

დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების დამუშავების სტანდარტი

I. შესავალი

ტექნოლოგიების განვითარებასთან ერთად, ადამიანის ცხოვრების თითქმის ყველა სფერო შეიცვალა, მათ შორის, ცვლილებები განათლების სისტემაშიც განხორციელდა. საქართველოსგან განსხვავებით,¹ მსოფლიოს ზოგიერთი ქვეყანა უკვე რამდენიმე ათეული წელია იყენებს დისტანციური სწავლების ფორმას,² რომელიც უფრო მეტად აქტუალური ახალი კორონავირუსის („კოვიდ-19“-ის) გავრცელების შემდეგ გახდა.³ ვირუსის გავრცელების თავიდან აცილების მიზნით, სახელმწიფოების მიერ დადგენილი შეზღუდვების გამო, საგანმანათლებლო დაწესებულებები იძულებულნი გახდნენ, ახალ რეალობას მორგებოდნენ და განათლების ტრადიციული მეთოდებისაგან განსხვავებით, სწავლება დისტანციურ რეჟიმში გაეგრძელებინათ.⁴

სწავლების განსხვავებულ ფორმაზე იძულებულმა გადასვლამ უმაღლესი საგანმანათლებლო დაწესებულებები ახალი გამოწვევების წინაშე დააყენა.⁵

* სულხან-საბა ორბელიანის უნივერსიტეტის სამართლის მაგისტრი.

¹ ტერმინი „დისტანციური სწავლება“ „უმაღლესი განათლების შესახებ“ საქართველოს კანონის მხოლოდ 2020 წელს დაემატა, საქართველოში კოვიდ-19-ის მიერ შექმნილი მდგომარეობიდან გამომდინარე, სწავლების ახალი ფორმისთვის სამართლებრივი საფუძვლის შექმნის მიზნით. იხ., „უმაღლესი განათლების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2020 წლის 15 ივნისის საქართველოს კანონი.

² იხ., <<https://bit.ly/3bMGU8R>> [10.06.2022].

³ საქართველოს სკოლის ორგანიზატორთა ასოციაცია, დისტანციური სწავლების მართვა, პრაქტიკული სახელმძღვანელო სკოლის ადმინისტრატორებისათვის, თბილისი, 2021, 8-13.

⁴ Huang R.H., Liu D.J., Guo J., Yang J.F., Zhao J.H., Wei X.F., Knyazeva S., Li, M., Zhuang, R.X., Looi, C.K., & Chang, T.W., Guidance On Flexible Learning During Campus Closures: Ensuring Course Quality of Higher Education in COVID-19 Outbreak, Beijing, 2020, 4; Aguilera-Hermida A. P., College Students' Use and Acceptance of Emergency Online Learning Due to COVID-19, *International Journal of Educational Research Open*, Vol. 1, 2020, 1.

⁵ ჯორბენაძე ს., Covid-19 და პერსონალურ მონაცემთა დაცვა „Zoom-ის“ გამოყენებით დისტანციური სწავლებისას, „შედარებითი სამართლის ქართულ – გერმანული ჟურნალი“, №5, 2020, 46.

მათ შორისაა, პერსონალური მონაცემების დაცვა, რომელიც ასეთი კრიტიკული მნიშვნელობის ჯერ არასდროს ყოფილა.⁶ საგანმანათლებლო პროცესის დისტანციურ რეჟიმში წარმართვის მიზნით, უნივერსიტეტები სრულად გახდნენ დამოკიდებულნი ტექნოლოგიებისა და ელექტრონული სისტემების გამოყენებაზე, რამაც, ერთი მხრივ, გააუმჯობესა მონაცემთა აღრიცხვისა და დამუშავების შესაძლებლობები, თუმცა, მეორე მხრივ, გაზარდა მონაცემებთან არაავტორიზებული წვდომის რისკები.⁷ მაშინ, როდესაც უმაღლესი საგანმანათლებლო დაწესებულებები საკმაოდ დიდი მოცულობის პერსონალურ მონაცემებს ამუშავებენ და ინახავენ,⁸ მნიშვნელოვანი და აუცილებელი გახდა ამ მონაცემთა დაცვის მაღალი სტანდარტის დანერგვა და აღსრულება,⁹ რაც საქართველოს რეალობაში დიდ გამოწვევას წარმოადგენს.

აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის უფლება, ადამიანის პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმონერის პატივისცემის უფლების¹⁰ ნაწილად ითვლება¹¹ და ზოგიერთ შემთხვევაში პერსონალური მონაცემების დაცვის აუცილებლობის შესახებ ჩანაწერი ქვეყნის კონსტიტუციის ტექსტშიც არის ხოლმე ასახული.¹² თუმცა, მიუხედავად ქვეყნის უზენაეს კანონში ცალკე არსებული ჩანაწერის არსებობისა, ორივე შემთხვევაში, პერსონალური მონაცემების კანონიერი დამუშავება და დაცვა აუცილებელია და პირდაპირ კავშირშია ადამიანის საყოველთაოდ აღიარებულ პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვასთან. შესაბამისად, სახელმწიფო თუ კერძო უნივერსიტეტების მიერ პერსონალური მონაცემების გამოყენების მზარდი დინამიკა, ამ მიმართულებით დანერგილი პრაქტიკა და მიდგომები, მნიშვნელოვანია, რომ თანხვედრაში იყოს ქვეყანაში არსებულ პერსონალურ მონაცემთა დაცვის მარეგულირებელ კანონმდებლობასთან, რითაც ასევე,

⁶ Huang, R.H., Liu D.J., Zhu L.X., Chen H.Y., Yang J.F., Tlili A., Fang H.G., Wang S.F., *Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents*, Beijing, 2020, 4.

⁷ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაცია უმაღლეს საგანმანათლებლო დაწესებულებებში პერსონალური მონაცემების დამუშავების შესახებ, 2018, 1.

⁸ Borgman, C. L., *Open Data, Grey Data, and Stewardship: Universities at The Privacy Frontier*, "Berkeley Technology Law Journal", Vol. 33(2), 2018, 370-382.

⁹ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაცია უმაღლეს საგანმანათლებლო დაწესებულებებში პერსონალური მონაცემების დაცვის შესახებ, 2018, 1.

¹⁰ ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია, 1950, მუხლი 8.

¹¹ *Case of Rotaru v. Romania*, [ECtHR] App. No. 28341/95, 4 May 2000; *Case of Amman v. Switzerland*, [ECtHR] App. No. 27798/95, 16 February 2000.

¹² *Constitution of 1978 with Amendments through 2011*, Sec. 18 (3); *Federal Constitution of the Swiss Confederation of 18 April 1999*, Art. 13(2).

უზრუნველყოფილი იქნება სტუდენტის პირად ცხოვრებაში გაუმართლებელი ჩარევისაგან დაცვა.

ზემოაღნიშნულიდან გამომდინარე, მოცემული ნაშრომის მიზანია საქართველოში უმაღლესი საგანმანათლებლო დაწესებულებების მიერ სტუდენტთა პერსონალური მონაცემების დამუშავების და დაცვის მიმართულებით არსებული მდგომარეობის შეფასება და იმ პრობლემების გამოკვეთა, რომლებიც კომპლექსურ მონესრიგებას საჭიროებენ. ასევე, ამ მიმართულებით არსებული სამართლებრივი ნორმებისა და საერთაშორისო გამოცდილების საფუძველზე იმ რეკომენდაციების შემუშავება, რომლებიც საგანმანათლებლო დაწესებულებებში სტუდენტთა პერსონალური მონაცემების დაცვის მაღალი სტანდარტის დანერგვას უზრუნველყოფენ.

