემზე, რომლებიც შეეხება მესამე პირებსაც, მაგალითად, კომუნიკაციის ისტორია, რომელიც მოიცავს შემომავალ და გამავალ შეტყობინებებს.[239]

საერთაშორისო პრაქტიკის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, უარი განაცხადოს ისეთი მოთხოვნის განხორციელებაზე, რომელიც აშკარად უსაფუძვლო ან გადაჭარბებულია, ან დაადგინოს გონივრული საფასური ასეთი მოთხოვნებისთვის; აქვე, საგულისხმოა, რომ მონაცემთა სუბიექტისთვის

[235] EDPB, Guidelines 01/2022 on Data Subject Rights - Right of Access, Adopted on 28 March 2023, 3, <https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf>, [20.12.2023].
[236] იქვე, 3.
[237] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 15, 465.
[238] იქვე, 4.
[239] იქვე.

საფასურის დაკისრების შემთხვევაში, დამმუშავებელს უნდა შეეძლოს მოთხოვნის აშკარად უსაფუძვლო ან გადაჭარბებული ხასიათის დემონსტრირება.[240]

არასრულწლოვნის სახელით მშობლის ან კანონიერი წარმომადგენლის მიერ მონაცემებზე წვდომის უფლების განხორციელებისას, გასათვალისწინებელია, რომ ბავშვის საუკეთესო ინტერესები, როგორც ძირითადი ორიენტირი პერსონალურ მონაცემებზე წვდომის უფლების განხორციელებაზე გადაწყვეტილების მიღებისას. ამასთანავე, მიზანშეწონილია, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა მიიღოს შესაბამისი ტექნიკური თუ ორგანიზაციული ზომები უფლებამოსილების არმქონე პირისთვის არასრულწლოვანთა პერსონალური მონაცემების ყოველგვარი გამჟღავნების, შესაბამისად, არაუფლებამოსილი წვდომის თავიდან ასაცილებლად. თუმცა აქვე აღსანიშნავია, რომ ეროვნული კანონმდებლობა შეიძლება, ითვალისწინებდეს მშობლის ან კანონიერი წარმომადგენლის უფლებას, მოითხოვოს და მიიღოს ინფორმაცია არასრულწლოვანთან დაკავშირებით (მაგალითად, ინფორმაცია ბავშვის აკადემიური მოსწრებისა და შეფასების შესახებ).[241]

4.3. მონაცემთა გასწორების, განახლების, დამატების მოთხოვნის უფლებები

მოქმედი კანონმდებლობის თანახმად, მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია გაასწოროს, განაახლოს, დაამატოს, დაბლოკოს, წაშალოს ან გაანადგუროს მონაცემები, თუ ისინი არასრულია, არაზუსტია, არ არის განახლებული ან თუ მათი შეგროვება და დამუშავება განხორციელდა კანონის საწინააღმდეგოდ.[242]

კანონის ახალი რედაქციის თანახმად, მონაცემთა სუბიექტს გააჩნია მონაცემთა განახლების, გასწორებისა და შევსების (მონაცემთა გასწორების უფლება) უფლებები.[243]

---

[240] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 15, 466.

[241] EDPB, Guidelines 01/2022 on Data Subject Rights - Right of Access, Adopted on 28 March 2023, paras. 83-87, <https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf>, [20.12.2023].

[242] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 22, კანონის მოქმედი რედაქცია, ერთად აჯგუფებს განსხვავებული ბუნების მქონე უფლებებს. აღნიშნულ მიდგომას არ ითვალისწინებს „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი. წინამდებარე ნაშრომი ითვალისწინებს კანონის ახალი რედაქციის მიდგომებს და შინაარსობრივად ერთი ტიპის უფლებათა შინაარს განიხილავს ერთად.

[243] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 15.

აღნიშნული მჭიდრო კავშირშია მონაცემთა სიზუსტისა და განახლების პრინციპთან, რომელიც ავალდებულებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, მიიღოს ყველა ზომა, რათა არაზუსტი მონაცემები წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე.[244] დამმუშავებელი ვალდებულია მონაცემთა ყველა მიმღებს, აგრეთვე, ამავე მონაცემთა ყველა სხვა დამუშავებისთვის პასუხისმგებელ პირს და დამუშავებაზე უფლებამოსილ პირს, რომლებსაც თავად გადასცა მონაცემები, შეატყობინოს მონაცემთა განახლებისა და შევსების შესახებ, გარდა იმ შემთხვევისა, როდესაც ასეთი ინფორმაციის მიწოდება შეუძლებელია დამმუშავებლების, უფლებამოსილი პირების ან მონაცემთა მიმღებების სიმრავლის ან/და არაპროპორციულად დიდი დანახარჯის გამო. ზემოთ აღნიშნული პირები შესაბამისი ინფორმაციის მიღების შემდეგ, ვალდებულნი არიან გონივრულ ვადაში გაასწორონ, განაახლონ ან/და შეავსონ მონაცემები. აღნიშნულით მონაცემთა სუბიექტს ეძლევა შესაძლებლობა თავიდან აირიდოს მის შესახებ არსებული არაზუსტი, მცდარი პერსონალური მონაცემების გავრცელება.[245]

მონაცემთა გასწორების უფლება წარმოადგენს მონაცემთა სუბიექტის უფლებამოსილების ილუსტრირებას მის შესახებ არსებული მონაცემების კონტროლთან (მათ შორის, მონაცემთა ხარისხის კონტროლთან) დაკავშირებით. მონაცემთა გასწორების უფლება არსობრივად მონაცემთა სუბიექტის მიერ წვდომის უფლების განხორციელებას უკავშირდება, რამდენადაც იმ შემთხვევაში თუკი მონაცემთა სუბიექტს არ ექნება წვდომა საკუთარ მონაცემებზე, მას არ შეეძლება, შეაფასოს დამუშავებული პერსონალური მონაცემების სიზუსტე, სისრულე ან განახლების საჭიროება.

აღსანიშნავია, რომ მონაცემთა გასწორების უფლება იყო ერთ-ერთი პირველი უფლება, რომელიც მინიჭებული იქნა მონაცემთა სუბიექტებისთვის მონაცემთა დაცვასთან დაკავშირებულ საერთაშორისოსამართლებრივ ინსტრუმენტებში. „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციის (108-ე კონვენცია) მე-8 მუხლის “c” ქვეპუნქტი ითვალისწინებს, რომ ნებისმიერ პირს უნდა მიეცეს საშუალება, რამდენადაც ეს შესაძლებელია, გასწორდეს მასთან დაკავშირებული პერსონალური მონაცემები, თუ ეს მონაცემები დამუშავდა მონაცემთა დაცვის ძირითადი პრინციპების

[244] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023. მუხლი 4, პუნქტი, 1, ქვეპუნქტი „დ“. სიზუსტის პრინციპი ასევე გათვალისწინებულია მოქმედი კანონმდებლობის მე-4 მუხლით.

[245] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 15.

საწინააღმდეგოდ. კონვენციის განმარტებით ბარათში მითითებულია, რომ აღნიშნული ნიშნავს „მცდარი ან შეუსაბამო ინფორმაციის“ გამოსწორებას.[246]

როგორც ზემოთ აღინიშნა, მონაცემთა გასწორების უფლება გულისხმობს არასრული ინფორმაციის შევსების უფლებას, რომელიც განისაზღვრება მონაცემთა დამუშავების მიზნიდან გამომდინარე. მონაცემთა დამუშავების მიზნიდან გამომდინარე, ერთი და იგივე მონაცემები შეიძლება მიჩნეულ იქნას როგორც სრული, ისე — არასრული. არასრული მონაცემების შევსება ხორციელდება მონაცემთა იმ ნაწილით, რომელიც აკლდა მონაცემებს. მაგალითისთვის, ამგვარი გარემოება შეიძლება არსებობდეს ნასამართლობის გაქარწყლებასთან დაკავშირებითაც.[247]

ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) რამდენიმე საქმეში დაადგინა, რომ პერსონალური მონაცემების შენახვა და გავრცელება, მონაცემთა სუბიექტისთვის მის დამუშავებაზე უარის თქმის შესაძლებლობის წართმევით, წარმოადგენს ჩარევას პირადი ცხოვრების პატივისცემის უფლებაში.[248] სასამართლომ დაადგინა, რომ „ადამიანის უფლებათა ევროპული კონვენციის“ მონაწილე სახელმწიფოს აქვს პოზიტიური ვალდებულება, ფიზიკური პირების მიერ შესაბამისი მტკიცებულებების წარდგენის შემთხვევაში, შეცვალოს აღნიშნულ ფიზიკურ პირთან დაკავშირებული პერსონალური მონაცემები.[249] სასამართლომ აღნიშნა, რომ არა მხოლოდ ყალბი, არაზუსტი ინფორმაციის შენახვა, მაგრამ, ასევე, არასრული ინფორმაციის მიწოდება სხვა პირებისთვის (როგორიცაა, მაგალითად, განმცხადებლის გამამართლებელი განაჩენის ხსენების გამოტოვება) წარმოადგენს ჩარევას პირადი ცხოვრების ხელშეუხებლობის უფლებაში.[250]

მონაცემთა გასწორების უფლება არაერთ საქმეში განიხილა ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”). სასამართლომ მონაცემთა გასწორების უფლება დაუკავშირა სამართლებრივი დაცვის ქმედითი საშუალების ფუნდამენტურ უფლებას და განმარტა, რომ აღნიშნული ფუნდამენტური უფლების არსი არ იქნება დაცული, თუ ფიზიკურ პირს არ ექნება შესაძლებლობა, მიმართოს უფლების დაცვის

[246] CoE, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, para. 54, <https://rm.coe.int/16800ca434#:~:text=The%20object%20of%20this%20convention,of%20computers%20for%20administrative%20purposes>, [20.12.2023].
[247] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art.16, 473.
[248] ECtHR, Leander v Sweden, para. 48; ECtHR, Rotaru v Romania, para. 46.
[249] ECtHR, Ciubotaru v Moldova, paras. 58–59.
[250] ECtHR, Cemalettin Canli v Turkey, paras. 41–42.

სამართლებრივ საშუალებებს, რათა წვდომა ჰქონდეს საკუთარ პერსონალურ მონაცემებზე და მოითხოვოს ამგვარი მონაცემების გასწორება ან წაშლა.[251]

მართლმსაჯულების ევროპულმა სასამართლომ, ასევე, განიხილა პერსონალურ მონაცემებზე წვდომის მოთხოვნის უფლება კანდიდატის მიერ გამოცდაზე წარდგენილ წერილობით პასუხებსა და გამომცდელების მიერ აღნიშნულ დოკუმენტებზე დართულ ნებისმიერ შენიშვნასთან დაკავშირებით, იმ მოტივით, რომ აღნიშნული დოკუმენტები, სავარაუდოდ, ექვემდებარებოდა მონაცემთა გასწორების უფლებას. სასამართლომ ამგვარი მონაცემები მიიჩნია პერსონალურ მონაცემებად და განმარტა, რომ მომჩივანი უფლებამოსილი იყო გაცნობოდა ტესტის პასუხებს, რათა გადაემოწმებინა, ხომ არ იყო დაშვებული რაიმე სახის ტექნიკური ხარვეზი (მაგალითად, ტესტის პასუხების არევა), თუმცა, ცხადია, აღნიშნული არ გულისხმობდა არასწორად შევსებული ტესტების გასწორებას.[252]

აღნიშნული მიდგომის არსს კარგად განმარტავს საპოლიციო სექტორში პერსონალურ მონაცემთა დამუშავების შესახებ ევროკავშირის 2016 წლის დირექტივის პრეამბულის 47-ე პარაგრაფი, რომლის თანახმად, გასწორების უფლება შეეხება ფაქტებს; კერძოდ, მოსაზრებები არ შეიძლება შეფასდეს როგორც ზუსტი ან არაზუსტი, მაშინ როდესაც ფაქტები შეიძლება იყოს რეალური და მცდარი; შესაბამისად, გასწორებას ექვემდებარება ფაქტობრივი გარემოებები და არა — მოსაზრებები.[253]

მონაცემთა გასწორების უფლება ხაზგასმულია ევროპის საბჭოს მინისტრთა კომიტეტის რეკომენდაციაში, რომელიც შეეხება ციფრულ გარემოში ბავშვთა უფლებების დაცვას. რეკომენდაციის თანახმად, სახელმწიფოებმა უნდა უზრუნველყონ, რომ ბავშვებს ან/და მათ მშობლებს, მზრუნველებს ან კანონიერ წარმომადგენელს უნდა ჰქონდეთ უფლება, გამოიხმონ თანხმობა მონაცემთა დამუშავებაზე, ჰქონდეთ წვდომა მათ პერსონალურ მონაცემებზე და გაასწორონ ან წაშალონ ისინი, განსაკუთრებით კი იმ შემთხვევაში, თუ მონაცემთა დამუშავება უკანონოა ან აღნიშნული დამუშავება საფრთხეს უქმნის მონაცემთა სუბიექტის,

[251] CJEU, Case C-362/14, Schrems, para. 95.
[252] CJEU, Case C-434/16, Nowak, para. 49.
[253] 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, recital 47, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680>, [20.12.2023].

მოცემულ შემთხვევაში კი არასრულწლოვნის ღირსებას, უსაფრთხოებას ან პირადი ცხოვრების ხელშეუხებლობას.[254]

4.4. მონაცემთა დაბლოკვის უფლება

მოქმედი კანონმდებლობის 22-ე მუხლი მონაცემთა სუბიექტის სხვა უფლებებთან ერთად ადგენს პერსონალური მონაცემების დამუშავების დაბლოკვის მოთხოვნის უფლებას.[255] შედარებით კონტექსტში აღსანიშნავია, რომ ახალი კანონის მე-17 მუხლის თანახმად, მონაცემთა სუბიექტს ასევე აქვს უფლება, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მონაცემთა დაბლოკვა, თუ არსებობს ერთ-ერთი შემდეგი გარემოება: ა) მონაცემთა სუბიექტი სადავოს ხდის მონაცემების ნამდვილობას ან სიზუსტეს; ბ) მონაცემთა დამუშავება უკანონოა, თუმცა მონაცემთა სუბიექტი ეწინააღმდეგება მათ წაშლას და ითხოვს მონაცემთა დაბლოკვას; გ) მონაცემები საჭირო აღარ არის მათი დამუშავების მიზნის მისაღწევად, თუმცა მონაცემთა სუბიექტს ისინი სჭირდება საჩივრის/სარჩელის წარსადგენად; დ) მონაცემთა სუბიექტი მოითხოვს მონაცემთა დამუშავების შეწყვეტას, წაშლას ან განადგურებას და მიმდინარეობს ამ მოთხოვნის განხილვა; ე) არსებობს მონაცემების მტკიცებულებად გამოყენების მიზნით შენახვის აუცილებლობა. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, დაბლოკოს მონაცემები ზემოთ ჩამოთვლილი ერთ-ერთი წინაპირობის არსებობისას, გარდა იმ შემთხვევისა, როდესაც არსებობს კანონით გათვალისწინებული გარემოებები.[256]

მნიშვნელოვანია, განიმარტოს, რომ მონაცემთა დაბლოკვა გულისხმობს პერსონალური მონაცემების დამუშავების ყველა შესაძლო მოქმედების შეწყვეტას, გარდა მონაცემთა შენახვისა. მონაცემთა დაბლოკვის უფლება წარმოადგენს ერთგვარ დამხმარე უფლებას მონაცემთა დამუშავებასთან დაკავშირებულ სხვა ძირითად უფლებებთან (მაგალითად, მონაცემთა გასწორების ან მონაცემთა დამუშავების

[254] CoE, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, para. 34, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [20.12.2023].