ნაშრომში დასახული მიზნების მისაღწევად, გამოყენებული იქნება დესკრიფციული მეთოდი, რის საფუძველზეც აღინერება საქართველოში დღეს მოქმედი კანონმდებლობით მოცემული ნორმების შინაარსი. ამ ნორმების სისტემური და ლოგიკური ანალიზის საფუძველზე, ასევე, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსისა და სასამართლო გადაწყვეტილებების შესწავლით გამოიკვეთება პრაქტიკაში გამოვლენილი მნიშვნელოვანი მიმართულებები. საქართველოში არსებულ მიდგომებთან და რეკომენდაციებთან ერთად გაანალიზდება საზღვარგარეთის ქვეყნების მაგალითები და მიდგომები, რომელთა გამოცდილებაზე დაყრდნობითაც მოხდება საუკეთესო პრაქტიკის გამოკვეთა/განზოგადება და შესაბამისი რჩევების შემუშავება. გარდა ამისა, განხილულ იქნება ამ სფეროში მოღვაწე მეცნიერებისა თუ პრაქტიკოსი იურისტების შეხედულებები, როგორც ქვეყნის მასშტაბით, ისე სხვა ქვეყნების მაგალითებზე. ამასთან, ნაშრომზე მუშაობის განმავლობაში, გამოყენებულ იქნება სოციოლოგიური კვლევის მეთოდი და წარმოდგენილ იქნება საქართველოში აკრედიტებულ უმაღლეს საგანმანათლებლო დაწესებულებებში ჩატარებული სოციოლოგიური კვლევის შედეგები. საბოლოოდ კი, ინდუქციური და დედუქციური მეთოდების გამოყენებით, წარმოდგენილ იქნება დასკვნები და შესაბამისი რეკომენდაციები, რომლებიც პრაქტიკული და გამოსადეგი იქნება უმაღლესი საგანმანათლებლო დაწესებულებებისთვის, ვინაიდან, მაღალია ალბათობა, რომ დისტანციური სწავლება არც ახლო მომავალში დაკარგავს აქტუალობას¹³.

ნაშრომი შედგება შესავლის, დასკვნის, ოთხი თავისა და 24 ქვეთავისგან, რომელთაგან პირველ თავი შეეხება დისტანციური სწავლებისას დამუშავებულ სტუდენტთა პერსონალური მონაცემების სპეციფიკურ სახეებს, მათ შორის, სა-

¹³ სამომავლოდ ონლაინ სწავლების ეფექტურად წარმართის მიზნით ევროკომისიამ შექმნა მომავალი წლების ციფრული განათლების სამოქმედო გეგმა – Digital Education Action Plan (2021-2027). იხ., <<https://bit.ly/3bMGU8R>> [11.06.2022].

იდენტიფიკაციო და საკონტაქტო მონაცემების, ასევე, ხმისა და ვიზუალური გამოსახულების დამუშავების საკითხებს. ასევე, სტუდენტთა მიერ შესრულებულ დავალებთან, გამოცდებთან და მონაცემების არამიზნობრივ დამუშავებასთან დაკავშირებულ გამონაკებს. ნაშრომის მეორე თავი ეთმობა სტუდენტთა პერსონალური მონაცემების კანონიერი დამუშავებისთვის აუცილებელი კომპონენტების განხილვას. კერძოდ, რა ვადის განმავლობაში უნდა ხდებოდეს დამუშავებული მონაცემების შენახვა, როგორ უნდა აღირიცხოს დამუშავებული მონაცემები და საჭიროა თუ არა ფაილური სისტემის კატალოგის წარმოება. ასევე, ვინ არის დისტანციური სწავლების პროცესში სტუდენტთა მონაცემების დამუშავებაზე პასუხისმგებელი პირი, ვის აქვს წვდომა მათზე და როგორ ხდება მონაცემთა უსაფრთხოების უზრუნველყოფა. ნაშრომის მესამე თავში განხილულ იქნება საქართველოს უნივერსიტეტებში ჩატარებული კვლევის შედეგები. კვლევის შედეგებისა და პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკის ანალიზიდან გამომდინარე, ნაშრომის მეოთხე თავში წარმოდგენილი იქნება ის რეკომენდაციები, რომლებიც შესაძლებლობას მისცემს არა მხოლოდ კვლევაში მონაწილე უნივერსიტეტებს, არამედ ასევე, საქართველოში აკრედიტებულ ნებისმიერ უმაღლეს საგანმანათლებლო დაწესებულებას დაძლიონ ის გამონაკები, რაც დისტანციური სწავლების პროცესში სტუდენტთა პერსონალური მონაცემების დამუშავებისა და დაცვის მიმართულებით არსებობს.

II. დისტანციური სწავლების მიმდინარეობისას უმაღლესი საგანმანათლებლო დაწესებულების მიერ დამუშავებული სტუდენტის პერსონალური მონაცემები

1. აქტიური სტატუსის მქონე სტუდენტის ვინაობისა და საკონტაქტო მონაცემების დამუშავება

ტერმინი „პერსონალური მონაცემი“ საკმაოდ ფართო სპექტრს მოიცავს.¹⁴ მას მიეკუთვნება ნებისმიერი ის ინფორმაცია, რომელიც პიროვნების პირდაპირი ან ირიბი ფორმით იდენტიფიკაციის შესაძლებლობას იძლევა.¹⁵

¹⁴ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბილისი, 2017, 66.

¹⁵ Regulation 2016/679 of the European Parliament and of the Council 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), 27

სტუდენტის პირდაპირი იდენტიფიცირებისას ყველაზე ფართოდ გავრცელებული პერსონალური მონაცემი მისი სახელი და გვარია,¹⁶ რომელიც არა მხოლოდ აუდიტორული, არამედ დისტანციური სწავლების პერიოდშიც მუშავდება უნივერსიტეტების მიერ.¹⁷ ცხადია, რომ სტუდენტის სახელისა და გვარის დამუშავება აუცილებელია მისი იდენტიფიცირებისთვის, რათა აღირიცხოს ინფორმაცია მისი ლექციაზე დასწრების, აკადემიური მოსწრების, შეფასების და შემდგომში აკადემიური ხარისხის მიღების მიზნით, ასევე, სასწავლო მიზნებიდან გამომდინარე მისი ინტერესების დასაცავად და კანონმდებლობით უნივერსიტეტზე დაკისრებული მოვალეობების შესასრულებლად. თუმცა, ვინაიდან მონაცემის ეს სახე არ არის უნიკალური, ხშირ შემთხვევაში მასთან ერთად მუშავდება პირის პერსონალიზებული ნომერიც¹⁸ (საგადასახადო კოდი¹⁹/ პირადი ნომერი²⁰). ამ მონაცემების ერთობლივი დამუშავება ხელს უწყობს იმავე სახელისა და გვარის სტუდენტებისთვის მეორე სტუდენტის პერსონალურ მონაცემებზე ხელმისაწვდომობის გამორიცხვას და სხვა ინციდენტების თავიდან აცილების შესაძლებლობას.²¹

სტუდენტის პერსონალურ მონაცემებს ასევე მიეკუთვნება პირის ისეთი საკონტაქტო ინფორმაცია, როგორიცაა მისი ტელეფონის ნომერი²² და ელექტრონული ფოსტის მისამართი.²³ ეს უკანასკნელი უნივერსიტეტების მიერ მუშავდება, ელექტრონულ პლატფორმებზე/პორტალებზე სტუდენტთა დაშვებისა და იდე-

April 2016, Art. 4 para.1; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Art. 2 para. A, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ ქვეპუნქტი.

¹⁶ მონაცემთა დაცვის ევროპული სამართალი, კ. გოშაძის თარგმანი, მ. ბეგიაშვილის რედაქტორობით, თბილისი, 2015, 51.

¹⁷ შპს „იუაი“ – ჩანტლაძე ტ., სულხანიშვილი ე., ცინცკილაძე გ., ჯიშიაშვილი გ., თემატური რეკომენდაციები COVID 19 პანდემიის დროს პერსონალური მონაცემების მართვაზე, ანგარიში დისტანციური სწავლებისას პერსონალურ მონაცემთა დაცვის შესახებ, 2021, 26.

¹⁸ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 104.

¹⁹ Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others, [CJEU], C-201/14, 1 October 2015; Satakunnan Markkinapörssi and Satamedia, [CJEU], C- 73/07, 16 December 2008.

²⁰ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 9 მარტის №გ-1/140/2018 გადაწყვეტილება „სსიპ აკაკი წერეთლის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“; საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 30 ივლისის №გ-1/252/2019 გადაწყვეტილება „სსიპ ილიას სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

²¹ Information Commissioner's Office, Annual Report and Financial Statements 2015/16, 50.

²² Criminal proceedings against Bodil Lindqvist, [CJEU], C-101/01, 6 November 2003.

²³ Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [CJEU], C293/12 and C594/12, 8 April 2014.

ნტიფიკაციის,²⁴ ასევე, სტუდენტების კომუნიკაციისა და მათთვის ინფორმაციის მიწოდების მიზნით.²⁵

სტუდენტთა ელექტრონული ფოსტის მისამართის, როგორც პერსონალური მონაცემის დამუშავების საჭიროება უფრო მეტად გამოიკვეთა დისტანციური სწავლების ფორმის დანერგვის შემდეგ. აუდიტორული სწავლებისგან განსხვავებით, ონლაინ სწავლება უნივერსიტეტის მიერ წინასწარ შერჩეული ელექტრონული პლატფორმის მეშვეობით მიმდინარეობს.²⁶ ხშირ შემთხვევაში, ლექცია/სემინარზე დასასწრებად სტუდენტი ინტერნეტთან დაკავშირებული ტექნიკის მეშვეობით,²⁷ შესაბამის ონლაინ პლატფორმაზე გადის რეგისტრაციას საგანმანათლებლო დაწესებულების ორგანიზაციული ელექტრონული ფოსტის გამოყენებით.²⁸ დისტანციური სწავლების წარმართვისთვის შერჩეული პლატფორმის მიხედვით, ერთ შემთხვევაში, სტუდენტს ლექციასთან შეერთების მიზნით შეჰყავს ონლაინ შეხვედრის ინდივიდუალური კოდი და პაროლი.²⁹ ხოლო, მეორე შემთხვევაში, სტუდენტი ვირტუალურ შეხვედრაზე წინასწარ არის მოწვეული სწორედ იმ ელექტრონული ფოსტის მისამართით, რომელიც უნივერსიტეტისთვის არის ცნობილი.³⁰ ამასთანავე, სტუდენტს სხვა ელექტრონული ფოსტის გამოყენების შემთხვევაში შეხვედრაზე დასასწრებად ორგანიზატორის თანხმობა სჭირდება ყოველ კონკრეტულ შემთხვევაზე,³¹ რაც უზრუნველყოფს პირთა განსაზღვრული

²⁴ Oliveira P., Cunha C., Nakayama M., Learning Management Systems (LMS) and e-learning management: an integrative review and research agenda, Journal of Information Systems and Technology Management, Vol. 13, No. 2, 2016, 161.

²⁵ Jones S., The Internet Goes to College: How Students Are Living in the Future with Today's Technology, Washington, 2002, 3-9; Lokanath M., Tushar G., Abha S., Online teaching-learning in higher education during lockdown period of COVID-19 pandemic, International Journal of Educational Research Open, Vol. 1, 2020, 7.

²⁶ Chan R.Y., Bista K., Allen R., M., Is Online and Distance Learning the Future in Global Higher Education?, in the book: Online Teaching and Learning in Higher Education during COVID-19: International Perspectives and Experiences, edited by Chan R.Y., Bista K., Allen R., M., New York, 2022, 3-4; განათლების ხარისხის განვითარების ეროვნული ცენტრი, რჩევები უმაღლესი საგანმანათლებლო დაწესებულებებისთვის ელექტრონული სწავლების ხარისხის უზრუნველყოფასთან დაკავშირებით, თბილისი, 2020, 3.

²⁷ Icheku, V., Challenges of protecting personal data and privacy during online teaching and learning, Academia Letters, Art. 3083, 2021, 3, იხ., <<https://bit.ly/3R7cV1W>> [03.06.2022].

²⁸ Dai Z., A Study on the Effectiveness of College English Blended Learning Under MOOCs Philosophy in China, in the book: Exploring Online Learning Through Synchronous and Asynchronous Instructional Methods, edited by Sistek-Chandler C., Hershey PA, 2020, 263.

²⁹ Brook N., Teaching in the Post Covid Classroom: 2020-2021 Complete Beginners Guide to Organize Online Lessons, Everything You Need to Know about Zoom, Google Classroom and Distance Learning, Kindle e-book, 2020, 36.

³⁰ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 10 მაისის №გ-1/141/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემოწმების დასრულების შესახებ“, 3-4.

³¹ იქვე.

წრის დაშვებას შესაბამის ლექცია/სემინარზე³² და სტუდენტთა პერსონალური მონაცემების სხვა პირებზე გამჟღავნების რისკების შემცირებას.

უნდა აღინიშნოს, რომ სტუდენტის ვინაობის დამდგენი და მისი საკონტაქტო მონაცემების დამუშავება უმაღლესი საგანმანათლებლო დაწესებულების ფუნქციონირებისა და კანონმდებლობით დადგენილი უფლებამოსილებების განხორციელებისთვის აუცილებელი საჭიროებაა. თუმცა, გარდა მონაცემების დამუშავების სამართლებრივი საფუძვლის არსებობისა, საგანმანათლებლო დაწესებულებებმა, მნიშვნელოვანია, ასევე დაიცვან მონაცემთა კანონიერი დამუშავებისთვის დადგენილი პრინციპები და წესები.

2. სტუდენტის ხმისა და ვიზუალური გამოსახულების დამუშავება

ადამიანის გამოსახულება, რომელიც პერსონალურ მონაცემთა კატეგორიას მიეკუთვნება,³³ მიჩნეულია მისი პიროვნულობის ერთ-ერთ მთავარ ატრიბუტად, რომელიც ადამიანის უნიკალურ მახასიათებლებს ამჟღავნებს და ამით გამოარჩევს მას სხვებისგან.³⁴ ფიზიკური პირის გამოსახულება შეიძლება არსებობდეს როგორც ფოტოსურათის, ასევე ვიდეო გამოსახულების ფორმით.³⁵ ეს უკანასკნელი კი შესაძლოა შეიქმნას როგორც ვიდეოთვალთვალის ან ვიდეოკამერის, ასევე სმარტფონის ან სხვა ელექტრონული მოწყობილობის დახმარებითაც.³⁶ გარდა ადამიანის ვიზუალური გამოსახულებისა, პერსონალურ მონაცემად ხშირ შემთხვევაში მიჩნეულია მისი ხმა.³⁷ სწორედ პერსონალური მონაცემების მოცემული სახეები – სტუდენტის სახის მოყვანილობა, ვიზუალური გამოსახულება და ხმა³⁸ – მუშავდება უნივერსიტეტის მიერ დისტანციური სწავლებისას. აღნიშნული

³² ჯორბენაძე ს., Covid-19 და პერსონალურ მონაცემთა დაცვა „Zoom-ის“ გამოყენებით დისტანციური სწავლებისას, „შედარებითი სამართლის ქართულ-გერმანული ჟურნალი“, №5, 2020, 45.

³³ Von Hannover v. Germany, [ECtHR], App. No. 59320/00, 24 June 2004, Sciacca v. Italy, [ECtHR], App. No. 50774/99, 11 January 2005.

³⁴ López Ribalda and Others v. Spain, [ECtHR], Apps. No. 1874/13 and 8567/13, 17 October 2019.

³⁵ European Data Protection Board (EDPB), Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 2020, 28.

³⁶ პერსონალური მონაცემების ანბანი, < <http://portal.personaldata.ge> > [9.06.2022].

³⁷ P.G. and J.H. v. the United Kingdom, [ECtHR], App. No. 44787/98, 25 September 2001; Wisse v. France, [ECtHR], App. No. 71611/01, 20 December 2005.

³⁸ Huang, R.H., Liu, D.J., Zhu, L.X., Chen, H.Y., Yang, J.F., Tili, A., Fang, H.G., Wang, S.F., Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents, Beijing, 2020, 18; Anthony E. Kelly and Mika Seppälä, Changing Policies Concerning Student Privacy and Ethics in Online Education, International Journal of Information and Education Technology, Vol. 6, No. 8, 2016, 653.

მონაცემების რომელიმე სახე შეიძლება დამუშავდეს ფოტო/ვიდეო და აუდიო გადაღებით, როგორც ცალ-ცალკე, ასევე ერთობლივად, სტუდენტის მიერ ვიდეოკამერის ჩართვის შემთხვევაში.