[255] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 22.

[256] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 17.

გასაჩივრების უფლებები) მიმართებით.[257] მართლმსაჯულების ევროპულმა სასამართლომ საქმეზე: "*College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*" განიხილა, ერთი მხრივ, მონაცემებზე წვდომის უფლების შინაარსი, ხოლო მეორე მხრივ — ვალდებულების ის ტვირთი, რომელიც აწევს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, შეინახოს მონაცემები, რომელთა სხვა მიზნებისთვის გამოყენების უფლებაც მას არ გააჩნია. აღნიშნულ გადაწყვეტილებაში სასამართლომ დაადგინა, რომ წევრმა სახელმწიფოებმა უნდა დაიცვან სამართლიანი ბალანსი მონაცემთა სუბიექტის ინტერესებსა და მონაცემთა დამუშავებისთვის პასუხისმგებელ პირზე დაკისრებულ ტვირთს შორის ინფორმაციის შენახვასთან დაკავშირებით.[258]

მართლმსაჯულების ევროპული სასამართლოს პრაქტიკით დადგენილია, რომ მონაცემთა სუბიექტს შეუძლია, „ევროკავშირის ფუნდამენტური უფლებების ქარტიის" მე-7 და მე-8 მუხლებიდან გამომდინარე, მისი ფუნდამენტური უფლებების გათვალისწინებით, მოითხოვოს, რომ გარკვეული მონაცემები აღარ იყოს ხელმისაწვდომი ფართო საზოგადოებისთვის, მათ შორის, მონაცემები არ იყოს ხელმისაწვდომი ინტერნეტის საძიებო სისტემების შედეგის სახით. ასევე, ერთ-ერთ საქმეზე სასამართლომ დაადგინა და განსაზღვრა მონაცემთა დაბლოკვის შემდეგი მეთოდები: მონაცემთა ნაწილი აღარ იყო ხელმისაწვდომი მომხმარებლებისთვის და გამოქვეყნებული მონაცემები დროებით ამოღებული იქნეს ვებგვერდიდან.[259]

4.5. მონაცემთა წაშლისა და განადგურების მოთხოვნის უფლება

„დავიწყების უფლება" წარმოადგენს მონაცემთა სუბიექტის მოთხოვნას, წაიშალოს კონკრეტული მონაცემი, აგრეთვე, განსაკუთრებული გარემოებების საფუძველზე, მონაცემთა სუბიექტს შეუძლია, მოსთხოვოს ონლაინ საძიებო სისტემის ოპერატორს, გააუქმოს ძებნის შედეგებიდან ის ელექტრონული მისამართები, რომელთა მეშვეობით ხელმისაწვდომია პერსონალური მონაცემების შემცველი ინტერნეტ-წყარო.[260] მონაცემთა წაშლისა და განადგურების უფლებებს, მსგავსად ახალი კანონისა,

---

[257] European Commission, When should I exercise my right to restriction of processing of my personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_en>, [20.12.2023].

[258] CJEU, Case C-553/07, Rijkeboer, para. 64.

[259] Case C-131/12, Google Spain, para. 99.

[260] ბერნსდორფი ბ., საძიებო სისტემის ოპერატორები და „დავიწყების უფლება", პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, № 1, 2023, 55.

ითვალისწინებს მოქმედი კანონი.[261] ხოლო რაც შეეხება, ახალ კანონს, მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მის შესახებ მონაცემთა დამუშავების (მათ შორის, პროფაილინგის) შეწყვეტა, წაშლა ან განადგურება. აღსანიშნავია, რომ „დავიწყების უფლება“ არ წარმოადგენს აბსოლუტურ უფლებას და იგი არ არის უპირობოდ გარანტირებული, განსაკუთრებით კი მაშინ, როდესაც აღნიშნული უფლება უპირისპირდება ინფორმაციული საზოგადოების გამოხატვის თავისუფლებასა და ინფორმაციის უფლებას.[262] მაშასადამე, დამუშავებისთვის პასუხისმგებელ პირს უფლება აქვს, უარი თქვას მოთხოვნის დაკმაყოფილებაზე, თუ:

- არსებობს მონაცემთა დამუშავების კანონით გათვალისწინებული რომელიმე საფუძველი;
- მონაცემები მუშავდება სამართლებრივი მოთხოვნის ან შესაგებლის დასაბუთების მიზნით;
- მონაცემთა დამუშავება აუცილებელია გამოხატვის ან ინფორმაციის თავისუფლების უფლების განსახორციელებლად;
- მონაცემები მუშავდება კანონით გათვალისწინებული საჯარო ინტერესებისთვის არქივირების მიზნით, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის და მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლების განხორციელება შეუძლებელს გახდის ან მნიშვნელოვნად დააზიანებს დამუშავების მიზნების მიღწევას.[263]

„მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) პრეამბულის 65-ე პარაგრაფი განმარტავს მონაცემთა სუბიექტის დავიწყების უფლებას და ხაზს უსვამს მის განსაკუთრებულ აქტუალურობას არასრულწლოვნებთან მიმართებით; კერძოდ, მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება, წაშალოს მისი პერსონალური მონაცემები და აღნიშნული მონაცემები აღარ დაექვემდებაროს დამუშავებას, თუ პერსონალური მონაცემები აღარ არის საჭირო იმ მიზნებთან დაკავშირებით, რისთვისაც ისინი შეგროვდა ან სხვაგვარად მუშავდებოდა, როდესაც მონაცემთა სუბიექტი უარს ამბობს მონაცემთა დამუშავებასთან დაკავშირებით გაცემულ თანხმობაზე ან ეწინააღმდეგება მის შესახებ პერსონალური მონაცემების დამუშავებას, ან როდესაც მისი პერსონალური მონაცემების დამუშავება სხვაგვარად არ შეესაბამება

[261] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 22.

[262] ბერნსდორფი ბ., საძიებო სისტემის ოპერატორები და „დავიწყების უფლება“, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, № 1, 2023, 55.

[263] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023. მუხლი 16.

ამ მონაცემთა დაცვის ძირითად რეგულაციას. აღნიშნული უფლება განსაკუთრებით აქტუალურია, როდესაც მონაცემთა სუბიექტმა ბავშვობის ასაკში გამოთქვა თანხმობა მონაცემთა დამუშავებაზე, დაკავშირებული რისკების სათანადო შეფასების გარეშე. თუმცა, აღსანიშნავია, რომ პერსონალური მონაცემების შემდგომი შენახვა კანონიერია იმ შემთხვევებში, როდესაც აღნიშნული აუცილებელია, გამოხატვისა და ინფორმაციის თავისუფლების უფლების განსახორციელებლად, კანონიერი ვალდებულების შესასრულებლად, საზოგადოებრივი ინტერესებიდან გამომდინარე დაკისრებული ვალდებულებების შესასრულებლად და სხვა გარემოებებიდან გამომდინარე.[264]

ციფრულ გარემოში წაშლის უფლების ეფექტიანი განხორციელებისთვის, აღნიშნული ფართოდ უნდა განიმარტოს იმგვარად, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, რომელმაც პერსონალური მონაცემები საჯარო გახადა, დაეკისროს ვალდებულება, აცნობოს სხვა დამმუშავებლებს წაშლას დაქვემდებარებულ მონაცემებთან დაკავშირებული ყველა ბმული, ასლი ან რეპლიკა. ამგვარად, დამმუშავებელმა, არსებული ტექნოლოგიებისა და დამმუშავებლისთვის ხელმისაწვდომი საშუალებების გათვალისწინებით, უნდა განახორციელოს ყველა გონივრული ზომა, რათა აცნობოს მონაცემთა დამუშავებისთვის პასუხისმგებელ სხვა პირებს მონაცემთა სუბიექტის აღნიშნული მოთხოვნის შესახებ.[265]

წაშლის უფლებას ასევე ითვალისწინებს „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციის (108-ე კონვენცია) მე-8 (c) მუხლში, რომელიც ეხება მონაცემთა სუბიექტის უფლებას, მოითხოვოს მონაცემების გასწორება ან წაშლა, თუ აღნიშნული მონაცემების დამუშავება ეწინააღმდეგება შიდა კანონმდებლობით გათვალისწინებულ დებულებებს, რომლებიც უზრუნველყოფს 108-ე კონვენციის მე-5 და მე-6 მუხლებით განსაზღვრული ძირითადი პრინციპების განხორციელებას.[266]

ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) საქმეში: “*Węgrzynowski and Smolczewski v Poland”*, იმსჯელა და განიხილა მონაცემთა სუბიექტის „დავიწყების უფლება“. საქმის ფაქტობრივი გარემოებების თანახმად, საკითხი შეეხებოდა მედია საშუალებების მიერ კონკრეტული გაზეთის ვებგვერდის არქივიდან მომჩივნის შესახებ სტატიის ამოღებას, მას შემდეგ, რაც დადგინდა, რომ სტატიის გამოქვეყნებით დაირღვა მომჩივნის უფლებები. ადამიანის უფლებათა ევროპულ სასამართლოს უნდა

---

[264] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 17, 475-476.

[265] იქვე, 476.

[266] CoE, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, Para. 54, <https://rm.coe.int/16800ca434#:~:text=The%20object%20of%20this%20convention,of%20computers%20for%20administrative%20purposes>, [20.12.2023].

შეეჯერებინა გამოხატვის თავისუფლება, კერძოდ, პრესის თავისუფლება მომჩივნის პირადი ცხოვრების ხელშეუხებლობის უფლებასთან. ევროპულმა სასამართლომ მიიჩნია, რომ განმცხადებლის უფლებების დასაცავად ადეკვატური საშუალება იქნებოდა კომენტარის დამატება ვებგვერდზე განთავსებულ სტატიაზე, რომელიც საზოგადოებას მიაწვდიდა ინფორმაციას სასამართლოს მიერ მიღებული გადაწყვეტილებების შესახებ. ევროპული სასამართლოს განმარტების თანახმად, არქივიდან მთლიანი სტატიის წაშლა შეიძლება ისტორიის ხელახლა გადაწერის მცდელობის ტოლფასი ყოფილიყო, რაც წინააღმდეგობაში მოვიდოდა პრესის საჯარო ინტერნეტ არქივებზე წვდომის შესახებ საზოგადოების ლეგიტიმურ ინტერესთან, რომელიც დაცულია ადამიანის უფლებათა ევროპული კონვენციის მე-10 მუხლით.[267] აღსანიშნავია, რომ ადამიანის უფლებათა ევროპულმა სასამართლომ, ასევე, განიხილა მონაცემების წაშლის უფლება შემდეგ საკითხებთან მიმართებით:

- მედია საშუალებების პრაქტიკა, ხანგრძლივი ვადით შეინახონ საკუთარ ვებგვერდზე არქივები, რომლებიც შეიცავს პიროვნების პერსონალურ იმგვარ მონაცემებს, როგორიცაა გვარი, სახელი და ფოტო, რომლებიც წარსულში იყო გამოქვეყნებული;[268]
- დანაშაულის ჩადენაში ბრალდებული ან უბრალოდ ეჭვმიტანილი პირების შესაძლებლობა გარკვეული დროის გასვლის შემდეგ მოიპოვონ ხელისუფლების მიერ შეგროვებული პერსონალური მონაცემების (დნმ პროფილი, პირადობის ფოტოები და თითის ანაბეჭდები) წაშლის უფლება მონაცემთა ბაზებიდან, რომლებიც მიზნად ისახავს დანაშაულის პრევენციასა და დანაშაულთან ბრძოლას;[269]
- ინდივიდის უუნარობა მოითხოვოს მისი წინა ნასამართლობის წაშლა პოლიციის არქივებიდან გარკვეული პერიოდის გასვლის შემდეგ;[270]
- განმცხადებლების პერსონალური მონაცემების გაჭიანურებული შენახვა უსაფრთხოების სამსახურის არქივში, რომლებიც აღარ აკმაყოფილებდა „დემოკრატიულ საზოგადოებაში აუცილებლობის“ მოთხოვნას ქმედების ბუნებისა და განმცხადებლის ასაკის გათვალისწინებით.[271]

[267] ECtHR, Węgrzynowski and Smolczewski v Poland, paras. 65 and 66.

[268] ECtHR, M.L. and W.W. v. Germany, 2018.

[269] ECtHR, B.B. v. France, 2009; Gardel v. France, 2009; M.B. v. France, 2009; M.K. v. France, 2013; Brunet v. France, 2014; Ayçaguer v. France, 2017; Catt v. the United Kingdom, 2019; Gaughran v. the United Kingdom, 2020.

[270] ECtHR, M.M. v. the United Kingdom, 2012.

[271] ECtHR, Segerstedt-Wiberg and Others v. Sweden, 2006.

ასევე აღსანიშნავია, რომ ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეზე: "M.M. v. the United Kingdom", პოლიციის ჩანაწერში პირის მიმართ გაფრთხილების უვადო რეგისტრაციის გამო, კონვენციის მე-8 მუხლის დარღვევა დაადგინა.[272] სასამართლოს განმარტებით, წარსულში მოხდილი სასჯელი ან მიღებული გაფრთხილება, დროთა განმავლობაში, ქმედების ჩამდენი პირის პირადი ცხოვრების განუყოფელი ნაწილი გახდა. მიუხედავად იმისა, რომ კრიმინალური ბაზის მონაცემები, გარკვეული გაგებით, საჯარო ინფორმაცია იყო, მისი სისტემატური შენახვა ცენტრალურ ფაილებში ნიშნავდა, რომ მონაცემების გამჟღავნება შეიძლებოდა მოვლენიდან დიდი ხნის გასვლის შემდეგაც, როდესაც მონაცემთა სუბიექტის გარდა ყველა დაივიწყებდა ინციდენტს. სასამართლომ შემაშფოთებლად მიიჩნია ის ფაქტი, რომ გადასინჯვის კრიტერიუმები, მონაცემთა წაშლის შესაძლებლობასთან დაკავშირებით, იყო ძალზე შემზღუდველი და რომ წაშლის მოთხოვნა დაშვებული იყო მხოლოდ გამონაკლის შემთხვევებში.[273] სასამართლომ დაადგინა, რომ როდესაც სახელმწიფო უკიდურესად ზრდის დისკრეციის ფარგლებს მონაცემთა შენახვის სფეროში უფლებამოსილების მაქსიმალური გაზრდით, ანუ მონაცემების განუსაზღვრელი ვადით შენახვის დაწესებით, გადამწყვეტია, ეფექტური გარანტიების არსებობა, რომლებიც უზრუნველყოფენ მონაცემთა წაშლას, როდესაც მათი შენახვა ლეგიტიმურ მიზანთან შეუთავსებელი ხდება.[274]

მართლმსაჯულების ევროპული სასამართლოს ("CJEU") ძირითადი გადაწყვეტილება წაშლის უფლების შესახებ გახლავთ "Google Spain"-ის საქმე, რომელშიც ესპანელმა მოქალაქემ სთხოვა "Google Spain"-ს, ამოეღო ესპანურ გაზეთში განთავსებული ორი პუბლიკაციის ბმული მისი სახელის საძიებო სისტემაში მითითებისას წარდგენილი შედეგების სიიდან. აღნიშნული პუბლიკაციების საფუძველზე, ესპანეთის სამინისტროს დაკვეთით, გამოცხადდა უძრავი ქონების აუქციონი, რომელიც უკავშირდებოდა ინდივიდის სახელის მითითებით სოციალური უზრუნველყოფის ვალების ამოღებას.[275] სასამართლოს განმარტების თანახმად, მონაცემთა სუბიექტის უფლებების დაცვა უპირატესია სხვა ინტერესებთან შედარებით. თუმცა, ზოგიერთ შემთხვევაში, ფართო საზოგადოების ინტერესები შეიძლება აღემატებოდეს მონაცემთა სუბიექტის ინტერესებს. სასამართლოს განმარტა, რომ აღნიშნული დამოკიდებულია კონკრეტული ინფორმაციის ბუნებაზე, მის გავლენაზე მონაცემთა სუბიექტის პირად ცხოვრებასა და საზოგადოებრივ ინტერესზე, ფლობდეს აღნიშნულ ინფორმაციას.