დისტანციური სწავლებისას ლექცია/სემინარები უმეტესად აუდიო-ვიდეო ონლაინ შეხვედრების საშუალებით მიმდინარეობს, რომელიც ლექტორებსა და სტუდენტებს ონლაინ რეჟიმში კომუნიკაციის შესაძლებლობას აძლევს.³⁹ თუმცა, ასინქრონული სწავლების უზრუნველსაყოფად,⁴⁰ საგანმანათლებლო დაწესებულებების მიერ ონლაინ შეხვედრები იწერება,⁴¹ შემდგომში სტუდენტებისთვის მათი ხელმისაწვდომობის,⁴² განათლების ხარისხის კონტროლისა⁴³ და საგანმანათლებლო დაწესებულებების მიერ წინასწარ განსაზღვრული სხვა მიზნების შესაბამისად. პრაქტიკაში, მათ შორის, საქართველოში აკრედიტებულ უმაღლეს საგანმანათლებლო დაწესებულებებში, განსხვავებული მიდგომა არსებობს სტუდენტების მიერ ვიდეოკამერის ჩართვის აუცილებლობასა და ლექცია/სემინარების აუდიო/ვიდეო ჩანერასთან მიმართებით.⁴⁴

აღსანიშნავია, რომ ლექციების მიმდინარეობისას, სტუდენტებს მათი პირადი და ოჯახური ცხოვრების უფლების გათვალისწინებით, არ უნდა ჰქონდეთ ვიდეოკამერის ჩართვის ვალდებულება. ვინაიდან, ამ შემთხვევაში, მესამე პირებს ავტომატურად შეუძლიათ სტუდენტის საცხოვრებელი სახლის, მასთან მცხოვრები ადამიანების და პირადი ცხოვრების მახასიათებლების შესახებ ინფორმაციის მიღება.⁴⁵ ვიდეოკამერის ჩართვამ შესაძლოა გამოიწვიოს ონლაინ ლექციის მიმდინარეობისას სტუდენტის ქცევის რეგულირება, მაშინ, როდესაც სწავლების მიზნებისათვის არ აქვს მნიშვნელობა, როგორ მდგომარეობაში დაესწრება სტუდენტი ლექციას. ასეთი ვალდებულების დაკისრება თავისთავად მოახდენს ზეგავლენას იმაზე, მოინესრიგებს თუ არა სტუდენტი თმას, რას ჩაიცვამს, რო-

³⁹ Adeyeye, B., Ojih, S.E., Bello, D., Adesina, E., Yartey, D., Ben-Enukora, C., Adeyeye, Q., Online Learning Platforms and Covenant University Students' Academic Performance in Practical Related Courses during COVID-19 Pandemic, Sustainability, Vol. 14(2), 878, 2022, 1-3.

⁴⁰ Beckwith E. G., The Importance of Synchronous Sessions in Online Asynchronous Classes, in the book: Exploring Online Learning Through Synchronous and Asynchronous Instructional Methods, edited by Sistek-Chandler C., Hershey PA, 2020, 37.

⁴¹ Sadler C., Privacy Considerations in Higher Education Online Learning, Washington, 2020, 11.

⁴² Basilaia G., Dgebuadze M., Kantaria M., Chokhoniidze G., Replacing the Classic Learning Form at Universities as an Immediate Response to the COVID-19 Virus Infection in Georgia, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 8, Iss. III, 2020, 101-103.

⁴³ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 17 აგვისტოს №გ-1/272/2020 გადაწყვეტილება „განცხადების განხილვის დასრულების შესახებ“.

⁴⁴ სახელმწიფო ინსპექტორის სამსახური, რეკომენდაცია – პერსონალური მონაცემების დამუშავება დისტანციური სწავლების პროცესში, იანვარი, 2022.

⁴⁵ Sadler C., Privacy Considerations in Higher Education Online Learning, Washington, 2020, 11.

მელი ადგილიდან ჩაერთვება ლექციას და სხვა მრავალ ფაქტორზე. ამასთანავე, კამერის ჩართვამ შესაძლოა გავლენა იქონიოს სტუდენტთან ერთად მცხოვრებ სხვა ადამიანებზეც, რომლებსაც ასევე მოუწევთ თავიანთი ქცევის რეგულირება. აღნიშნულით კი შესაძლებელია სტუდენტის პირად ცხოვრებაში გაუმართლებელი ჩარევის რისკების გაზრდა.⁴⁶ შესაბამისად, დისტანციურ რეჟიმში ლექციის მიმდინარეობისას სტუდენტისათვის ვიდეოკამერის ჩართვის ვალდებულება აშკარად შეიცავს იმ რისკს, რომ დამუშავდება მათი პერსონალური მონაცემების არასაჭირო რაოდენობა, მაშინ, როდესაც ლექციის მიმდინარეობისას, ლექტორის მიერ ცოდნის გადაცემის პროცესი არ საჭიროებს სტუდენტის გამოსახულების დამუშავების აუცილებლობას. თუმცა, შესაძლებელია ასეთი ვალდებულების შემოღებას თავისი მიზანიც გააჩნდეს და ზოგიერთ შემთხვევაში გამართლებულიც და გარდაუვალიც იყოს. მაგალითად, ასეთი მიზანია საგამოცდო პროცესის მიმდინარეობისას სტუდენტის იდენტიფიკაცია.⁴⁷ შესაბამისად, სტუდენტის მიერ ვიდეოკამერის ჩართვა უნდა იყოს ნებაყოფლობითი, გარდა იმ შემთხვევისა, თუ ეს გამოცდის ან ტესტირების ჩატარების მიზნებისთვის არ არის აუცილებელი.

რაც შეეხება ლექციების მიმდინარეობის აუდიო-ვიდეო ჩანერას, უნდა აღინიშნოს, რომ ლექცია/სემინარების მიმდინარეობისას, ლექტორი შესაბამის ცოდნას უზიარებს სტუდენტს, რომელიც მონაწილეობას იღებს საგანმანათლებლო ხასიათის აქტივობებში პრეზენტაციების განხორციელებით, კითხვების დასმით თუ ინტერაქციის სხვა ფორმით,⁴⁸ მათ შორის ორმხრივი ურთიერთობა ყალიბდება, სადაც ისინი საკუთარ სოციალურ იდენტობას ამჟღავნებენ.⁴⁹ აღსანიშნავია, რომ ადამიანის უფლებათა ევროპული სასამართლო გამონაკლისი შემთხვევების გარდა,⁵⁰ დაუშვებლად მიიჩნევს აუდიტორიებში ლექციების მიმდინარეობის აუდიო/ვიდეოთვალთვალს და მას ადამიანის პირადი და ოჯახური ცხოვრებაში გაუმართლებელ ჩარევად მიიჩნევს.⁵¹ მიუხედავად იმისა, რომ დისტანციური სწა-

⁴⁶ საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №11/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტულუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ.“

⁴⁷ სახელმწიფო ინსპექტორის სამსახური, რეკომენდაცია-პერსონალური მონაცემების დამუშავება დისტანციური სწავლების პროცესში, იანვარი, 2022, 6.

⁴⁸ Sadler C., *Privacy Considerations in Higher Education Online Learning*, Washington, 2020, 11.

⁴⁹ Antovic and Mirkovic v. Montenegro, [ECtHR], App. No. 70838/13, 28 November 2017.

⁵⁰ Bărbulescu v. Romania, [ECtHR], App. No. 61496/08, 5 September 2017.

⁵¹ Antovic and Mirkovic v. Montenegro, [ECtHR], App. No. 70838/13, 28 November 2017.

ვლება საგანმანათლებლო დაწესებულებებისათვის განსაკუთრებული სიახლეს არ წარმოადგენს, კორონავირუსის („COVID-19“-ის) პანდემიამ ახალი რეალობის წინაშე დააყენა უმაღლესი განათლების სისტემა. ისინი იძულებულები გახდნენ დაუყოვნებლივ გადასულიყვნენ სწავლების ონლაინ რეჟიმზე.⁵² სწავლების ეს ფორმა განსაკუთრებულ მზადყოფნას და მომზადებას საჭიროებდა უმაღლესი საგანმანათლებლო ორგანოს მხრიდან.⁵³ ამასთანვე, დიდი გამოწვევა იყო სტუდენტის შეზღუდული წვდომა ინტერნეტთან,⁵⁴ რისი გამომწვევი მიზეზიც სტუდენტზე შესაძლოა არ ყოფილიყო დამოკიდებული.⁵⁵ ამდენად, ამ პროცესის სიახლიდან და განათლების უფლების შეზღუდვის მინიმიზაციიდან,⁵⁶ ასევე, სწავლების ხარისხის ამაღლების⁵⁷ მიზნებიდან გამომდინარე, შესაბამისი მიზნისა და საფუძვლის არსებობის შემთხვევაში, დასაშვებად უნდა მივიჩნიოთ ონლაინ ჩატარებული ლექციების აუდიო/ვიდეო ჩანერა. თუმცა, ვინაიდან ეს პროცესი სტუდენტთა პერსონალური მონაცემების ავტომატური დამუშავებაა⁵⁸ უნივერსიტეტებმა მკაფიოდ უნდა დაიცვან მონაცემთა დამუშავებისათვის აუცილებელი პრინციპები და საფუძვლები, კერძოდ, ჩაინერონ ლექციები მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და კანონიერი მიზნებისთვის⁵⁹. ამისთვის კი, უმაღლესმა სა-

⁵² Goudeau, S., Sanrey, C., Stanczak, A., Manstead A., Darnon C., Why lockdown and distance learning during the COVID-19 pandemic are likely to increase the social class achievement gap, "Nature Human Behaviour", №5, 2021, 1273.

⁵³ Kaspar K., R  th M., The e-learning setting circle: first steps toward theory development in e-learning research, The Electronic Journal of e-Learning (EJEL), Vol. 15, No. 1, 2017, 94–101, იხ., <<https://bit.ly/3urrXG9>> [04.07.2022].

⁵⁴ Icheku, V., Challenges of protecting personal data and privacy during online teaching and learning, Academia Letters, Article 3083, 2021, 3, იხ., < shorturl.at/hyDY9 > [03.06.2022].

⁵⁵ ინტერნეტის ხელმისაწვდომობისა და გამოყენების ტენდენციები საქართველოში, ინფორმაციის განვითარების ინსტიტუტი, 2020, <<https://bit.ly/3NLI7Sy>> [3.06.2022]; Percentage of global population accessing the internet from 2005 to 2021, by market maturity, <<https://bit.ly/3R7f1rS>> [3.06.2022]; Most Students Now Have Home Internet Access, But What About the Ones Who Don't?, <<https://bit.ly/3ApvKHU>> [3.06.2022]; Quality and Qualifications Ireland, The Impact of COVID19 Modifications to Teaching, Learning and Assessment in Irish Further Education and Training and Higher Education, 2020, 76.

⁵⁶ ხოფერია რ., განათლების უფლების შეზღუდვის კონსტიტუციურობის საკითხი COVID-19-ის პანდემიის პირობებში, ადამიანის უფლებათა დაცვა, პანდემია და სამართლის უზენაესობა, კ. კორკელიას რედაქტორობით, თბილისი, 2021, 85-95; Basilaia G., Dgebuadze M., Kantaria M., Chokhonelidze G., Replacing the Classic Learning Form at Universities as an Immediate Response to the COVID-19 Virus Infection in Georgia, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 8, Iss. III, 2020, 101.

⁵⁷ Noetel M., Griffith S., Delaney O., Sanders T., Parker P., del Pozo Cruz B., Lonsdale C., Video Improves Learning in Higher Education: A Systematic Review, "Review of Educational Research", Vol. 91, No. 2, 2021, 204-236.

⁵⁸ Franti  ek Ryne   v.   řad pro ochranu osobn  ch   daj  , [CJEU], C212/13, 11 December 2014.

⁵⁹ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „ბ“ ქვეპუნქტი.

განმანათლებლო დაწესებულებამ უნდა შეაფასოს ონლაინ ლექციების ჩანერის მიზანი და საფუძველი, შეისწავლოს სტუდენტთა რეალური საჭიროება, მოიპოვოს თანხმობა ლექციების ჩანერასა და ამ ჩანაწერების მიწოდების თაობაზე. ამდენად, ასინქრონული სწავლების მიზანს შეიძლება წარმოადგენდეს საგანმანათლებლო მასალაზე სტუდენტების ხელმისაწვდომობის უზრუნველყოფა. თუმცა, მსგავსი მიზანი ვერ იარსებებს ონლაინ რეჟიმში ჩატარებული სემინარების აუდიო/ვიდეო ჩანერის შემთხვევაში, რადგან სემინარის მთავარი დანიშნულება ლექტორის მიერ ახსნილი მასალის გამოკითხვაა, რა დროსაც უფრო მაღალია სტუდენტის ისეთი პერსონალური მონაცემების დამუშავების რისკი, როგორიცაა მისი შეფასება და უკუკავშირი. სწორედ, ამიტომ, ლექციებსა და სემინარების აუდიო-ვიდეო ჩანერა არ შეიძლება ერთი და იმავე მიზნითა და სამართლებრივი საფუძველით განხორციელდეს.

აღსანიშნავია, რომ გარდა ლექცია/სემინარებისა, სტუდენტის ხმა და ვიზუალური გამოსახულება შეიძლება დამუშავდეს სინქრონულ რეჟიმში მიმდინარე გამოცდის ვიდეოთვალთვალისას, რაც არა მარტო დისტანციურად,⁶⁰ არამედ აუდიტორიაში ჩატარებული გამოცდების შემთხვევაშიც გამართლებულია.⁶¹

სტუდენტის ხმისა და ვიზუალური გამოსახულების აუდიო/ვიდეო ჩანაწერის ფორმით დამუშავებისას, შესაძლოა რომელიმე შემთხვევაში ეს მონაცემები განსაკუთრებული კატეგორიის მონაცემად ჩაითვალოს.⁶² საქართველოსა⁶³ და ევროკავშირის კანონმდებლობა⁶⁴ ცალკე გამოყოფს განსაკუთრებული კატეგორიის მონაცემებს, რომელიც მოიცავს ინფორმაციას პირის რასობრივი და ეთნიკური წარმომავლობის, პოლიტიკური, რელიგიური ან სხვა შეხედულებების (ფილოსოფიურის ჩათვლით) და კანონმდებლობით დადგენილი სხვა კატეგორიების შესახებ, აგრეთვე იმ ბიომეტრიულ და გენეტიკურ მონაცემებს, რომლებიც ჩამოთვლილი ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა. მონაცემთა ზემოთ აღნიშნული სახეები, მათი სენსიტიური ხასიათიდან გამომდინარე,

⁶⁰ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 8 ივლისის №გ-1/231/2020 გადაწყვეტილება „განცხადების განხილვის დასრულების შესახებ“.

⁶¹ სახელმწიფო ინსპექტორის სამსახური, რეკომენდაცია-ვიდეოთვალთვალის განხორციელების წესი, 2021, 26.

⁶² European Data Protection Board (EDPB), Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 2020, 14; When is voice (a special category of) personal data under GDPR?, <<https://bit.ly/3bJh2y>> [03.06.2022].

⁶³ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ბ“ ქვეპუნქტი.

⁶⁴ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Article 9 par.1; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Art. 6 para.1.

ნარე, განსაკუთრებულ კატეგორიათა რიცხვს შესაძლოა მიეკუთვნოს, რადგანაც მათი უკანონოდ დამუშავება საფრთხეს უქმნის ადამიანის პირადი ცხოვრების ხელყოფას.⁶⁵ თუმცა, აუდიო/ვიდეო ჩანაწერის განსაკუთრებული კატეგორიის პერსონალურ მონაცემად ჩათვლა *per se* არ არის მართებული. მაგალითად, სტუდენტის მიერ სათვალის ტარებისას, ვიდეოჩანაწერი ავტომატურად განსაკუთრებული კატეგორიის მონაცემებად არ შეიძლება იქნეს მიჩნეული. ასეთ შემთხვევაში გასათვალისწინებელია ფოტოსურათის/ვიდეოჩანაწერის ხარისხი, შინაარსი და საგანმანათლებლო მონაცემის დამუშავების მიზანიც. მხოლოდ ამ კატეგორიების ერთობლიობაში განხილვით და ყოველი კონკრეტული შემთხვევის შეფასების შემდეგ, თუ პირის იდენტიფიცირება შესაძლებელია კანონმდებლობაში აღნიშნული განსაკუთრებული ნიშნების საფუძველზე, ვიდეო/აუდიო ჩანაწერი უნდა ჩაითვალოს განსაკუთრებული კატეგორიის პერსონალურ მონაცემად.⁶⁶ თუმცა, მიუხედავად იმისა, დამუშავდება თუ არა ამ ფორმით სტუდენტის განსაკუთრებული კატეგორიის პერსონალური მონაცემები, ცხადია, რომ სტუდენტის ვიზუალური გამოსახულებისა და ხმის, როგორც პერსონალური მონაცემების არაკანონიერად გამოყენების შემთხვევაში არსებობს დიდი რისკი, რომ სტუდენტის ინტერესებს და მის უფლებებს შეექმნას საფრთხე, განსაკუთრებით, დისკრიმინაციის კუთხით⁶⁷.