[272] ECtHR, M.M. v. the United Kingdom, 2012, §§187-207.
[273] იქვე, § 202.
[274] ECtHR, Catt v. the United Kingdom, 2019, § 119; Gaughran v. the United Kingdom, 2020, § 94.
[275] Case C-131/12, Google Spain.

ინტერესის მნიშვნელობა კი შეიძლება განსხვავდებოდეს მონაცემთა სუბიექტის საზოგადოებრივი როლისა და მისი საჯარო ცხოვრებაში მონაწილეობის მიხედვით. [276]

4.6. თანხმობის გამოხმობის უფლება

მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, განმარტების გარეშე უარი განაცხადოს მის მიერვე გაცემულ თანხმობაზე და მოითხოვოს მონაცემთა დამუშავების შეწყვეტა ან/და დამუშავებულ მონაცემთა განადგურება.[277] საქართველოს კანონმდებლობის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. ამ შემთხვევაში, მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა, თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს. მონაცემთა სუბიექტს უფლება აქვს, თანხმობა გამოიხმოს იმავე ფორმით, რომლითაც თანხმობა განაცხადა. ამასთანავე, მონაცემთა სუბიექტს თანხმობის გამოხმობამდე უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს და მიიღოს ინფორმაცია თანხმობის გამოხმობის შესაძლო შედეგების შესახებ.[278] საგულისხმოა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა თანხმობის მიცემამდე უნდა აცნობოს მონაცემთა სუბიექტს აღნიშნული უფლების შესახებ. თანხმობის გამოხმობა ისეთივე ადვილი უნდა იყოს, როგორც თანხმობის გაცემა. მაგალითად, როდესაც თანხმობა გაცემულია ელექტრონული საშუალებებით, მისი გაუქმება ასევე შესაძლებელი იქნება თანაბრად მიზანშეწონილი საშუალებებით. თანხმობის გამოხმობა არ გულისხმობს თანხმობის გამოხმობამდე განხორციელებული მონაცემთა დამუშავების უკანონოდ ცნობას. აქვე აღსანიშნავია, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს აქვს მონაცემთა დამუშავების სხვა ლეგიტიმური საფუძველი, თანხმობის გაუქმება არ იწვევს მონაცემთა დამუშავების დასრულებას. მას არ მოეთხოვება წაშალოს პერსონალური მონაცემები, რომლებიც ლეგიტიმურად დამუშავდა მიღებული თანხმობის საფუძველზე, თუ არ არსებობს სხვა სამართლებრივი საფუძველი.[279] თუმცა, ასეთ შემთხვევებში, მონაცემთა სუბიექტს უნდა ეცნობოს მონაცემთა დამუშავების

[276] Case C-131/12, Google Spain, paras. 81 and 97.

[277] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 25.

[278] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მუხლი 20.

[279] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 7, 351.

კანონიერი საფუძვლის ცვლილების შესახებ.[280] მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დამუშავების დასაწყისშივე უნდა ჰქონდეს მკაფიოდ გამიჯნული მონაცემთა დამუშავება რომელ მიზანსა და რომელ კანონიერ საფუძველს ემყარება.[281] „მონაცემთა დაცვის ევროპული საბჭოს“ სახელმძღვანელო რეკომენდაციის თანახმად, როდესაც მონაცემთა სუბიექტი გამოიხმობს თანხმობას და მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს სურს, განაგრძოს პერსონალური მონაცემების სხვა კანონიერ საფუძველზე დაყრდნობით დამუშავება, დამმუშავებელმა უნდა აცნობოს მონაცემთა სუბიექტს მონაცემთა დამუშავების კანონიერი საფუძვლის ცვლილების შესახებ.[282]

მომსახურების გაწევის მიზნით, როდესაც სპეციფიკური მომხმარებლის ანგარიშის გამოყენებით ხორციელდება თანხმობის გაცხადება (მაგალითად, ვებგვერდის, აპლიკაციის, ავტორიზაციის, ე. წ. „ნივთების ინტერნეტის მოწყობილობის“ (“IoT”) ინტერფეისის ან ელექტრონული ფოსტით), მონაცემთა სუბიექტს უნდა შეეძლოს თანხმობის რაიმე სახის ზიანის მიღების გარეშე, იმავე ელექტრონული საშუალებების მეშვეობით გამოხმობა, რადგან სხვა საშუალების გამოყენებით თანხმობის გამოხმობა მოითხოვს ზედმეტ ძალისხმევას. აღნიშნული გულისხმობს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს თანხმობის გაუქმება უფასოდ ან მომსახურების ხარისხის დონის შემცირების გარეშე.[283]

საგულისხმოა, რომ ახალი კანონი განსაკუთრებულ ზომებს აწესებს ბავშვის, როგორც მონაცემთა სუბიექტის თანხმობის მიღებასთან დაკავშირებით.[284] ვინაიდან მონაცემთა დამუშავებაზე თანხმობის გამოხმობა, ინფორმირებული და თავისუფალი ნების საფუძველზე გაცემული თანხმობის მნიშვნელოვანი ელემენტია, თანხმობის გამოხმობაზე, ასევე, ვრცელდება ბავშვის უფლებების დაცვის დამატებითი გარანტიები.

4.7. მონაცემთა გადატანის — პორტირების უფლება

[280] იქვე.
[281] იქვე, paras. 115-118.
[282] იქვე, para. 120.
[283] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 2020, para. 114, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, [20.09.2023].
[284] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023. მუხლი 7.

ახალი კანონის მე-18 მუხლის თანახმად, მე-5 მუხლის პირველი პუნქტის „ა“ და „ბ“ ქვეპუნქტებითა[285] და მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით[286] გათვალისწინებული საფუძვლებით მონაცემთა ავტომატური დამუშავების შემთხვევაში, მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელი პირისგან სტრუქტურირებული, საზოგადოდ გამოყენებადი და მანქანურად წაკითხვადი ფორმატით მიიღოს მის მიერ მიწოდებული მონაცემები ან მოითხოვოს ამ მონაცემთა სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა, თუ აღნიშნული ტექნიკურად შესაძლებელია. მონაცემთა გადატანის უფლება მიზნად ისახავს, ხელი შეუწყოს მონაცემთა სუბიექტს გადაიტანოს, გადაიღოს ასლი ან მარტივად გადასცეს საკუთარი პერსონალური მონაცემები ერთი “IT” სისტემიდან მეორეს (იქნება ეს მონაცემთა სუბიექტის, სანდო მესამე მხარის, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი ახალი პირების დაცული სისტემები).[287]

მონაცემთა გადატანის უფლების ძირითადი ელემენტებია: პერსონალური მონაცემების მიღების უფლება; პერსონალურ მონაცემთა გადაცემის უფლება მონაცემთა დამუშავებისთვის პასუხისმგებელი ერთი პირიდან მეორისთვის; მონაცემთა დამუშავების კონტროლი.[288]

პერსონალურ მონაცემთა მიღების უფლება — უპირველეს ყოვლისა, მონაცემთა გადატანის უფლება არის მონაცემთა სუბიექტის უფლება, მიიღოს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ დამუშავებული პერსონალური მონაცემების ის ქვეჯგუფი, რომელიც შეეხება მას და შეინახოს აღნიშნული მონაცემები შემდგომი პირადი გამოყენებისთვის. ამგვარი შენახვა შეიძლება, მოხდეს პირადი მოწყობილობების ან პირადი ღრუბლოვანი სერვერების გამოყენებით, მონაცემთა დამუშავებისთვის პასუხისმგებელი სხვა პირებისთვის მონაცემების გადაცემის გარეშე; ამ თვალსაზრისით, მონაცემთა გადატანის უფლება ავსებს მონაცემებზე წვდომის უფლებას. მონაცემთა გადატანის ერთ-ერთი სპეციფიკა მდგომარეობს იმაში,

---

[285] მონაცემთა დამუშავება დასაშვებია, თუ არსებობს ერთ-ერთი შემდეგი საფუძველი: ა) მონაცემთა სუბიექტმა განაცხადა თანხმობა მის შესახებ მონაცემთა ერთი ან რამდენიმე კონკრეტული მიზნით დამუშავებაზე; ბ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტთან დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან მონაცემთა სუბიექტის მოთხოვნით გარიგების დასადებად.

[286] განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირის მიერ უზრუნველყოფილია მონაცემთა სუბიექტის უფლებებისა და ინტერესების დაცვის ამ კანონით გათვალისწინებული გარანტიები და არსებობს ერთ-ერთი შემდეგი საფუძველი: ა) მონაცემთა სუბიექტმა განაცხადა წერილობითი თანხმობა ერთი ან რამდენიმე კონკრეტული მიზნით განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე.

[287] Article 29 Data Protection Working Party, Guidelines on the right to data portability, 2017, 4, <https://ec.europa.eu/newsroom/article29/items/611233>, [20.09.2023].

[288] იქვე, 4-6.

რომ იგი სთავაზობს მარტივ გზას მონაცემთა სუბიექტებს, საკუთარი პერსონალური მონაცემების მართვისა და ხელახლა გამოყენებისთვის.[289]

პერსონალური მონაცემების გადაცემის უფლება მონაცემთა დამუშავებისთვის პასუხისმგებელი ერთი პირიდან მეორისთვის — გადატანის უფლება მონაცემთა სუბიექტებს ანიჭებს უფლებას, გადასცენ პერსონალური მონაცემები მონაცემთა დამუშავებისთვის პასუხისმგებელი ერთი პირიდან მეორეს, რაიმე დაბრკოლების გარეშე. მონაცემები ასევე შეიძლება, გადაეცეს უშუალოდ პასუხისმგებელი ერთი პირიდან მეორეს მონაცემთა სუბიექტის მოთხოვნით და იმ შემთხვევებში, როდესაც აღნიშნული ტექნიკურად შესაძლებელია. მიზანშეწონილია, დამმუშავებლებმა შეიმუშაონ თავსებადი ფორმატები, რომლებიც უზრუნველყოფს მონაცემთა პორტირებას, თუმცა დამმუშავებლისათვის ტექნიკურად თავსებადი დამუშავების სისტემების დანერგვის ან შენარჩუნების ვალდებულების წარმოშობის გარეშე. მონაცემთა გადატანის უფლების აღნიშნული ელემენტი აძლევს მონაცემთა სუბიექტებს შესაძლებლობას არა მხოლოდ მოიპოვონ და ხელახლა გამოიყენონ, არამედ გადასცენ მათ მიერ მიღებული მონაცემები მომსახურების სხვა მიმწოდებლებს.[290]

კონტროლი — მონაცემთა გადატანის უფლება უზრუნველყოფს პერსონალური მონაცემების მიღებისა და მათი დამუშავების უფლებას მონაცემთა სუბიექტის სურვილის შესაბამისად; მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც განიხილავენ მონაცემთა გადატანის მოთხოვნებს, არ არიან პასუხისმგებელნი მონაცემთა სუბიექტის ან პერსონალური მონაცემების მიმღები სხვა პირების მიერ მონაცემთა დამუშავებაზე.[291] ისინი მოქმედებენ მონაცემთა სუბიექტის სახელით, იმ შემთხვევაშიც, როდესაც პერსონალური მონაცემები პირდაპირ გადაეცემა მონაცემთა დამუშავებისთვის პასუხისმგებელ სხვა პირს. ამ მხრივ, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს არ ეკისრება პასუხისმგებლობა მიმღები პირის მიერ განხორციელებული დამუშავების მოქმედებების მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობაზე, იმის გათვალისწინებით, რომ მონაცემთა მიმღებ პირს არ ირჩევს მონაცემთა გამგზავნი. ამავდროულად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დააწესოს გარანტიები, რათა დარწმუნდეს, რომ ნამდვილად მოქმედებს მონაცემთა სუბიექტის სახელით. მაგალითად, მას შეუძლია დააწესოს პროცედურები, რათა უზრუნველყოს, რომ გადაცემული პერსონალური მონაცემები მართლაც იყოს იმ შინაარსითა და ფორმით

[289] იქვე, 4-5.
[290] იქვე, 5.
[291] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 20, 504-505.

წარდგენილი, რა სახითაც მათი გადაცემა სურს მონაცემთა სუბიექტს. ეს შეიძლება, განხორციელდეს მონაცემთა გადაცემამდე მონაცემთა სუბიექტისგან დადასტურების მოპოვებით, დამუშავებაზე თავდაპირველი თანხმობის გაცემისას ან შესაბამისი ხელშეკრულების პირობების ფორმირებისას.[292]

მონაცემთა სუბიექტის რეალური ნების აღსრულება განსაკუთრებით მნიშვნელოვანი შეიძლება იყოს ბავშვებთან მიმართებით, ვინაიდან მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს წარმოეშობა დამატებითი ვალდებულებები უფლების შინაარსისა და განხორციელების უშუალო ფორმის არასრულწლოვნისათვის გასაგები ენით განმარტებასთან დაკავშირებით.

4.8. ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღება და მასთან დაკავშირებული უფლებები

ახალი კანონის მე-19 მუხლის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, არ დაექვემდებაროს მხოლოდ ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე, მიღებულ გადაწყვეტილებას, რომელიც მისთვის წარმოშობს სამართლებრივ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს, გარდა იმ შემთხვევისა, როდესაც პროფაილინგის საფუძველზე გადაწყვეტილების მიღება ეფუძნება მონაცემთა სუბიექტის აშკარად გამოხატულ თანხმობას, აუცილებელია მასსა და დამუშავებისთვის პასუხისმგებელ პირს შორის ხელშეკრულების დასადებად ან ხელშეკრულების შესასრულებლად, გათვალისწინებულია კანონით ან კანონის საფუძველზე დელეგირებული უფლებამოსილების ფარგლებში გამოცემული კანონქვემდებარე ნორმატიული აქტით.

პროფაილინგი და გადაწყვეტილების ავტომატიზებული მიღება ტენდენციურია როგორც კერძო, ისე საჯარო სექტორში. ტექნოლოგიურმა პროგრესმა და დიდი მოცულობის მონაცემების ანალიტიკის, ხელოვნური ინტელექტისა და მანქანათმცოდნეობის შესაძლებლობებმა გააადვილა პროფილების შექმნა და ავტომატიზებული გადაწყვეტილებების მიღება, რომელთაც არსებითი ზეგავლენა აქვთ ინდივიდების უფლებებსა და თავისუფლებებზე.[293] პერსონალური მონაცემების ფართო ხელმისაწვდომობას ინტერნეტსა და ე. წ. „ნივთების ინტერნეტის მოწყობილობების“ (“IoT”) გამოყენებით, კორელაციების პოვნისა და კავშირების

[292] Article 29 Data Protection Working Party, Guidelines on the right to data portability, 2017, 6, <https://ec.europa.eu/newsroom/article29/items/611233>, [20.09.2023].

[293] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, 5, < https://ec.europa.eu/newsroom/article29/items/612053/en >, [20.09.2023].

შექმნის უნარს შეუძლია ინდივიდის პიროვნული მახასიათებლების, ქცევის, ინტერესებისა და ჩვევების ასპექტების განსაზღვრა, ანალიზი და პროგნოზირება.[294]

პროფაილინგი და გადაწყვეტილების ავტომატიზებული მიღება შეიძლება, სასარგებლო იყოს ინდივიდებისა და ორგანიზაციებისთვის, რაც უზრუნველყოფს გაზრდილ ეფექტურობასა და რესურსების დაზოგვას.[295] თუმცა, აღნიშნული პროცესები რისკის შემცველია ფიზიკურ პირთა უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით, რაც მოითხოვს შესაბამისი გარანტიების უზრუნველყოფას. 29-ე სამუშაო ჯგუფის სახელმძღვანელო რეკომენდაციის თანახმად, ზოგიერთ შემთხვევაში, პროფაილინგმა შეიძლება, გამოიწვიოს არაზუსტი პროგნოზები, სხვა შემთხვევებში კი — მომსახურების უარყოფა და გაუმართლებელი დისკრიმინაცია.[296]

პროფაილინგი არის პროცედურა, რომელიც შეიძლება მოიცავდეს სტატისტიკურ დედუქციებს. იგი ხშირად გამოიყენება ადამიანების შესახებ პროგნოზების გასაკეთებლად, სხვადასხვა წყაროდან მიღებული მონაცემების გამოყენებით ინდივიდის შესახებ დასკვნების მომზადების მიზნით, პირის სხვა თვისებებზე დაყრდნობით, რომლებიც სტატისტიკურად მსგავსია.[297] ზოგადად, პროფაილინგი ნიშნავს ინდივიდის ან ინდივიდთა ჯგუფის შესახებ ინფორმაციის შეგროვებას და მათი მახასიათებლების ან ქცევის ნიმუშების შეფასებას, მათი კატეგორიზაციის მიზნით, კერძოდ, ანალიტიკური შეფასების ან/და წინასწარი პროგნოზის გაკეთების მიზნით, ისეთ საკითხებთან დაკავშირებით, როგორიცაა, მაგალითად, დავალების შესრულების უნარი, ინტერესები ან სავარაუდო ქცევა.[298]

საგულისხმოა, რომ გადაწყვეტილების ავტომატიზებულ მიღებას განსხვავებული ფარგლები აქვს და შეიძლება ნაწილობრივ გადაფაროს ან თან სდევდეს პროფაილინგს. გადაწყვეტილების მხოლოდ ავტომატიზებული მიღება არის გადაწყვეტილების მიღების უნარი ტექნოლოგიური საშუალებებით, ფიზიკური პირის ჩარევის გარეშე. ავტომატიზებული გადაწყვეტილებები შეიძლება, დაეფუძნოს ნებისმიერი ტიპის მონაცემს, მაგალითად, უშუალოდ დაინტერესებული პირების მიერ მიწოდებულ მონაცემებს (როგორიცაა კითხვარზე პასუხები); ინდივიდების შესახებ დაკვირვების შედეგად მიღებულ მონაცემებს (როგორიცაა აპლიკაციის საშუალებით შეგროვებული მდებარეობის მონაცემები); დასკვნით მონაცემებს, როგორიცაა პიროვნების უკვე

[294] იქვე.
[295] იქვე.
[296] იქვე, 6.
[297] იქვე, 7.
[298] იქვე.

შექმნილი პროფილები (მაგალითად, საკრედიტო ქულა).[299] ავტომატიზებული გადაწყვეტილებების მიღება შესაძლებელია პროფაილინგით ან მის გარეშე, ხოლო პროფაილინგი შეიძლება, მოხდეს ავტომატიზებული გადაწყვეტილებების მიღების გარეშე. ამავდროულად, მარტივი ავტომატიზებული გადაწყვეტილების მიღების პროცესი შეიძლება, ემყარებოდეს პროფაილინგს.[300]

სრულად ავტომატიზებული გადაწყვეტილების მიღებისა და პროფაილინგის დროს არასრულწლოვანი მონაცემთა სუბიექტის დაცვის განსაკუთრებით მაღალი ინტერესი არსებობს. „მონაცემთა დაცვის ძირითადი რეგულაცია“ ქმნის დამატებით ვალდებულებებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის, როდესაც ისინი ამუშავებენ არასრულწლოვანთა პერსონალურ მონაცემებს.[301] რეგულაციის პრეამბულის 71-ე პარაგრაფის თანახმად, მხოლოდ ავტომატიზებული გადაწყვეტილების მიღება, მათ შორის, პროფაილინგი, ლეგალური ან მსგავსი მნიშვნელოვანი ეფექტით, არ უნდა გავრცელდეს ბავშვებზე. თუმცა, იმის გათვალისწინებით, რომ აღნიშნული ფორმულირება არ არის ასახული „მონაცემთა დაცვის ძირითადი რეგულაციის“ შესაბამის მუხლში, 29-ე მუხლის სამუშაო ჯგუფი არ მიიჩნევს, რომ 71-ე პუნქტის დათქმა წარმოადგენს ამ ტიპის დამუშავების აბსოლუტურ აკრძალვას ბავშვებთან მიმართებით.[302] რეგულაციის 22-ე მუხლი არ კრძალავს ბავშვთან მიმართებით მხოლოდ ავტომატიზებული გადაწყვეტილების მიღებას, თუკი მას არ ექნება სამართლებრივი ან მსგავსი მნიშვნელოვანი ეფექტი ბავშვზე.[303] ბავშვების მიმართ ავტომატიზებული გადაწყვეტილების მიღების ან პროფაილინგის შემთხვევაში უნდა არსებობდეს შესაბამისი გარანტიები, რომლებიც არასრულწლოვანთა საუკეთესო ინტერესების შესაბამისი იქნება. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს აღნიშნული გარანტიების ეფექტიანობა ბავშვების, როგორც მონაცემთა სუბიექტების, უფლებების, თავისუფლებებისა და ლეგიტიმური ინტერესების დასაცავად.[304]

ვინაიდან ბავშვები წარმოადგენენ საზოგადოების უფრო დაუცველ ჯგუფს, ორგანიზაციებმა, ზოგადად, თავი უნდა შეიკავონ მარკეტინგული მიზნებისთვის მათი პროფაილინგისგან. ბავშვები შეიძლება იყვნენ განსაკუთრებით მგრძნობიარენი ონლაინ გარემოში და უფრო ადვილად მოექცნენ ქცევითი რეკლამის გავლენის ქვეშ.

[299] იქვე, 8.
[300] იქვე.
[301] GDPR, Recital, para. 71.
[302] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, 28, < https://ec.europa.eu/newsroom/article29/items/612053/en >, [20.09.2023].
[303] იქვე, 29.
[304] იქვე, 28.

მაგალითად, ონლაინ თამაშებში პროფაილინგი შეიძლება გამოყენებულ იქნას იმ მოთამაშეებისთვის, რომლებიც ალგორითმის თანახმად, მეტად არიან მიდრეკილები თამაშში ფულის დახარჯვისკენ. ბავშვის ასაკმა და განვითარების დონემ შეიძლება, გავლენა მოახდინოს მის უნარზე, გაიაზროს აღნიშნული ტიპის მარკეტინგის მოტივაცია ან შედეგები.[305]

4.9. გასაჩივრების უფლება

მონაცემთა სუბიექტს უფლება აქვს, მისი უფლებების დარღვევის შემთხვევაში, კანონით დადგენილი წესით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს[306] ან სასამართლოს, ხოლო თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი საჯარო დაწესებულებაა, საჩივრის წარდგენა შესაძლებელია აგრეთვე იმავე ან ზემდგომ ადმინისტრაციულ ორგანოში. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი მონაცემთა სუბიექტის მიმართვას განიხილავს კანონითა და პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტებით დადგენილი წესით.[307]

პერსონალურ მონაცემთა დაცვის სამსახური არის მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანო, რომლის ერთ-ერთ ფუნქციასაც საქართველოში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი წარმოადგენს. მონაცემთა დაცვის საზედამხედველო ორგანო არის დამოუკიდებელი საჯარო ორგანო, რომელიც ზედამხედველობს მონაცემთა დაცვის კანონმდებლობის განხორციელებას, პერსონალურ მონაცემთა დამუშავების კანონიერებაზე კონტროლის განხორციელებითა და სხვადასხვა პრევენციული ღონისძიებების გამოყენებით. ამასთანავე, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო გასცემს კონსულტაციებს და განიხილავს მონაცემთა დაცვის კანონმდებლობის დარღვევასთან დაკავშირებულ საჩივრებს.[308]

საერთაშორისოსამართლებრივ კონტექსტში აღსანიშნავია, რომ „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“

[305] იქვე, 29.

[306] დამატებითი ინფორმაცია, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის ოფიციალურ ვებგვერდზე: <www.personaldata.ge>.

[307] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 28/12/2011, მუხლი 26.

[308] European Commission, What are Data Protection Authorities (DPAs), <https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en>, [20.12.2023].

ევროპის საბჭოს მოდერნიზებული კონვენცია (108+ კონვენცია) აღიარებს მონაცემთა სუბიექტის უფლებას, კონვენციით გათვალისწინებული უფლებებით სარგებლობისას, დაიხმაროს საზედამხედველო ორგანო, მისი წარმომავლობისა და საცხოვრებელი ადგილის მიუხედავად.[309] ამასთანავე, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ თანახმად, საზედამხედველო ორგანოებმა უნდა მიიღონ შესაბამისი ღონისძიებები, რომლებიც ხელს შეუწყობს საჩივრების წარდგენას ისეთი ფორმით, რომელთა შევსება ელექტრონულადაც არის შესაძლებელი, კომუნიკაციის სხვა საშუალებების გამორიცხვის გარეშე.[310]

4.10. პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკა

- *სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა, დაზარალებულთა დახმარების სააგენტოს შემოწმება*

პერსონალურ მონაცემთა დაცვის სამსახურმა სახელმწიფო ზრუნვის ქვეშ მყოფი არასრულწლოვნის განცხადების საფუძველზე შეისწავლა სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა, დაზარალებულთა დახმარების სააგენტოს (შემდგომში - სააგენტო) მიერ მისი ინფორმირების კანონიერება.

განცხადების განხილვის ფარგლებში დადგინდა, რომ არასრულწლოვნის თანხმობით, მისმა წარმომადგენელმა, სააგენტოდან წერილობითი ფორმით ორჯერ გამოითხოვა არასრულწლოვანთან დაკავშირებული ინფორმაცია და დოკუმენტაცია. პირველ შემთხვევაში, გამოთხოვილ იქნა არასრულწლოვნის საცხოვრებლის შეცვლის მიზეზისა და მის მიმართ გაწეული სერვისების თაობაზე ინფორმაცია, ასევე, არასრულწლოვნის მონაცემების შემცველი დოკუმენტაცია. მეორე შემთხვევაში კი - დამატებითი ინფორმაცია დროის კონკრეტულ პერიოდში არასრულწლოვნის მიერ მცირე საოჯახო ტიპის სახლის დატოვებასთან დაკავშირებით.

მოთხოვნების საპასუხოდ, სააგენტომ არასრულწლოვნის წარმომადგენელს, ორივე ჯერზე წერილობით აცნობა, რომ მოთხოვნილი ინფორმაციის და დოკუმენტაციის მიწოდება განხორციელდებოდა შესაბამისი რეგიონული ცენტრებიდან ინფორმაციის გამოთხოვის და მიღების შემდგომ. საბოლოოდ, სააგენტომ წარმომადგენელს სრულად გადასცა მოთხოვნილი ინფორმაცია და დოკუმენტაცია, თუმცა შეზღუდულ იქნა

[309] CoE, Convention 108 +, Convention for the Protection of Individuals with regard to the Processing of Personal Data, 2018, Article 18, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, [20.12.2023].
[310] GDPR, Article 57 (2).

მონაცემთა სუბიექტის (არასრულწლოვნის) უფლება - კანონით დადგენილ 10 დღიან ვადაში მიეღო გამოთხოვილი ინფორმაცია.

განცხადების განხილვის ფარგლებში დადგინდა, რომ გამოთხოვილი ინფორმაციისა და დოკუმენტაციის მისაწოდებლად საჭირო იყო სააგენტოს მიერ ინფორმაციის მიღება თავისი სხვადასხვა სტრუქტურული ერთეულებიდან. სააგენტოს სოციალური მუშაკის განმარტებით კი, სახელმწიფო ზრუნვაში მყოფი არასრულწლოვნისთვის მიწოდებული სერვისების შესახებ ინფორმაციას ამუშავებენ სოციალური მუშაკები, რომლებიც უძღვებიან შესაბამისი არასრულწლოვნის საქმეს, თუმცა მათი გრაფიკი გადატვირთულია. სოციალური მუშაკების დროის და შრომითი რესურსის გათვალისწინებით მონაცემთა სუბიექტისთვის დოკუმენტაციის გადაცემა შეიძლება შეფერხდეს სხვა პირების (ბენეფიციარების) ინტერესებიდან გამომდინარე. სააგენტოს პოზიციით, მოცემულ შემთხვევაშიც, არასრულწლოვნის წარმომადგენლის მიერ გამოთხოვილი ინფორმაციის გასაცემად საჭირო იყო სხვადასხვა რეგიონულ ცენტრში დაცული დოკუმენტების შეგროვება, გაანალიზება და დამუშავება, რაც სოციალური მუშაკების რესურსების, ასევე სხვადასხვა დაწესებულებებიდან მოგროვების საჭიროების გათვალისწინებით დაუყოვნებლივ ან/და 10 დღის ვადაში ვერ მოხერხდა.

მოცემულ შემთხვევაში, სოციალური მუშაობის და სააგენტოს სტრუქტურული თავისებურებების, მისი კომპეტენციური სპეციფიკის, განცხადების განხილვის ფარგლებში წარმოდგენილი ინფორმაციის და სააგენტოს განმარტებების მიხედვით სამსახურმა დადგინდა, რომ ვინაიდან მონაცემთა სუბიექტისთვის ინფორმაციის და მასალების გადაცემა სააგენტოს სხვადასხვა ტერიტორიული ერთეულიდან ინფორმაციის მოძიებას, ანალიზსა და დამუშავებას საჭიროებდა, სხვა არასრულწლოვნების (სააგენტოსთან დაკავშირებული ბენეფიციარების) მიმართ სოციალური მუშაობის შეუფერხებლად განხორციელების აუცილებლობიდან გამომდინარე, სააგენტომ კანონით დადგენილზე ხანგრძლივი ვადის გამოყენებით თანაზომიერად შეზღუდა მონაცემთა სუბიექტის უფლება. აღნიშნულის მოლოდინი კი მონაცემთა სუბიექტს უნდა ჰქონოდა, ვინაიდან მონაცემთა დამმუშავებლის მიერ დაუყოვნებლივ ეცნობა ინფორმაციის მოძიების საჭიროების შესახებ. შესაბამისად, კანონით მინიჭებული მონაცემთა სუბიექტის უფლების შეზღუდვის საფუძვლისა და საჭიროების პროპორციული ზომით გამოყენების გათვალისწინებით, სააგენტოს მიერ მონაცემთა სუბიექტის ინფორმირებასთან დაკავშირებით ადმინისტრაციული სამართალდარღვევის ჩადენის ფაქტი არ გამოიკვეთა.