3. შესრულებული დავალება და საგამოცდო ნაშრომი, როგორც სტუდენტის პერსონალური მონაცემი

აღსანიშნავია, რომ პროფესიული საგამოცდო ნაშრომი, რომელსაც სტუდენტი ასრულებს, გამომცდელის კომენტარებთან და შეფასებასთან ერთად⁶⁸ წარმოადგენს უნივერსიტეტის მიერ დამუშავებულ პერსონალურ მონაცემს.

კანონმდებლობით ჩამოყალიბებული პერსონალური მონაცემის ცნების დეფინიცია საკმაოდ ფართო ინტერპრეტაციის შესაძლებლობას იძლევა. ამიტომ, მნიშვნელოვანია, განხილულ იქნეს, რამდენად შეიძლება სტუდენტის ელექტრონულად შესრულებული საგამოცდო ნაშრომი ჩაითვალოს იმ ტიპის ინფორმაციად, რომელიც მისი პირდაპირი ან ირიბი ფორმით იდენტიფიკაციის შესაძლებლობას იძლევა. მიჩნეულია, რომ პიროვნების საგამოცდო ნაშრომი, ერთი

⁶⁵ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბილისი, 2017, 68.

⁶⁶ European Data Protection Supervisor, The EDPS video-surveillance guidelines, 2017, 8-26.

⁶⁷ Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Art. 6.

⁶⁸ Peter Nowak v Data Protection Commissioner, [CJEU], C-434/16, 20 December 2017.

მხრივ, მიუთითებს გამოცდაში მისი მონაწილეობის თაობაზე,⁶⁹ ხოლო, მეორე მხრივ, მის მიერ შესრულებულ დავალებაში/ნაშრომში მითითებული ინფორმაცია ასახავს კანდიდატის ცოდნისა და კომპეტენციის დონეს მოცემულ სფეროში და, ზოგიერთ შემთხვევაში, მის ინტელექტს, აზროვნების პროცესსა და მსჯელობას.⁷⁰ ევროპის მართლმსაჯულების სასამართლოს განმარტებით,⁷¹ პროფესიული საგამოცდო ნაშრომი, ვინაიდან ასახავს კანდიდატის ცოდნას, გროვდება სწორედ მისი პროფესიული შესაძლებლობების შეფასების მიზნით და როდესაც მის წარმატებით თუ წარუმატებლად ჩაბარებას შეუძლია პიროვნების უფლებებზე და ინტერესებზე მოახდინოს გავლენა, მაგალითად, მის მიერ შერჩეული პროფესიით საქმიანობა და სასურველი თანამდებობის დაკავება, უნდა ჩაითვალოს პერსონალური მონაცემის შემცველ ინფორმაციად. მართალია აღნიშნული მსჯელობა ევროპის მართლმსაჯულების სასამართლომ პროფესიული ნაშრომის პერსონალურ მონაცემად მიჩნევასთან მიმართებით ჩამოაყალიბა, თუმცა მსგავსი მიდგომა უნივერსიტეტში ჩატარებულ შუალედურ და ფინალურ გამოცდებთან მიმართებითაც შეიძლება განვაყალიბოთ.

უმაღლესი საგანმანათლებლო დაწესებულებები ამზადებენ პიროვნებას პროფესიული მოღვაწეობისთვის, რომელიც მოითხოვს შესაბამის სამეცნიერო ცოდნისა და მეცნიერული მეთოდების გამოყენებას.⁷² შესაბამისად, სტუდენტი უმაღლეს საგანმანათლებლო დაწესებულებაში ეუფლება მის მიერ შერჩეულ პროფესიას და იღებს თეორიულ ცოდნას სალექციო კურსების დახმარებით და გამოცდის წარმატებით ჩაბარების შემთხვევაში დასტურდება მისი ცოდნა და კომპეტენცია პროფესიული საქმიანობის რომელიმე ნაწილთან/კომპონენტთან მიმართებით. ამასთანავე, გამოცდის წარმატებით ან წარუმატებლად ჩაბარება ცალსახად ახდენს გავლენას კონკრეტული პროფესიული საგნის წარმატებით დახურვაზე, რაც საბოლოოდ სტუდენტისათვის ცოდნის დამადასტურებელი საბუთის-დიპლომის გაცემის საკითხზეც მოქმედებს, რაც ზოგიერთი პროფესიული საქმიანობის განხორციელებისათვის აუცილებელი კომპონენტია. შესაბამისად, სტუდენტის მიერ შესრულებული საგამოცდო ნაშრომი, მის პერსონალურ ინფორმაციად განხილვასთან მიმართებით შეიძლება გავუტოლოთ პროფესიული გამოცდის ჩაბარებას.

ინფორმაციის პერსონალურ მონაცემად ჩასათვლელად მთავარი კრიტერიუმია ინფორმაციის საფუძველზე პიროვნების პირდაპირი ან არაპირდაპირი

⁶⁹ იქვე, para. 21-23.

⁷⁰ Peter Nowak v Data Protection Commissioner, [CJEU], C-434/16, 20 December 2017.

⁷¹ იქვე.

⁷² „უმაღლესი განათლების შესახებ“ საქართველოს კანონის მე-3 მუხლის მესამე პუნქტის „ა“ ქვეპუნქტი.

ფორმით იდენტიფიკაცია,⁷³ რაც თითოეული შემთხვევის გარემოებებზეა დამოკიდებული,⁷⁴ მათ შორის, საჭიროებს შეფასებას, „მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიებისა და, ზოგადად, ტექნოლოგიური განვითარების გათვალისწინებით“.⁷⁵ ასევე, ვინაიდან, ევროპულ სამართალში პირადი მონაცემის ქვეშ მოიაზრება ირიბი იდენტიფიკაციის შესაძლებლობაც, ევროპის მართლმსაჯულების სასამართლოს მითითებით,⁷⁶ საერთოდ არ არის აუცილებელი გამოცდის შემსწორებელს ნაშრომის გასწორებისას პირდაპირ შეეძლოს გამოსაცდელი პირის იდენტიფიცირება. შესაბამისად, საგამოცდო ნაშრომი ითვლება პერსონალურ მონაცემად, იმ შემთხვევაშიც კი, თუ იგი დაშტრიხულია, მაგრამ ამ ინფორმაციის საფუძველზე, დიდი ძალისხმევითა და დაბრკოლებების გარეშე, შესაძლებელია არაპირდაპირი, დამატებითი მახასიათებლებით სტუდენტის ვინაობის დადგენა.

საქართველოს საგანმანათლებლო დაწესებულებებში არსებული პრაქტიკით, დისტანციური სწავლების მიმდინარეობისას, სტუდენტები ელექტრონულ პროგრამაში ტვირთავენ შესრულებულ დავალებებს და საგამოცდო ნაშრომებს ან იყენებენ ელექტრონულ ფოსტას მათი პირდაპირ ლექტორისთვის გასაგზავნად.⁷⁷ მასწავლებლები/ლექტორები შესრულებულ დავალებებზე უკუკავშირის ასევე ელექტრონული პროგრამის ან ელექტრონული ფოსტის მეშვეობით ახორციელებენ.⁷⁸ შესაბამისად, საგამოცდო ნაშრომებით სტუდენტის პირდაპირი გზით იდენტიფიცირება შესაძლებელი და ეს მონაცემი ცალსახად პირის პერსონალური მონაცემია.

გარდა საგამოცდო ნაშრომებისა, სტუდენტის მიერ ელექტრონულ ფორმატში შესრულებული დავალებებიც უნდა ჩაითვალოს მის პერსონალურ მონაცემად. მოცემულ შემთხვევაშიც დავალებები დაკავშირებულია სტუდენტის პროფესიის თეორიული თუ პრაქტიკული კომპონენტის რომელიმე ნაწილში ცოდნის გამოვლენაზე, ხშირ შემთხვევაში, გარდა წმინდა თეორიული მასალისა, მოიცავს

⁷³ თბილისის სააპელაციო სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2016 წლის 26 აპრილის გადაწყვეტილება №33/1059-15.

⁷⁴ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბილისი, 2017, 67.

⁷⁵ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, preamble, para. 26.

⁷⁶ Peter Nowak v Data Protection Commissioner, [CJEU], C-434/16, 20 December 2017.

⁷⁷ სახელმწიფო ინსპექტორის სამსახური, რეკომენდაცია-პერსონალური მონაცემების დამუშავება დისტანციური სწავლების პროცესში, იანვარი, 2022, 7.

⁷⁸ იქვე.