ამასთან, სამსახურის გადაწყვეტილებით აღინიშნა, რომ მართალია სააგენტომ განმცხადებელს აცნობა ინფორმაციის სხვადასხვა სტრუქტურული ერთეულებიდან

მოპოვების საჭიროებაზე, მაგრამ წერილებში ცალსახად არ იყო განმარტებული, რომ ინფორმაციის მიწოდება შეიძლება ვერ მომხდარიყო კანონით განსაზღვრულ ვადებში ან/და რა ვადაში იგეგმებოდა მისი მიწოდება. სამსახურმა გადაწყვეტილებაში მიუთითა „ბავშვის უფლებების შესახებ“ გაეროს კონვენციის მე-3 მუხლზე, რომლის თანახმადაც ბავშვების მიმართ ყველა მოქმედებაში, იმის მიუხედავად, მიმართავენ მას სოციალური უზრუნველყოფის საკითხებზე მომუშავე სახელმწიფო თუ კერძო დაწესებულებები, სასამართლოები, ადმინისტრაციული თუ საკანონმდებლო ორგანოები, უპირველესი ყურადღება ეთმობა ბავშვის საუკეთესო ინტერესების უზრუნველყოფას. სამსახურმა ასევე ხაზი გაუსვა, რომ როგორც წესი, მონაცემთა სუბიექტის მიერ ინფორმაციის/დოკუმენტაციის გამოთხოვის უფლების რეალიზება უშუალო კავშირშია სხვადასხვა სამართლებრივი წარმოების პროცესში საკუთარი უფლებების ჯეროვან განხორციელებასთან, აღნიშნული კი, განსაკუთრებულ მნიშვნელობას იძენს არასრულწლოვნის უფლებების დაცვისას. ამდენად, სამსახურის უფროსის გადაწყვეტილებით, სააგენტოს დაევალა მონაცემთა სუბიექტის უფლების შეზღუდვის ობიექტური საფუძვლების არსებობის შემთხვევაში მაქსიმალური სიცხადით მიაწოდოს მას ინფორმაცია უფლების შეზღუდვის მიზნისა და ვადის თაობაზე.

- *სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა დაზარალებულთა დახმარების სააგენტო*

პერსონალურ მონაცემთა დაცვის სამსახურმა სახელმწიფო ზრუნვაში მყოფი, შეზღუდული შესაძლებლობის მქონე არასრულწლოვნის მომართვის საფუძველზე შეისწავლა სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა დაზარალებულთა დახმარების სააგენტოს (შემდგომში - სააგენტო) მიერ მისი ინფორმირების კანონიერება.

შემოწმების ფარგლებში დადგინდა, რომ ბრაილის შრიფტით შედგენილი და შემდგომ სკოლის მასწავლებლის მიერ ხელით გადაწერილი წერილით 2022 წლის 13 დეკემბერს არასრულწლოვანმა სააგენტოდან გამოითხოვა თავისი პერსონალური მონაცემების შემცველი დოკუმენტაცია. სააგენტოს მითითებით, ვინაიდან მოთხოვნილი იყო მოცულობითი დოკუმენტაცია (200 გვერდამდე), მას არ გააჩნდა ასეთი მოცულობის დოკუმენტაციის დამუშავებისა და განმცხადებლისთვის აღქმადი, ბრაილის შრიფტით დაწერილი ფორმატით გადაცემის რესურსი. არასრულწლოვნისთვის დოკუმენტაციის გადაცემის გზის შეფასების მიზნით, სააგენტო დაუკავშირდა არასრულწლოვნის სკოლის დირექტორს, რომელმაც გამოთქვა მზადყოფნა - დოკუმენტაცია მიეღო და

გაეცნო არასრულწლოვნისთვის. თუმცა, ვინაიდან სკოლა წარმოადგენდა მესამე პირს (არ იყო არასრულწლოვნის ოფიციალური წარმომადგენელი), საქმისწარმოების მასალაში მითითებული სენსიტიური ინფორმაციის გათვალისწინებით, სააგენტომ მიზანშეწონილად არ მიიჩნია მოთხოვნილი დოკუმენტაციის სკოლისათვის ხელმისაწვდომობა.

შემოწმების ფარგლებში სააგენტოს განმარტებით, არასრულწლოვანი განცხადებაში მისამართად უთითებდა ერთ-ერთი ორგანიზაციის ოფიციალურ მისამართს. თუმცა, განცხადების წარდგენის პერიოდში აღნიშნული ორგანიზაციის თანამშრომლებზე არ იყო გაცემული შესაბამისი მინდობილობა, რაც მათ არასრულწლოვნის პერსონალური მონაცემების შემცველი მასალის მიღების/მოპოვების უფლებამოსილებას მიანიჭებდა. შესაბამისად, ორგანიზაციის ადვოკატებისთვის სათანადო უფლებამოსილების მინიჭებამდე სააგენტომ მიზანშეწონილად არ მიიჩნია მათ მისამართზე არასრულწლოვნის მონაცემების შემცველი დოკუმენტაციის გაგზავნა. ამასთანავე, სააგენტო მიუთითებდა, რომ 2022 წლის დეკემბერში არასრულწლოვანს დანიშნული ჰყავდა სოციალური მუშაკი, რომელიც იმყოფებოდა ბიულეტენზე, ხოლო 2023 წლის 01 იანვრიდან აღნიშნულ სოციალურ მუშაკსა და სააგენტოს შორის შეწყდა შრომითი ურთიერთობა. აღნიშნულის შემდგომ კი არასრულწლოვანს შეეცვალა სოციალური მუშაკი. ამდენად, სააგენტოს ადამიანური რესურსის და გამოთხოვილი მასალის მოცულობის გათვალისწინებით, სოციალური მუშაკის მიერ ვერ განხორციელდა შესაბამისი დოკუმენტების არასრულწლოვნისთვის გაცნობა და ვერ დაკმაყოფილდა არასრულწლოვნის 2022 წლის 13 დეკემბრის განცხადება.

არასრულწლოვნის უფლებების დამცველი ორგანიზაციის ადვოკატებმა, სააგენტოში 2023 წლის 27 იანვარს წარდგენილი განცხადებით მოითხოვეს არასრულწლოვნის უფლებების დაცვის მიზნით სააგენტოს მიერ მათთვის წარმომადგენლობითი უფლებამოსილების მინიჭება. აღნიშნულის საფუძველზე, 2023 წლის 06 თებერვალს სააგენტომ გასცა მინდობილობა და იმავე დღეს ამავე ორგანიზაციის ადვოკატს ხელზე გადაეცა არასრულწლოვნის პერსონალური მონაცემების შემცველი სრული დოკუმენტაცია.

აღსანიშნავია, რომ არასრულწლოვანზე ძალადობის თაობაზე აღძრული სისხლის სამართლის საქმის გამოძიების ფარგლებში, არასრულწლოვანთან დაკავშირებული საქმისწარმოების მასალები სააგენტოდან ასევე გამოითხოვა საქართველოს პროკურატურამ, რომელსაც არასრულწლოვნის მონაცემების შემცველი სრული მასალა სააგენტოს მიერ გაეგზავნა 2022 წლის 29 დეკემბერს.

საკითხის შესწავლის შედეგად პერსონალურ მონაცემთა დაცვის სამსახურმა (შემდგომში - სამსახური) გადაწყვეტილებაში აღნიშნა, რომ კანონმდებლობით დადგენილი მონაცემთა დამუშავების სტანდარტებიდან გამომდინარე მონაცემთა სუბიექტის მიერ მონაცემთა დამმუშავებლისთვის მიმართვის და მისი მონაცემების შემცველი დოკუმენტაციის გამოთხოვის უფლება წარმოადგენს მონაცემთა სუბიექტის უფლებების რეალიზების ერთ-ერთ მნიშვნელოვან წინაპირობას. ამ გზით, მონაცემთა სუბიექტს ეძლევა საშუალება და უფლება გაეცნოს თავისი მონაცემების შემცველ დოკუმენტებს, მოიპოვოს მათი ასლები და მიიღოს ინფორმაცია, რა კონტექსტში და რა ფორმით ხდება საკუთარი მონაცემების დამუშავება. აღნიშნული შესაძლებლობა მონაცემთა სუბიექტს უქმნის წარმოდგენას თავისი მონაცემების კანონიერად დამუშავების პროცესებზე და ეხმარება ინტერესების განსაზღვრასა და დაცვაში. სამსახურმა ხაზი გაუსვა, რომ აღნიშნული უფლების ეფექტური რეალიზება განსაკუთრებულ მნიშვნელობას იძენს, როდესაც საკითხი შეეხება შეზღუდული შესაძლებლობის მქონე ბავშვის კანონიერი ინტერესების უზრუნველყოფას და სხვადასხვა სამართალწარმოების ფარგლებში მისი ან/და მის მიერ არჩეული პირების კვალიფიციურ ჩართულობას, რაც მნიშვნელოვნადაა დაკავშირებული ბავშვის/მისი წარმომადგენლის სათანადო ინფორმაციით აღჭურვასთან. აღნიშნულთან მიმართებით სამსახურმა მიუთითა „ბავშვის უფლებათა კოდექსის“ მე-5 მუხლის პირველ, მე-2 და მე-3 ნაწილებზე, რომელთა თანახმად, ბავშვს უფლება აქვს, მასთან დაკავშირებული ნებისმიერი გადაწყვეტილების მიღებისას უპირატესობა მიენიჭოს მის საუკეთესო ინტერესებს, რომლებიც ბავშვისთვის ინდივიდუალურად, ამ კოდექსის, საქართველოს კონსტიტუციის, ბავშვის უფლებათა კონვენციის, მისი დამატებითი ოქმებისა და საქართველოს სხვა საერთაშორისო ხელშეკრულებების შესაბამისად განისაზღვრება. ბავშვის საუკეთესო ინტერესების განსაზღვრისას გათვალისწინებული უნდა იყოს მისი ოჯახურ გარემოში პიროვნული განვითარების უფლება, ბავშვის სოციალური და კულტურული მახასიათებლები, მის მიერ საკუთარი უფლებებისა და თავისუფლებების დამოუკიდებლად რეალიზების შესაძლებლობა და ბავშვის მოსაზრებები. ბავშვის საუკეთესო ინტერესებისთვის უპირატესობის მინიჭება (მათი უპირატესი გათვალისწინება) სავალდებულოა საქართველოს საკანონმდებლო, აღმასრულებელი და სასამართლო ხელისუფლებების ორგანოების, საჯარო დაწესებულების, ფიზიკური და იურიდიული პირების მიერ ბავშვთან დაკავშირებული ნებისმიერი გადაწყვეტილების მიღებისას ან/და ქმედების განხორციელებისას.

გადაწყვეტილებაში ასევე მითითებულია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს 1981 წლის 28

იანვრის კონვენციის მე-8 მუხლის „ბ“ ქვეპუნქტი, რომლის თანახმადაც, ნებისმიერ პირს უნდა შეეძლოს, საჭიროების შემთხვევაში, გარკვეული პერიოდულობითა და გადაჭარბებული დაგვიანებისა თუ დანახარჯების გარეშე, მონაცემთა ავტომატიზებულ ფაილში მასთან დაკავშირებული პერსონალური მონაცემების არსებობის ფაქტის დადასტურება, ასევე მისთვის მონაცემთა მიწოდება მისაღები ფორმით. ამასთან, მონაცემთა სუბიექტის მიერ, თავისი მონაცემების შემცველი მასალების მოთხოვნის უფლება და მოთხოვნის დაკმაყოფილების ფარგლები რეგულირებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 21-ე მუხლის მე-5 პუნქტით, რომლის შესაბამისად, პირს უფლება აქვს, გაეცნოს მის შესახებ საჯარო დაწესებულებაში არსებულ პერსონალურ მონაცემებს და მიიღოს ამ მონაცემების ასლები.

მითითებული სამართლებრივი და ფაქტობრივი გარემოებების გათვალისწინებით, სამსახურმა არ გაიზიარა სააგენტოს მიერ წარმოდგენილი არგუმენტაცია არასრულწლოვნის განცხადების დაკმაყოფილების გაჭიანურების მიზეზებთან დაკავშირებით. გადაწყვეტილებაში აღნიშნულია, რომ პერიოდი (2022 წლის 13 დეკემბრიდან 2023 წლის 06 თებერვლამდე), რომელიც სააგენტომ გამოიყენა განმცხადებლის მოთხოვნის დასაკმაყოფილებლად, მაშინ, როდესაც მოთხოვნილი დოკუმენტაცია მოძიებული იქნა გაცილებით მოკლე პერიოდში, რასაც მისი საქართველოს პროკურატურისთვის 2022 წლის 29 დეკემბერს გადაცემა ცხადყოფს, არასრულწლოვნის საუკეთესო ინტერესებთან თანმხვედრ, გონივრულ ვადად ვერ შეფასდება. შესაბამისად, სსიპ - სახელმწიფო ზრუნვისა და ტრეფიკინგის მსხვერპლთა დაზარალებულთა დახმარების სააგენტო ცნობილ იქნა სამართალდამრღვევად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 50-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში და ადმინისტრაციული სახდელის სახით შეეფარდა გაფრთხილება.

5. არასრულწლოვანთა მონაცემების დამუშავების საერთაშორისოსამართლებრივი ინსტრუმენტები და პრაქტიკა

5.1. არასრულწლოვანთა პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვა გაერთიანებული ერების სამართლებრივ სისტემაში

ადამიანის უფლებათა საყოველთაო დეკლარაციის ("UDHR")[311] მე-12 მუხლით საერთაშორისო დონეზე პირველად იქნა აღიარებული ადამიანის პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, რომლის თანახმად, დაუშვებელია ადამიანის პირად სივრცეში არამართლზომიერი ჩარევა. შეიძლება ითქვას, რომ მოცემულმა დეკლარაციამ საფუძველი ჩაუყარა ადამიანის უფლებათა საერთაშორისო სამართლის განვითარებას.[312] „ადამიანის სამოქალაქო და პოლიტიკური უფლებების შესახებ" საერთაშორისო პაქტის მე-17 მუხლის თანახმად, დაუშვებელია პირად სივრცეში, საცხოვრებელში ან მიმოწერის განხორციელებაში თვითნებური და უკანონო ჩარევა.[313]

აღსანიშნავია „ბავშვის უფლებების შესახებ" 1989 წლის კონვენცია ("CRC")[314], რომელიც განსაზღვრავს არასრულწლოვნის კეთილდღეობის მინიმალურ სტანდარტებს. მასში აღიარებულია ბავშვთა განსაკუთრებული ზრუნვისა და დაცვის საჭიროება.[315] კონვენცია ისტორიაში ყველაზე მეტი ქვეყნის მიერ არის რატიფიცირებული,[316] რომელმაც სახელმწიფოებს ბავშვებთან დაკავშირებული საკანონმდებლო მოწესრიგების ცვლილებებისკენ უბიძგა.[317] აღსანიშნავია, რომ ევროპის საბჭოსა და ევროპის კავშირის წევრი სახელმწიფოები წარმოადგენენ კონვენციის ხელშემკვრელ მხარეებს, რაც ხაზს უსვამს კონვენციის მნიშვნელობას ევროპის მასშტაბით. იგი ადგენს სახელმწიფოთა ვალდებულებას, შესაბამისმა ინსტიტუციებმა უზრუნველყონ ბავშვთა უფლებების დაცვა.[318]

კონვენციის ძირითადი პრინციპებია:

---

[311] United Nations (UN), Universal Declaration of Human Rights, 10 December, 1948.
[312] Handbook on European Data Protection Law, 2018 edition, 21.
[313] United Nations (UN), International Covenant on Civil and Political Rights, 16 December 1966.
[314] UN, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989.
[315] Children's rights in the digital environment: Moving from theory to practice, Best practice guideline, May 2021, 4, <https://www.betterinternetforkids.eu/documents/167024/200055/Best-practice+guideline+-+Childrens+rights+in+the+digital+environment+-+May+2021+-+v2+FINAL+CC+BY.pdf/f947d4f9-4ec4-49ae-5e2e-b6e9402c5fa2?t=1624532196598>, [11.08.2023].
[316] Unicef, Convention on the Rights of the Child, https://www.unicef.org/child-rights-convention#:~:text=In%201989%2C%20world%20leaders%20made,children's%20lives%20around%20the%20world, [11.08.2023].
[317] Unicef, for every child, Convention on the Rights of the Child for every child, every right, <https://www.unicef.org/child-rights-convention#:~:text=In%201989%2C%20world%20leaders%20made,children's%20lives%20around%20the%20world>, [15.08.2023].
[318] Handbook on European Law relating to the rights of the child, 2017, 27.

- *დისკრიმინაციის აკრძალვა:* ბავშვის უფლებები უნდა იქნას უზრუნველყოფილი ყოველგვარი დისკრიმინაციის გარეშე;
- *ბავშვის საუკეთესო ინტერესები:* ნებისმიერი გადაწყვეტილებისას ან ქმედების განხორციელებისას, რაც გავლენას ახდენს ბავშვებზე, უპირატესად უნდა იქნას გათვალისწინებული ბავშვის საუკეთესო ინტერესები;
- *ბავშვის სიცოცხლისა და განვითარების უფლება:* ყველა ბავშვს უნდა ჰქონდეს განვითარების შესაძლებლობა შესაბამისი გზით — ფიზიკურად, მენტალურად, სულიერად, მორალურად, სოციალურად და სხვა;
- *ბავშვის მოსაზრებების პატივისცემა:* ბავშვებს უნდა ჰქონდეთ შესაძლებლობა, მათთან დაკავშირებულ ნებისმიერ საკითხზე გამოხატონ საკუთარი შეხედულებები, მონაწილეობა მიიღონ მათ ცხოვრებასთან დაკავშირებული გადაწყვეტილების მიღების პროცესში ასაკისა და განვითარების დონის გათვალისწინებით.[319]

„ბავშვის უფლებების შესახებ“ 1989 წლის კონვენციის ფარგლებში, ბავშვების პერსონალური მონაცემების დაცვა გარანტირებულია მე-16 მუხლით, რომლის შესაბამისად: *„ბავშვი არ შეიძლება იყოს მისი პირადი ცხოვრების, ოჯახური ცხოვრების, საცხოვრებლის ხელშეუხებლობის ან კორესპონდენციის საიდუმლოების უფლების განხორციელებაში ნებისმიერი ან უკანონო ჩარევის ან მისი ღირსებისა და რეპუტაციის შელახვის ობიექტი*“. გასათვალისწინებელია, 1989 წელს, კონვენციის მიღების ეტაპზე, თანამედროვე ტექნოლოგიები არ იყო იმდენად განვითარებული, რამდენადაც დღეს და შესაბამისად, ბავშვებს არ ჰქონდათ აქტიური წვდომა ინტერნეტზე. ამდენად, უფლებების პირველადი სამართლებრივი კონცეფცია არ იყო მორგებული დღევანდელ ციფრულ რეალობას და ნაკლები იყო პერსონალურ მონაცემთა დარღვევის რისკი. აღსანიშნავია, რომ კონვენციის ცალკეული დებულება იძლევა ინტერპრეტაციის იმგვარ შესაძლებლობას, რათა ბავშვის უფლებები ჯეროვნად იქნას დაცული, მათ შორის, ციფრულ სივრცეში.[320]

2018 წლის დასაწყისში, ბავშვის უფლებათა კომიტეტმა ზოგადი კომენტარის შემუშავება გადაწყვიტა, რომელშიც წარმოდგენილი იქნებოდა კონვენციის ციფრულ

[319] Information Commissioner's Office (ICO), The United Nations Convention on the rights of the child and what it means for online services, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/the-united-nations-convention-on-the-rights-of-the-child/#:~:text=The%20UNCRC%20embodies%20the%20idea,been%20transformed%20in%20many%20areas>, [15.08.2023].

[320] Children's rights in the digital environment: Moving from theory to practice, Best practice guideline, May 2021, 4-5.

სამყაროსთან შესაბამისობის საკითხები. კომენტარი ძალაში 2021 წლის 24 მარტს შევიდა. მასში წარმოდგენილია, თუ როგორ უნდა იმოქმედონ სახელმწიფოებმა ციფრულ სამყაროში ბავშვის უფლებათა რეალიზებისთვის.[321] იმდენად, რამდენადაც ციფრული სამყარო მუდმივად განვითარებადია, არსებითად მნიშვნელოვანია ბავშვის უფლებების დაცვის სათანადო გარანტიების უზრუნველყოფა,[322] რა მიზნით, კონვენციის წევრ სახელმწიფოებში უნდა არსებობდეს საერთაშორისო სტანდარტების შესაბამისი ეროვნული კანონმდებლობა.[323]

5.2. ევროპის საბჭოს სამართლებრივი ჩარჩო არასრულწლოვანთა პერსონალურ მონაცემთა დაცვის შესახებ

ევროპის საბჭოს ფარგლებში პერსონალური მონაცემების დაცვის უფლება გარანტირებულია „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის“ მე-8 მუხლით,[324] რომელიც ადგენს პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის დაცვის უფლებასა და განსაზღვრავს აღნიშნულ უფლებათა შეზღუდვის წინაპირობებს. მე-8 მუხლის მე-2 პუნქტი ადგენს საჯარო ხელისუფლების მხრიდან უფლების შეზღუდვის მართლზომიერების განმსაზღვრელ სამ კრიტერიუმს: ა) კანონთან შესაბამისობა; ბ) კანონიერი მიზანი; გ) დემოკრატიულ საზოგადოებაში აუცილებლობა. ბავშვების პერსონალური მონაცემების სავარაუდო დარღვევის საკითხებიც სწორედ კონვენციის მე-8 მუხლის ფარგლებში ექცევა. შესაბამისად, ადამიანის უფლებათა ევროპული სასამართლოც ბავშვთა პერსონალური მონაცემების დარღვევის არსებობას აღნიშნული მუხლით გათვალისწინებული მოთხოვნების შესაბამისად ადგენს.

აღსანიშნავია, რომ პირველი იურიდიულად სავალდებულო საერთაშორისო დოკუმენტი — „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ“ ევროპის საბჭოს 1981 წლის კონვენცია (108-ე კონვენცია) და მისი დამატებითი ოქმი ვრცელდება კერძო და საჯარო სექტორებში მონაცემთა დამუშავებაზე და უზრუნველყოფს ფიზიკური პირის დაცვას, პერსონალური მონაცემების დამუშავებისას მათი უფლებების შესაძლო ხელყოფისაგან.[325] 108-ე

[321] UN Committee on the Rights of the Child, ‘General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment, 3.
[322] იქვე, 1.
[323] იქვე, 4.
[324] CoE, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.
[325] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 193.

კონვენციაში წარმოდგენილი პრინციპები უკავშირდება პერსონალური მონაცემების სამართლიან, ასევე, კანონიერ შეგროვებასა და დამუშავებას, რომელიც უნდა განხორციელდეს თავდაპირველად განსაზღვრული ლეგიტიმური მიზნებისთვის. ასევე, მონაცემები არ უნდა შეინახოს იმაზე ხანგრძლივი ვადით, ვიდრე საჭიროა. ამასთანავე, შესაბამისი სამართლებრივი დაცვის გარანტიების არარსებობისას, დაუშვებელია „განსაკუთრებული კატეგორიის“ პერსონალური მონაცემების დამუშავება. კონვენცია უზრუნველყოფს ინდივიდის, მათ შორის ბავშვის უფლებას, იცოდეს თუ რა ინფორმაცია ინახება მის შესახებ და საჭიროების შემთხვევაში, ჰქონდეს აღნიშნული ინფორმაციის შესწორების უფლება.[326]

5.2.1. ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის მიმოხილვა

ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) არაერთ გადაწყვეტილებაში იმსჯელა ბავშვის უფლებების დაცვის, ასევე, პირადი ცხოვრების ხელშეუხებლობის დაცვის საკითხებზე. გასათვალისწინებელია, რომ “ECtHR” ხშირად აკეთებს მითითებას გაეროს ბავშვის უფლებათა კონვენციაზე და დასაბუთებისას ეყრდნობა „ბავშვის უფლებების შესახებ“ 1989 წლის კონვენციის პრინციპებს. ევროპული სასამართლოს პრეცედენტული სამართალში ხაზგასმითაა აღნიშნული სახელმწიფოთა ვალდებულება, განახორციელონ ქმედითი ღონისძიებები ბავშვების პირადი ცხოვრების ხელშეუხებლობის უფლების დასაცავად. წინამდებარე თავში განხილულია ევროპული სასამართლოს რამდენიმე მნიშვნელოვანი გადაწყვეტილება, რაც წარმოადგენს სასამართლოს მიდგომებს ბავშვების პერსონალურ მონაცემთა დაცვის საკითხზე.

საქმეში: “*K.U. v. Finland*”[327] განმცხადებელს წარმოადგენდა ბავშვი, რომელიც ასაჩივრებდა ინტერნეტ სივრცეში, კერძოდ, ე. წ. „გაცნობის“ ვებგვერდზე, მისი სახელით განთავსებული სექსუალური შინაარსის განცხადებას. მომსახურების მიმწოდებელმა, ფინეთის კანონმდებლობაზე დაყრდნობით, კონფიდენციალურობასთან დაკავშირებული ვალდებულებების გამო უარი განაცხადა იმ პირის ვინაობის გამჟღავნებაზე, რომელმაც განათავსა აღნიშნული ინფორმაცია. მომჩივნის თქმით, ეროვნული კანონმდებლობა მისი უფლებების ჯეროვანი დაცვის გარანტიებს არ ითვალისწინებდა. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ სახელმწიფოებს ეკისრებათ პოზიტიური ვალდებულება, რომელიც

[326] იქვე.

[327] ECtHR, K.U. v. FINLAND, Appl. No. 2872/02, 2 December 2008, <https://hudoc.echr.coe.int/?i=001-89964>, [16.08.2023].

გულისხმობს პირადი ცხოვრების პატივისცემის უფლების უზრუნველსაყოფად შესაბამისი ღონისძიებების მიღებას ინდივიდებს შორის ურთიერთობის კონტექსტშიც. მოცემულ შემთხვევაში, სახელმწიფოს უნდა გადაედგა ეფექტიანი ნაბიჯები დანაშაულის ჩამდენი პირის იდენტიფიცირებისა და დასჯისთვის. ვინაიდან სახელმწიფომ ამგვარი ვალდებულება ვერ შეასრულა, სასამართლომ დაადგინა „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის“ მე-8 მუხლის დარღვევა.[328]

საქმე: *“Avilkina and Others v. Russia”*[329] შეეხება ორი წლის გოგოს სამედიცინო დოკუმენტაციის გამჟღავნებას პროკურორის მოთხოვნის საფუძველზე. მოთხოვნის მიზანს სისხლის გადასხმის თაობაზე იეჰოვას მოწმის უარის შესახებ ინფორმაციის მიღება წარმოადგენდა. სასამართლომ აღნიშნა, რომ დანაშაულის გამოძიების საჯარო ინტერესმა შესაძლოა, გადაწონოს პაციენტისა და, ზოგადად, საზოგადოების ინტერესი სამედიცინო დოკუმენტაციის კონფიდენციალურობის დაცვასთან მიმართებით. ამასთანავე, აღინიშნა, რომ სისხლისსამართლებრივ წარმოებაში მომჩივანი არ წარმოადგენდა არც ბრალდებულ და არც ეჭვმიტანილ პირს. მომჩივნის მკურნალ სამედიცინო პერსონალს შესაძლებლობა ჰქონდა სისხლის გადასხმის თაობაზე ნებართვის მისანიჭებლად მიემართა სასამართლოსთვის, თუ მიიჩნევდნენ, რომ პაციენტის სიცოცხლეს ემუქრებოდა საფრთხე. იქიდან გამომდინარე, რომ განმცხადებლის ჯანმრთელობასთან დაკავშირებული ინფორმაციის გამჟღავნებისათვის არ არსებობდა აუცილებელი სოციალური საჭიროება, ევროპულმა სასამართლომ დაადგინა „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის“ მე-8 მუხლის დარღვევა.[330]

საქმის: “*S. and Marper v. the United Kingdom*”[331] ფაქტობრივი გარემოებების თანახმად, საგამოძიებო ორგანოებმა, ყაჩაღობის მცდელობის ბრალდების გამო, მიუხედავად ხანდაზმულობის ვადის ამოწურვისა, თერთმეტი წლის ბავშვის თითის ანაბეჭდები და დნმ-ის ნიმუშები აიღეს. პერსონალური ინფორმაციის შენახვა, მისი ბუნებისა და მოცულობის გათვალისწინებით, გულისხმობდა პირველი მომჩივნის პირადი ცხოვრების პატივისცემის დაცულობის უფლებაში ჩარევას. ევროპის საბჭოს ფარგლებში მოქმედი ძირითადი პრინციპები და სხვა წევრი ქვეყნების

[328] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 191.

[329] Avilkina and Others V. Russia, Appl. No. 1585/09, 6 June 2013, <https://hudoc.echr.coe.int/eng?i=001-120071>, [17.08.2023].

[330] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 192.

[331] ECtHR, S. and Marper v. the United Kindgom [GC], Nos. 30562/04 and 30566/04, 4 December 2008, <https://hudoc.echr.coe.int/eng?i=001-61194>, [17.08.2023].

კანონმდებლობა, ასევე, პრაქტიკა წევრ სახელმწიფოებს ავალდებულებს, რომ პერსონალური მონაცემების შენახვა დამუშავების მიზნის პროპორციული იყოს; ამასთანავე, მაქსიმალურად იქნეს შეზღუდული დროში, რაც განსაკუთრებით აქტუალურია საპოლიციო სისტემისათვის. სასამართლოს შეფასებით, მონაცემთა შენახვის განუსაზღვრელი ვადა, მიუხედავად ქმედების სამართლებრივი ბუნებისა და სიმძიმისა, შემაშფოთებელი იყო. არასრულწლოვნების შემთხვევაში, პერსონალური მონაცემების შენახვა განსაკუთრებით საზიანო შეიძლებოდა ყოფილიყო, საზოგადოებაში მათი ინტეგრაციისა და განვითარების კონტექსტიდან გამომდინარე. შესაბამისად, სასამართლომ დაადგინა „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის“ კონვენციის მე-8 მუხლის დარღვევა, ვინაიდან მონაცემთა შენახვა წარმოადგენდა მომჩივნის პირადი ცხოვრების ხელშეუხებლობის უფლების დაცულ სფეროში არაპროპორციულ ჩარევას.[332]

5.2.2. ევროპის საბჭოს მინისტრთა კომიტეტის მიერ შემუშავებული დოკუმენტები

2018 წელს ევროპის საბჭოს მინისტრთა კომიტეტმა შეიმუშავა რეკომენდაცია, რომელშიც თავმოყრილია ციფრულ გარემოში ბავშვის უფლებების პატივისცემისა და დაცვის ძირითადი პრინციპები. აღნიშნული რეკომენდაცია არ არის შესასრულებლად სავალდებულო ძალის მქონე, თუმცა ეყრდნობა ევროსაბჭოს იურიდიულად მბოჭავ კონვენციებს, ასევე, ბავშვის უფლებების შესახებ გაერთიანებული ერების სტანდარტებსა და რეკომენდაციებს. სახელმძღვანელოში ხაზგასმულია სახელმწიფოების მხრიდან ბავშვის პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვისა და პატივისცემის მნიშვნელობა. ამასთან, გამოყოფილია ბავშვების პერსონალურ მონაცემთა დაცვასთან დაკავშირებული ძირითადი პრინციპები, კერძოდ, ბავშვის საუკეთესო ინტერესები; ბავშვის შესაძლებლობების განვითარება; დისკრიმინაციის აკრძალვა; ბავშვების მოსაზრებების გათვალისწინება; ბავშვებთან დაკავშირებული საკითხების გადაწყვეტისას ყველა მნიშვნელოვანი პირის ჩართვა. გარდა აღნიშნულისა, წარმოდგენილია ბავშვების უფლებების ჩამონათვალი, რომელთა დაცვა განსაკუთრებით მნიშვნელოვანია თანამედროვე ტექნოლოგიების ეპოქაში: ციფრულ გარემოზე წვდომა; გამოხატვისა და ინფორმაციის თავისუფლების უფლება; მონაწილეობის, თამაშის, შეკრებისა და გაერთიანების უფლება; პირადი

[332] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 192.