სტუდენტის ნააზრევს და პირად შეხედულებებს. ამასთანავე, სტუდენტის მიერ შესრულებული დავალებების შედეგად დაგროვებული ქულები, საგამოცდო ქულებთან ერთობლიობაში გავლენას ახდენს საგნის და საბოლოოდ უნივერსიტეტის წარმატებით დასრულებაზე. ცხადია, რომ სტუდენტის იდენტიფიცირება არცერთ შემთხვევაში არ არის დაკავშირებული დიდ სირთულესთან, და არანაირ პრობლემას არ წარმოადგენს მათ მიერ შესრულებული დავალებების შემთხვევაშიც. დასკვნის სახით კი შეიძლება ითქვას, რომ საგანმანათლებლო დაწესებულებებში დაცული შესრულებული დავალება და საგამოცდო ნაშრომი, წარმოადგენს სტუდენტის პერსონალურ მონაცემს.

4. უნივერსიტეტის ელექტრონული პლატფორმის მეშვეობით არამიზნობრივად დამუშავებული პერსონალური მონაცემები

უკვე რამდენიმე ათწლეულია, რაც უნივერსიტეტები სასწავლო პროცესის მართვისას ელექტრონულ პლატფორმებს იყენებენ, რომლებიც კიდევ უფრო აქტიუალური დისტანციური სწავლების განმავლობაში გახდა.⁷⁹ ელექტრონული პლატფორმის ფუნქციების გათვალისწინებით, სტუდენტს აქვს შესაძლებლობა დარეგისტრირდეს მისთვის სასურველ საგანზე, ჰქონდეს წვდომა სალექციო კურსის მასალებზე, სილაბუსებზე და შესასრულებელ აქტივობებზე, ასევე, საკუთარ აკადემიურ მოსწრებასა და ფინანსურ დავალიანებაზე. ამასთანავე, შესაძლებელია ჰქონდეს შეტყობინებების მიღებისა და გაგზავნის, ონლაინ რეჟიმში განცხადებების დაწერისა და გაგზავნის შესაძლებლობა და სხვა.⁸⁰

მსგავსი ტიპის პლატფორმები საქართველოშიც დაწერგილია, რომლებიც უმეტესწილად უნივერსიტეტის საკუთრებაშია, იმართება მათ მიერ და საკმაოდ აქტიურად გამოიყენება, განსაკუთრებით დისტანციური სწავლების მიმდინარეობისას.⁸¹ საგანმანათლებლო დაწესებულებების მიერ ამ პლატფორმების მეშვეობით მუშავდება ისეთი პერსონალური მონაცემები, როგორიცაა სტუდენტის

⁷⁹ Sadler C., Privacy Considerations in Higher Education Online Learning, Washington, October, 2020, 10.

⁸⁰ Bradley V., M., Simkova M., Stepanek J., Using Learning Management Systems to Promote Online Instruction in the book: Exploring Online Learning Through Synchronous and Asynchronous Instructional Methods, edited by Sistek-Chandler C., Hershey PA, 2020, 124-125.

⁸¹ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 14 ივნისის №1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემონმების დასრულების შესახებ“, სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 20 აპრილის №1/115/2021 გადაწყვეტილება „სსიპ – ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

სახელი, გვარი, ელ-ფოსტა, პაროლი, საგანმანათლებლო პროგრამა, აკადემიური მოსწრება/შეფასებები და ფინანსური დავალიანება.⁸² თუმცა, არსებობს რისკი, რომ უნივერსიტეტები ამ პლატფორმების მეშვეობით, არამიზნობრივად დაამუშავენ მეტი მოცულობის პერსონალურ ინფორმაციას, რაც შესაძლოა პირად ცხოვრებაში ჩარევადაც კი მივიჩნიოთ. მათ შორის, შეიძლება იყოს ისეთი ინფორმაცია, როგორიცაა სტუდენტის ოჯახური მდგომარეობა, პირადობის მოწმობის ნომერი, დაბადების ადგილი⁸³ და სხვა.

უნდა აღინიშნოს, რომ მონაცემთა დამუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად საჭირო მონაცემების დამუშავება წარმოადგენს მონაცემთა დამუშავების დასაშვებობის ერთ-ერთ მთავარ საფუძველს.⁸⁴ ცხადია, საგანმანათლებლო დაწესებულებას, თავისი უფლებამოსილებების განსახორციელებლად ესაჭიროება სტუდენტის იდენტიფიკაცია, რაც მხოლოდ მისი სახელისა და გვარის საფუძველზე ვერ განხორციელება, რადგან ერთი და იმავე სახელითა და გვარით ხშირად რამდენიმე ადამიანია რეგისტრირებული. ამდენად, საქართველოს უნივერსიტეტები სახელსა და გვართან ერთად, ასევე ამუშავენ ისეთ პერსონალურ მონაცემს, როგორიცაა სტუდენტის პირადი ნომერი.

მნიშვნელოვანია, რომ საგანმანათლებლო უწყებები მონაცემებს ამუშავენდნენ კონკრეტული, მკაფიო და ლეგიტიმური მიზნებისთვის და იმ მოცულობით, რაც მიზნის მისაღწევად არის საჭირო და პროპორციული.⁸⁵ ვინაიდან, მონაცემთა დამუშავებელი მკაცრად არის შეზღუდული მონაცემთა შეგროვებაში და მას მხოლოდ იმ მონაცემების დამუშავება შეუძლია, რომლებიც პირდაპირ შეესაბამება დამუშავების კონკრეტულ მიზანს. უნდა აღინიშნოს, რომ პირის პირადი ნომერი უნიკალური საიდენტიფიკაციო მონაცემია,⁸⁶ რომლის მეშვეობითაც, პირდაპირ, ყოველგვარი დამატებითი მონაცემის გარეშე შესაძლებელია პირის იდენტიფიცირება. ამიტომაც, ამ მონაცემებთან ერთად, საგანმანათლებლო დაწესებულებების მიერ, დამატებითად, ფოტოსურათის, დაბადების ადგილისა და

⁸² იქვე.

⁸³ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №1/205/2021 გადაწყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემომწმობის დასრულების შესახებ“, 16.

⁸⁴ საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2021 წლის 27 მაისის განჩინება №ბს-962(კ-19).

⁸⁵ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Art. 5, para. 1c.

⁸⁶ „სამოქალაქო აქტების შესახებ“ საქართველოს კანონის 27-ე მუხლის პირველი პუნქტი.

პირადობის მონმობის ნომრის დამუშავება მხოლოდ სტუდენტის ვინაობის დადგენის და მისი საგანმანათლებლო პროცესში მონაწილეობისთვის იდენტიფიცირების მიზნით⁸⁷ დაუშვებლად უნდა მივიჩნიოთ. ამასთანავე, პირის პირადობის მონმობის ნომერი არ არის მუდმივი და იგი შეიცვლება ყოველ ჯერზე, როდესაც სტუდენტი ახალ პირადობის დამადასტურებელ მონმობას აიღებს. შესაბამისად, მონაცემთა მინიმიზაციის პრინციპიდან გამომდინარე, ვინაიდან მხოლოდ სახელის, გვარის და პირადი ნომრის გამოყენებით შესაძლებელია მიზნის მიღწევა, დამატებითი მონაცემების დამუშავება დაუშვებლად უნდა მივიჩნიოთ, თუ არ არსებობს ამ დამატებითი მონაცემების დამუშავების აუცილებელი საჭიროება. ამასთან, დისტანციური სწავლების ფარგლებში და მის ფარგლებს გარეთ გამოყენებული ელექტრონული სისტემის მეშვეობით ამ მონაცემების სავალდებულოდ მოპოვება არც ამ სისტემის მეშვეობით სასწავლო პროცესის მართვასთანაა დაკავშირებული და სტუდენტის გადაჭარბებული, არამიზნობრივი პერსონალური მონაცემია, რომელიც უნივერსიტეტის მიერ არ უნდა მუშავდებოდეს⁸⁸.