ცხოვრების ხელშეუხებლობა და მონაცემთა დაცვა; განათლების უფლება; დაცვისა და უსაფრთხოების უფლება; სამართლებრივი დაცვის საშუალებების უზრუნველყოფა.[333]

2019 წელს მინისტრთა კომიტეტმა გამოსცა რეკომენდაცია წევრი სახელმწიფოებისთვის ციფრული მოქალაქეობის სწავლების განვითარების თაობაზე, რომელშიც, სხვა საკითხებთან ერთად, ხაზი ესმევა ბავშვებისათვის ციფრული მოქალაქეობის განათლების უზრუნველყოფის მნიშვნელობას. ასევე, მითითებულია, რომ ხელი უნდა შეეწყოთ მშობლებს, ასევე, სხვა კანონიერ წარმომადგენლებს, რათა გააძლიერონ ბავშვების ციფრულ გარემოში ჩართულობა და დაიცვან შესაბამისი ბალანსი ონლაინ უსაფრთხოებასა და მათ მონაწილეობას შორის. საგულისხმოა მასწავლებლების როლიც ამ სფეროში.[334]

2021 წლის 28 აპრილს, ევროპის საბჭოს მინისტრთა კომიტეტმა მიიღო დეკლარაცია „ციფრულ გარემოში ბავშვების პირადი ცხოვრების ხელშეუხებლობის დაცვის საჭიროების შესახებ“, რომელიც განამტკიცებს გაეროს ბავშვის უფლებათა კონვენციისა და ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციით გათვალისწინებული უფლებების რეალიზაციას. დოკუმენტში ყურადღება ეთმობა რისკებს, რომლებსაც ბავშვი თანამედროვე ტექნოლოგიების გამოყენებისას აწყდება. ასევე, ხაზგასმით არის აღნიშნული კორონავირუსით (“Covid-19”) გამოწვეული პანდემიის პირობებში ბავშვების პირადი ცხოვრებისა და პერსონალური მონაცემების გაძლიერებული დაცვის მნიშვნელობა.[335]

გარდა ზემოაღნიშნულისა, ევროპის საბჭომ შეიმუშავა 2022-2027 წლების სტრატეგიის დოკუმენტი, რომელშიც ბავშვებთან დაკავშირებულ სხვა საკითხებთან ერთად ყურადღებაა გამახვილებული ბავშვების მიერ თანამედროვე ტექნოლოგიების გამოყენების საკითხებზე. დოკუმენტში გამოყოფილია ექვსი ძირითადი პრიორიტეტული მიმართულება, რომელთა შორის არის ყველა ბავშვისთვის ტექნოლოგიებზე წვდომის უზრუნველყოფა და მათი უსაფრთხო გამოყენება. მასში ასევე აღნიშნულია, რომ პანდემიამ (“Covid-19”), საგანმანათლებლო სისტემის ონლაინ

[333] Recommendation CM/Rec (2018)7 of the Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 4 July 2018, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7>, [18.08.2023].

[334] Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, <https://library.parenthelp.eu/wp-content/uploads/2019/12/CoE-digital-citizenship-education-recommendations-CM_Rec201910E.pdf>, [22.08.2023].

[335] Declaration by the Committee of Ministers on the need to protect children’s privacy in the digital environment, 28 April 2021, <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a2436a>, [23.08.2023].

სწავლების რეჟიმზე გადასვლამ ბავშვთა პერსონალური მონაცემების დაცვის თვალსაზრისით არაერთი რისკი წარმოშვა.[336]

5.3. არასრულწლოვანთა პერსონალურ მონაცემთა დაცვის მოწესრიგება ევროპის კავშირში

ევროპაში პირადი ცხოვრება და მონაცემთა დაცვის უფლებები მიიჩნევა დემოკრატიის ფუნდამენტად. „ფუნდამენტურ უფლებათა ევროპული კავშირის ქარტიის“[337] მე-7 მუხლი უზრუნველყოფს პირადი და ოჯახური ცხოვრების პატივისცემას, ხოლო მე-8 მუხლი ადგენს მონაცემთა დაცვის უფლებას და განსაზღვრავს ძირითად უფლებად. ამ უკანასკნელი მუხლის პირველ პუნქტით უზრუნველყოფილია მონაცემთა დაცვის უფლება, მისი მე-2 პუნქტი ადგენს მონაცემთა დაცვის არსებით პრინციპებს, ხოლო მე-3 პუნქტში ხაზგასმულია, რომ ამ პრინციპების იმპლემენტაცია უნდა უზრუნველყოს დამოუკიდებელმა საზედამხედველო ორგანომ.[338]

2018 წლის 25 მაისს, ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”)[339], რომელმაც პერსონალურ მონაცემთა დაცვის სფეროში დაამკვიდრა ახალი საერთაშორისო სტანდარტი. რეგულაციის მიზანია ტექნოლოგიური პროგრესისა და თანამედროვე გამოწვევების პირობებში ინდივიდთა უფლებების სათანადო დაცვა. “GDPR”-ში, სხვა საკითხებს შორის, ყურადღებაა გამახვილებული ბავშვების პერსონალური მონაცემების დაცვის მნიშვნელობაზე. პრეამბულის 38-ე პუნქტის შესაბამისად, ბავშვები, მათი პერსონალური მონაცემების დამუშავებისას, საჭიროებენ განსაკუთრებულ დაცვას, რადგან მათ შეიძლება ნაკლები იცოდნენ პერსონალური მონაცემების დამუშავებასთან დაკავშირებული რისკების, შედეგების, დაცვის საშუალებებისა და უფლებების თაობაზე.[340] პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული რისკების შესახებ ბავშვების ინფორმირებისას, გასათვალისწინებელია მათი ასაკი, განვითარების დონე და უნარები, რაც გავლენას იქონიებს მათ უნარზე რისკების შემცირების თვალსაზრისით.[341]

---

[336] Council of Europe Strategy for the Rights of the Child (2022-2027), “Children’s Rights in Action: from continuous implementation to joint innovation”.

[337] Charter of Fundamental Rights of the European Union, 2000/C364/01.

[338] Handbook on European Data Protection Law, 2018, 28.

[339] 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).

[340] იქვე, recital 38.

[341] Data Protection Commission (DPC), The Fundamentals for a Child-Oriented Approach to Data Processing, 12.

ევროპის კავშირის მართლმსაჯულების სასამართლო (“CJEU”) ეყრდნობა „ბავშვის უფლებების შესახებ“ 1989 წლის კონვენციით განმტკიცებულ ძირითად პრინციპებს.[342] გასათვალისწინებელია, რომ სასამართლო განსაკუთრებული სიფრთხილით ეკიდება ბავშვებთან დაკავშირებული საკითხების გადაწყვეტას.

2021 წლის მარტში, გამოქვეყნდა ორი მნიშვნელოვანი დოკუმენტი, რომელიც შეეხება ევროპის კავშირის გეგმებს ციფრულ სივრცეში ბავშვების უფლებების დაცვისა და ხელშეწყობის თაობაზე.[343] პირველი მათგანი უკავშირდება ევროპის კავშირის სტრატეგიას[344] ბავშვის უფლებებთან დაკავშირებით და წარმოადგენს ჩარჩო დოკუმენტს ევროკავშირისა და წევრი სახელმწიფოების მოქმედებისთვის. მასში გათვალისწინებულია ექვსი თემატური სფერო და ევროპული კომისიის მიერ დაგეგმილი ძირითადი აქტივობები ბავშვების უფლებების დაცვის ხელშესაწყობად. სტრატეგიის დოკუმენტის თანახმად, პანდემიამ წარმოშვა დამატებითი გამოწვევები, რომლებსაც ბავშვები ყოველდღიურად, ონლაინ სივრცეში აწყდებიან, კერძოდ, ხშირია კიბერბულინგის, ექსპლუატაციის, სექსუალური შინაარსის მასალების გავრცელების შემთხვევები. სტრატეგიის დოკუმენტი ეყრდნობა ბავშვის უფლებათა კონვენციასა და ევროსაბჭოს სტანდარტებს ბავშვის უფლებათა დაცვის კონტექსტში.[345] მეორე დოკუმენტი წარმოადგენს ევროპის კომისიის მიერ შემუშავებულ „ციფრულ კომპასს“,[346] რომელიც აერთიანებს ევროპის წარმატებული ციფრული გარდაქმნის შესახებ ხედვას, მიზნებსა და პერსპექტივებს 2030 წლისთვის. ევროკომისია აცხადებს, რომ არსებითად მნიშვნელოვანია ბავშვების ციფრული უფლებების რეალიზაცია.[347]

5.4. საზღვარგარეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა მიდგომები და პრაქტიკა

მონაცემთა დაცვის საზედამხედველო ორგანოები (“DPA”)[348] განსაკუთრებულ ყურადღებას უთმობენ ბავშვების პერსონალური მონაცემების დაცვას. ბავშვების მიერ თანამედროვე ტექნოლოგიების მზარდი გამოყენება ზრდის მათი პირადი ცხოვრების

[342] CJEU, C-244/06, Dynamic Medien Vertriebs GmbH v. Avides Media AG, 14 February 2008, paras. 42 and 52.
[343] Children’s rights in the digital environment: Moving from theory to practice, Best-practice guideline, 2021, 6.
[344] European Commission, “EU Strategy on the Rights of the Child” <https://ec.europa.eu/info/sites/default/files/child_rights_strategy_version_with_visuals3.pdf>, [24.08.2023].
[345] Children’s rights in the digital environment: Moving from theory to practice, Best-practice guideline, 2021, 6-7.
[346] Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983>, [25.08.2023].
[347] Children’s rights in the digital environment: Moving from theory to practice, Best-practice guideline, 2021, 7.
[348] Data Protection Authorities.

ხელშეუხებლობის უფლების დაცვასთან დაკავშირებულ რისკებს. არასრულწლოვნების პერსონალური მონაცემების არაკანონიერად დამუშავებამ შესაძლოა, გამოუსწორებელი ზიანი მიაყენოს ბავშვის ფსიქიკას. ამდენად, სამართლებრივი დაცვის მექანიზმების შემუშავებასთან ერთად, ძალზე მნიშვნელოვანია საზოგადოების ცნობიერების ამაღლება.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანოს ("ICO")[349] შემუშავებული აქვს სახელმძღვანელო ბავშვთა პერსონალურ მონაცემთა დაცვის თემატიკაზე.[350] დოკუმენტი განკუთვნილია იმ ორგანიზაციებისთვის, რომლებიც ამუშავებენ ბავშვების პირად ინფორმაციას. აღსანიშნავია, რომ ბავშვის უფლებათა კონვენციაზე დაყრდნობით, ბავშვში მოიაზრება 18 წლამდე პირი. გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის აქტი — "UK GDPR" მოიცავს დებულებებს, რომლებიც მიზნად ისახავს ბავშვთა პერსონალური მონაცემების დაცვის გაძლიერებასა და მარტივი, გასაგები ენით ინფორმაციის მიწოდებას. ბავშვების მიერ ონლაინ სერვისებით სარგებლობისას, არსებითად მნიშვნელოვანია გამჭვირვალობისა და ანგარიშვალდებულების უზრუნველყოფა.[351] გარდა აღნიშნულისა, მასწავლებლებისთვის "ICO"-ს შემუშავებული აქვს პირადი ცხოვრების ხელშეუხებლობის თაობაზე სასწავლო კურსი, რომლის მიზანია ბავშვებისათვის პერსონალური მონაცემების დაცვის შესახებ ინფორმაციის მიწოდება. მასალები მარტივად ხელმისაწვდომია და ყველას შეუძლია აღნიშნულით სარგებლობა.[352] ამასთანავე, "ICO"-მ შეიმუშავა ე. წ. „დიზაინის ტესტი",[353] რომლის მიზანია დაეხმაროს დიზაინერებს სხვადასხვა პროდუქტისა და სერვისის ბავშვთა კოდექსთან შესაბამისობის უზრუნველყოფაში, რომლებზე წვდომაც შემდგომში ბავშვებს ექნებათ. „ასაკის შესაბამისი დიზაინი: ონლაინ სერვისების პრაქტიკის კოდექსის"[354] მიზანია GDPR-თან შესაბამისობის უზრუნველყოფის მხარდაჭერა, რათა ციფრული სერვისები ითვალისწინებდეს ბავშვის პერსონალურ მონაცემთა დაცვის სათანადო გარანტიებს. თითოეული ტესტი[355] მოიცავს ინფორმაციას, რომელშიც დეტალურადაა აღწერილი

[349] Information Commissioner's Office (ICO).
[350] Information Commissioner's Office (ICO), Children and the GDPR, 22 March 2018.
[351] იქვე, 8.
[352] Information Commissioner's Office (ICO), New school resources for teachers, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/school-resources>, [29.08.2023].
[353] IAPP, ICO creates Children's Code design tests, <https://iapp.org/news/a/uk-ico-creates-childrens-code-design-tests>, [29.08.2023].
[354] Explanatory memorandum to the Age Appropriate Design Code 2020, <https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020>, [29.08.2023].
[355] ICO, Information Commissioner's Office (ICO), Children's Code design tests, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/practical-tools/childrens-code-design-tests/>, [29.08.2023].

საუკეთესო პრაქტიკა და ბავშვთა კოდექსთან შესაბამისობის უზრუნველსაყოფად საჭირო ღონისძიებები.

ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ ("DPC")[356] გამოაქვეყნა სახელმძღვანელო სახელწოდებით: „ბავშვზე ორიენტირებული მიდგომების საფუძვლები მონაცემთა დამუშავების პროცესში".[357] დოკუმენტის მიზანია ბავშვთა მონაცემთა დამუშავების სტანდარტების გაძლიერება. მასში წარმოდგენილია ძირითადი პრინციპები და შესაბამისი ღონისძიებები ბავშვთა უფლებების დასაცავად როგორც ციფრულ, ისე ყოველდღიურ რეალობაში. სახელმძღვანელო, პრინციპების განმარტების საშუალებით, დაეხმარება დამმუშავებლებს "GDPR"-ით გათვალისწინებული ვალდებულებების შესრულებაში. "ICO"-ს მსგავსად, ირლანდიის საზედამხედველო ორგანოც იზიარებს გაეროს ბავშვის უფლებათა კონვენციაში წარმოდგენილ დეფინიციებს. "DPC"-მ განსაზღვრა ბავშვთა პერსონალური მონაცემების დამუშავებისას გასათვალისწინებელი ძირითადი ასპექტები, მაგალითად, როგორიცაა: მონაცემთა დაცვის დონე; აშკარა თანხმობა; სამიზნე აუდიტორიის განსაზღვრა; დეტალური ინფორმირება; ბავშვზე ორიენტირებული გამჭვირვალობა; ბავშვების აზრის გათვალისწინება და ა. შ.[358]
ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("AEPD"),[359] 2023 წლის 22 ივნისს განაცხადა, რომ მხარს უჭერს სახელმწიფოს შეთანხმების თაობაზე წინადადებას, რომელიც ინტერნეტ სივრცესა და სოციალური ქსელებით სარგებლობას ბავშვების პერსონალური მონაცემების დაცვას შეეხება. ინიციატივა ეყრდნობა საფრთხეებს, რომლებსაც აწყდებიან არასრულწლოვნები ონლაინ სივრცეში შესაბამისი სერვისების გამოყენებისას. ამ თვალსაზრისით, "AEPD"-მ აღნიშნა, რომ ინიციატივის მხარდაჭერა უზრუნველყოფს ბავშვების პერსონალური მონაცემების ეფექტიან დაცვას.[360]

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("CNIL")[361] ბავშვების პერსონალური მონაცემების დაცვის მიზნით არაერთი აქტივობა განახორციელა.[362] "CNIL"-მა ციფრულ სივრცეში ბავშვების პერსონალური მონაცემების დასაცავად რვა

[356] Data Protection Commission (DPC).
[357] Data Protection Commission, Fundamentals for a Child-Oriented Approach to Data Processing, 2021.
[358] იქვე, 6.
[359] Spanish Agency for Data Protection (AEPD).
[360] OneTrust DataGuidance, Spain: AEPD supports initiative on minors' protection in digital environment, 2023, <https://www.dataguidance.com/news/spain-aepd-supports-initiative-minors-protection>, [29.08.2023].
[361] Commission Nationale de l'Informatique et des Libertés (CNIL).
[362] CNIL, Digital rights of children, <https://www.cnil.fr/en/digital-rights-children>, [29.08.2023].

რეკომენდაცია გამოაქვეყნა.[363] რეკომენდაციების ფარგლებში სიღრმისეულად იქნა შესწავლილი ბავშვების პერსონალური მონაცემების დაცვის საკითხები და გამოვლენილ იქნა შესაბამისი გამოწვევები. აღსანიშნავია, რომ რეკომენდაციები შემუშავდა საჯარო კონსულტაციებისა და სიღრმისეული სამართლებრივი ანალიზის შედეგად. საზედამხედველო ორგანომ ბავშვებთან სამუშაო შეხვედრები წამოიწყო, რათა ინფორმაცია მიეღო პირადი ცხოვრებისა და მონაცემთა დაცვის შესახებ ბავშვების აღქმების თაობაზე.[364] რეკომენდაციების შემუშავების მიზანს წარმოადგენს პრაქტიკული რჩევების მიცემა და კანონმდებლობის დებულებებთან დაკავშირებით შესაბამისი განმარტებების გაკეთება. რეკომენდაციები მიემართება როგორც ბავშვებს, ასევე, მათ მშობლებსა და ციფრულ სივრცეში მომუშავე პირებს.

ბავშვების პერსონალური მონაცემების დაცვის მიმართულებით, ასევე, აქტიურად მუშაობს შვედეთის საზედამხედველო ორგანო ("IMY")[365]. ამ მიზნით, შვედეთის მონაცემთა დაცვის საზედამხედველო ორგანომ, სხვა უწყებებთან თანამშრომლობით, შეიმუშავა სახელმძღვანელო[366] ბავშვების უფლებათა დაცვის მხარდაჭერის მიზნით, რომელიც იზიარებს "GDPR"-ით და ბავშვის უფლებათა კონვენციით გათვალისწინებულ ღირებულებებს. დოკუმენტში წარმოდგენილია რჩევები ციფრულ სივრცეში ბავშვთა პერსონალური მონაცემების დასაცავად. რეკომენდაციების მიზანია ბავშვთა ეფექტიანი დაცვა თანამედროვე ტექნოლოგიებით სარგებლობისას.[367]

აღსანიშნავია, რომ მონაცემთა დაცვის საზედამხედველო ორგანოებს არაერთხელ უმსჯელიათ ბავშვების პერსონალური მონაცემების დაცვის საკითხებზე. წინამდებარე თავში საილუსტრაციოდ წარმოდგენილია მხოლოდ რამდენიმე ორგანოს გადაწყვეტილება, რომელიც ქმნის ზოგად წარმოდგენას ბავშვის პერსონალურ მონაცემთა დაცვასთან დაკავშირებით არსებულ მიდგომებზე.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ ("ICO") შეისწავლა ინტერნეტ პლატფორმა "TikTok"-ის ფარგლებში ბავშვების მონაცემების დამუშავების კანონიერება, რომელიც ხორციელდებოდა მათი მშობლების თანხმობის გარეშე. გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის აქტის — "UK GDPR"-ის თანახმად, დამმუშავებლებმა 13 წლამდე პირებისათვის გარკვეული

[363] CNIL, 8 recommendations to enhance the protection of children online, 09 August 2021, <https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online>, [30.08.2023].
[364] იქვე.
[365] Swedish Authority for Privacy Protection (IMY).
[366] The rights of Children and Young People on Digital Platforms, Stakeholder Guide, Swedish Authority for Privacy Protection.
[367] იქვე, 3.

მომსახურების შეთავაზებისას უნდა მოიპოვონ მშობლებისგან ან კანონიერი წარმომადგენლებისგან თანხმობა. საზედამხედველო ორგანოს შეფასებით, არსებობდა ბავშვების მონაცემების გამოყენების ალბათობა „მიდევნებისა“ (“tracking”) და „პროფაილინგის“ მიზნებისთვის, რაც შესაძლოა, ბავშვებისთვის ზიანის მომტანი ყოფილიყო. თავის მხრივ, ბავშვები პლატფორმის დათვალიერების პროცესში შეიძლებოდა, გაცნობოდნენ არასასურველი შინაარსის ინფორმაციას. “TikTok” გაერთიანებულ სამეფოში მცხოვრებ მილიონზე მეტ ბავშვს, 13 წლამდე პირებს, ნებას რთავდა, რომ გამოეყენებინათ პლატფორმა. საზედამხედველო ორგანოს შეფასებით, პერსონალური მონაცემები, რომლებიც უკავშირდებოდა ბავშვებს, გამოიყენებოდა მშობლების თანხმობის გარეშე და “TikTok”-მა არ უზრუნველყო ასაკის დამადასტურებელი მექანიზმების დანერგვა. ასევე, არ იყო 13 წლამდე პირების პლატფორმიდან ამოშლის შესაძლებლობა. გარდა აღნიშნულისა, “TikTok”-მა ვერ წარუდგენდა მის მომხმარებლებს ამომწურავ ინფორმაციას, თუ როგორ გროვდებოდა და მუშავდებოდა მათი მონაცემები. პლატფორმა “TikTok” ვერ უზრუნველყოფდა პერსონალური მონაცემების კანონიერ, სამართლიან და გამჭვირვალე დამუშავებას, რის გამოც “TikTok”-ს დაეკისრა ჯარიმა.[368]

აღსანიშნავია, რომ ინტერნეტ პლატფორმა “TikTok” ჰოლანდიის მონაცემთა დაცვის საზედამხედველო ორგანოს[369] სამიზნეც აღმოჩნდა. საზედამხედველო ორგანო მიუთითებდა, რომ ჰოლანდიაში მცხოვრები 16 წლამდე ბავშვთა დიდი ჯგუფი იყენებს აღნიშნულ პლატფორმას. როდესაც მომხმარებელი ქმნის ანგარიშს, იგი ჰოლანდიურ ენაზე ეცნობა და თანხმდება კონფიდენციალურობის პოლიტიკას. საზედამხედველო ორგანომ დაადგინა, რომ 2018 წლის 25 მაისიდან 2020 წლის 28 ივლისამდე პერიოდში, ჰოლანდიელ მომხმარებლებს, მათ შორის ბავშვებს, კონფიდენციალურობის პოლიტიკის შესახებ ინფორმაცია მიეწოდებოდათ მხოლოდ ინგლისურ ენაზე. აღნიშნულის გამო “TikTok”-მა დაარღვია “GDPR”-ის მე-12 მუხლის პირველი პუნქტი, რომლის შესაბამისადაც მონაცემთა დამმუშავებელმა უნდა მიიღოს შესაბამისი ღონისძიებები, რათა მონაცემთა სუბიექტს მიაწოდოს ინფორმაცია მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი ფორმით, ნათელი და მარტივი ენით, განსაკუთრებით კი მაშინ, როდესაც აღნიშნული შეეხება არასრულწლოვნის ინფორმირებას. ფაქტობრივი გარემოებების გათვალისწინებით, ჰოლანდიის საზედამხედველო ორგანომ დააჯარიმა პლატფორმა “TikTok”.[370]

---

[368] Information Commissioner’s Office (ICO), GDPRhub, <https://gdprhub.eu/index.php?title=ICO_(UK)_-_TikTok_ICO>, [30.08.2023].

[369] Dutch Data Protection Authority (AP).

[370] AP (The Netherlands) – TikTok, GDPRhub, <https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_TikTok>, [30.08.2023].

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ, ასევე, შეისწავლა ბავშვების პერსონალური მონაცემების არაკანონიერი დამუშავების შემთხვევები. ერთ-ერთი საქმის ფაქტობრივი გარემოებების შესაბამისად, კონკრეტულმა ტანვარჯიშის კლუბმა, საკუთარი "Instagram"-ის გვერდზე გამოაქვეყნა ვარჯიშის დროს გადაღებული ორი ბავშვის ფოტოსურათი. არასრულწლოვნების დედამ არაერთხელ სთხოვა კლუბს, არ გაესაჯაროვებინა მისი შვილების ფოტოსურათები სოციალურ ქსელში. ასევე, განმარტა, რომ სავარჯიშო კლუბისთვის არ მიუცია თანხმობა მისი 10 და 12 წლის ქალიშვილებისთვის ფოტოსურათების გადაღებასა და ჩაწერაზე. აღნიშნულის გამო, დედამ შეიტანა საჩივარი ესპანეთის საზედამხედველო ორგანოში, რომლის შეფასებით, კლუბმა დაარღვია "GDPR"-ის მე-6 მუხლის პირველი პუნქტი, რადგან "Insagram"-ზე გამოაქვეყნა მომჩივნის შვილების სურათები, ყოველგვარი სამართლებრივი საფუძვლის გარეშე. კლუბმა ვერ დაასაბუთა, რომ ჰქონდა მომჩივნის არასრულწლოვანი შვილების მონაცემების დამუშავების უფლება. აღნიშნულის გათვალისწინებით, ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ტანვარჯიშის კლუბი დააჯარიმა 5000 ევროს ოდენობით.[371]

ბავშვების პერსონალურ მონაცემთა დაცვასთან მიმართებით უნდა აღინიშნოს ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ მიღებული რეზონანსული გადაწყვეტილება პლატფორმა "Instagram"-ის მიერ პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, რომელიც არასრულწლოვან მომხმარებელთა პერსონალური მონაცემების დამუშავებას, კერძოდ, ბავშვთა ელექტრონული ფოსტის მისამართების, ტელეფონის ნომრების საჯარო გამჟღავნებას, ასევე, მათი "Instagram"-ის პირადი ანგარიშების ავტომატურ გასაჯაროებას შეეხებოდა. ფაქტობრივი გარემოებების თანახმად, "Instagram"-მა 13-დან 17 წლამდე ასაკის მომხმარებლებს პლატფორმაზე ბიზნეს ანგარიშების ოპერირების შესაძლებლობა მისცა. ანგარიშებში მომხმარებელთა ტელეფონის ნომრები და ელექტრონული ფოსტის მისამართები საჯაროდ ჩანდა. ასევე, პლატფორმაზე მოქმედებდა მომხმარებლის რეგისტრაციის სისტემა, რომლის თანახმად, 13-დან 17 წლამდე მომხმარებელთა ანგარიშები ავტომატურად ხდებოდა საჯარო. საკითხის სიღრმისეულად შესწავლის შემდეგ, ირლანდიის საზედამხედველო ორგანომ ორგანიზაცია 405 მილიონი ევროს ოდენობით დააჯარიმა. მათ შორის, გათვალისწინებულ იქნა 20 მილიონი ევროს ოდენობის ჯარიმა "GDPR"-ის მე-6 მუხლის პირველი პუნქტის დარღვევისთვის. გარდა აღნიშნულისა, ირლანდიის

[371] GDPR hub, AEPD (Spain) - PS/00209/2021, <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00209/2021>, [30.08.2023].

საზედამხედველო ორგანომ “Instagram”-ს დაავალა სხვადასხვა ღონისძიების გატარება დამუშავების ოპერაციების “GDPR”-თან შესაბამისობაში მოსაყვანად.[372]

5.5. პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეის (“GPA”) რეზოლუცია ბავშვის ციფრულ უფლებებთან დაკავშირებით

2021 წელს, პირადი ცხოვრების გლობალური ასამბლეის (“GPA”) მიერ მიღებული იქნა რეზოლუცია[373] ციფრული უფლებების შესახებ, რომელშიც გაცხადებულია ბავშვების განსაკუთრებული დაცვის საჭიროება. რეზოლუციის თანახმად, ბავშვები სარგებლობენ გაეროს ბავშვის უფლებების კონვენციით აღიარებული უფლებებით, რომლებიც უნდა გავრცელდეს ცხოვრების ყველა სფეროში, მათ შორის ონლაინ სივრცეში. ამ მიმართულებით ხაზი ესმევა ციფრული გარემოს გავლენას ბავშვების განვითარებაზე, ყოველდღიურ ცხოვრებაზე, მათ მომავალსა და შესაძლებლობებზე.[374] ონლაინ სივრცეში განხორციელებული ყველა ქმედება ტოვებს გარკვეულ კვალს და, შესაბამისად, ინფორმაციის ინტერნეტში განთავსებისას, შესაძლოა, მასზე კონტროლი დაიკარგოს. განთავსებული ინფორმაცია შეიძლება შეგროვდეს და გამოყენებული იქნას მესამე მხარის კონკრეტული ცოდნის გარეშე. მომსახურების მიმწოდებლების მიმართ გაცემულია რეკომენდაცია, რომლის თანახმად, ბავშვების მხრიდან ონლაინ სერვისებით სარგებლობისას უნდა გაიაზრონ პასუხისმგებლობა.[375]

[372] Data Protection Commission, Data Protection Commission announces decision in Instagram Inquiry, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry>, [30.08.2023].

[373] Global Privacy Assembly (GPA) 43rd Closed Session of the Global Privacy Assembly October 2021 Adopted Resolution on children's digital rights.

[374] იქვე.

[375] იქვე.

პერსონალურ მონაცემთა
დაცვის სამსახური

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

ნატო ვაჩნაძის ქუჩა N° 7, თბილისი

ბაქოს ქუჩა N° 48, ბათუმი

(+995 32) 242 1000

office@pdps.ge

pdps.ge, personaldata.ge