მართალია, საკანონმდებლო დონეზე არსად არსებობს პირის პირადი და ოჯახური ცხოვრების უფლების⁸⁹ ერთგვაროვანი განმარტება, ამ სფეროს ამოუწურვადობიდან გამომდინარე,⁹⁰ თუმცა, პირის ოჯახური მდგომარეობის შესახებ ინფორმაცია ცალსახად წარმოადგენს ამ უფლებით დაცულ სფეროს და იგი მაქსიმალურად უნდა იყოს დაცული საჯაროობისაგან.⁹¹ ამდენად, რაც შეეხება ელექტრონული პლატფორმის მეშვეობით სტუდენტის ოჯახური მდგომარეობის შესახებ ინფორმაციის დამუშავებას, საგანმანათლებლო დაწესებულებას ამ მონაცემის დასამუშავებლად უნდა ჰქონდეს მკაფიოდ განსაზღვრული მიზანი და საფუძველი. თუმცა, დისტანციური სწავლებისას, ელექტრონული პორტალის მეშვეობით სასწავლო პროცესის მართვის მიზნებისთვის, ასეთი ინფორმაციის სამართლებრივი საფუძვლის გარეშე დამუშავება, მიზნის მიღწევის არამართლზომიერ და არაპროპორციულ საშუალებად შეიძლება ჩაითვალოს.

გარდა აღნიშნულისა, ელექტრონული პლატფორმის მეშვეობით სტუდენტის პერსონალური მონაცემების დამუშავებისას, ასევე, მნიშვნელოვანია გა-

⁸⁷ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №1/205/2021 გადაწყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

⁸⁸ იქვე.

⁸⁹ საქართველოს კონსტიტუციის მე-15 მუხლის პირველი პუნქტი; ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია, 1950, მუხლი 8.

⁹⁰ ქათამაძე ნ., პირადი არაქონებრივი უფლებების დაცვის სამოქალაქო სამართლებრივი მექანიზმი, სადისერტაციო ნაშრომი, თბილისი, 2020, 105.

⁹¹ საქართველოს უზენაესი სასამართლოს 2003 წლის 24 აპრილის გადაწყვეტილება №3კ-1240-02.

ნებისმიერ ინტერნეტპროტოკოლის (IP) მისამართი. იგი ლოკალურ ქსელში ან ინტერნეტში ჩართული მონაცემების უნიკალური იდენტიფიკატორია⁹² და პირის პერსონალური მონაცემს წარმოადგენს.⁹³ IP მისამართი მომხმარებლის ზუსტი იდენტიფიცირების საშუალებას იძლევა.⁹⁴ ასეთი მონაცემის დამუშავებას შესაძლებელია ჰქონდეს კიბერთავდასხმების პრევენციისა და, საჭიროების შემთხვევაში, სისხლისსამართლებრივი წარმოების დაწყების მიზანი⁹⁵ ან საჭირო იყოს სხვა საჯარო ინტერესების დასაცავად, მათ შორის, შესაძლოა საჭირო იყოს დისტანციური სწავლების მიმდინარეობისასაც. მაგალითად, IP მისამართის დამუშავება დასაშვებად უნდა მივიჩნიოთ სტუდენტთა პერსონალურ ინფორმაციაზე წვდომის მქონე პირების შემთხვევაში, რათა აღირიცხოს მონაცემთა მიმართ შესრულებული ნებისმიერი ქმედება, მათ შორის, მონაცემთა დათვალიერება თუ მათში რაიმე ცვლილების განხორციელება. თუმცა, რამდენად არის დასაშვები სტუდენტის IP მისამართის დამუშავება მსჯელობის საგანია და დამოკიდებულია კონკრეტულ გარემოებებზე. ვინაიდან, პერსონალურ მონაცემთა დაცვის სამსახურმა არაერთხელ მიუთითა კანონმდებლობის მოთხოვნაზე – ავტომატური სახით დამუშავებული პერსონალური მონაცემების მიმართ ნებისმიერი ქმედების აღრიცხვის ვალდებულებაზე,⁹⁶ შეგვიძლია დავასახელოთ ერთი მნიშვნელოვანი გარემოება, რომელიც ყოველ კონკრეტულ შემთხვევაში უნდა მივიღოთ მხედველობაში. კერძოდ, იმ შემთხვევაში, თუ უნივერსიტეტის ელექტრონულ პროგრამას აქვს შესაბამისი ფუნქცია, რომლის მეშვეობითაც სტუდენტს შეუძლია გარკვეული ცვლილებები შეიტანოს მის პერსონალურ მონაცემებში, მაშინ სტუდენტის IP მისამართის დამუშავება დასაშვებია იმ მიზნით, რომ აღირიცხოს ამ პერსონალური მონაცემის მიმართ განხორციელებული ცვლილება. მაგალითად, თუ პლატფორმის მეშვეობით სტუდენტს შეუძლია შეაგოს მისი რომელიმე პერსონალური მონაცემის შესახებ ინფორმაცია და შეიტანოს მასში ცვლილება თავისი სურვილისამებრ (მაგ. გადააკეთოს, წაშალოს, ა.შ.), ან თუ ამ პლატფორმის მეშვეობით ტვირთავს საგამოცდო ნაშრომს და სა-

⁹² სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 20 აპრილის №1/115/2021 გადაწყვეტილება „სსიპ – ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

⁹³ Patrick Breyer v. Bundesrepublik Deutschland, [CJEU], C-582/14, 19 October 2016.

⁹⁴ Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), [CJEU], C-70/10, 24 November 2011.

⁹⁵ Patrick Breyer v Bundesrepublik Deutschland, [CJEU], C-582/14, 19 October 2016.

⁹⁶ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №1/205/2021 გადაწყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“; საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 14 ივნისის №გ-1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემოწმების დასრულების შესახებ“.

შინაო დავალებას. მსგავს შემთხვევებში სტუდენტის IP მისამართის დამუშავების კანონიერი ინტერესი ექნება საგანმანათლებლო დაწესებულებასაც, რათა აღრიცხოს პერსონალურ მონაცემთა განხორციელებული ნებისმიერი ცვლილება და რაც, ასევე მიმართული იქნება სტუდენტების ინტერესების დასაცავად. აღნიშნულისგან განსხვავებით, დაუშვებელია სტუდენტის IP მისამართის დამუშავება ლექციაზე დასწრების მიზნებისთვის. მოცემული განპირობებულია იმით, რომ დისტანციური სწავლების მიმდინარეობისას არანაირი სამართლებრივი საფუძველი არ აქვს პირის ადგილმდებარეობის შესახებ ინფორმაციის მოპოვებას და შენახვას. შესაბამისად, სტუდენტის IP მისამართის დამუშავება საგანმანათლებლო დაწესებულებაში არსებული ელექტრონული პლატფორმის მეშვეობით არ შეიძლება ნებისმიერი შემთხვევისთვის ჩაითვალოს პერსონალური მონაცემის არამიზნობრივ დამუშავებად, პირიქით, გარკვეულ შემთხვევებში გამართლებულიც კი შეიძლება იყოს.

გარდა ზემოაღნიშნულისა, მნიშვნელოვანია ყურადღება გავამახვილოთ დისტანციური სწავლების პროცესში, სინქრონულ რეჟიმში მიმდინარე ონლაინგამოცდების ჩატარებისას, უმაღლესი საგანმანათლებლო დაწესებულებების მიერ სპეციალური ელექტრონული სისტემის/პლატფორმის გამოყენებაზე, რომელიც უზრუნველყოფს სტუდენტის იდენტიფიკაციასა და გადანერის რისკების შემცირებას.⁹⁷ მსგავსი ტიპის ელექტრონული პროგრამები ხშირად გამოიყენება საზღვარგარეთის ქვეყნებში, თუმცა პერსონალურ მონაცემთა დაცვის სამსახურის მიერ უნივერსიტეტების შემონმების დასრულების შესახებ გამოთხოვილი გადანყვეტილებების ანალიზის საფუძველზე არ იკვეთება, რომ მსგავსი პრაქტიკა საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებებს დაემკვიდრებინოთ. აღსანიშნავია, რომ პლატფორმის მეშვეობით სტუდენტების ხმისა და ვიზუალური გამოსახულების დამუშავება და მათ ქცევაზე დაკვირვება, გამოცდის გადანერის რისკების მინიმიზაციის მიზნით, დანიის პერსონალურ მონაცემთა დაცვის სააგენტომ პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან შესაბამისად ცნო და დაადგინა, რომ ამ შემთხვევაშიც მონაცემთა დამუშავებელი შესაბამისი საგანმანათლებლო დაწესებულებაა, რომელიც სტუდენტის პერსონალურ მონაცემებს ამუშავებს უფლებამოსილი პირის მეშვეობით.⁹⁸ მაგრამ, ასეთი გადანყვეტილების მიღებით, გზა არ უნდა გაეხსნას საგანმანათლებლო დაწესებულებებს, გაუმართლებლად ჩაერიონ სტუდენტის პირად ცხოვრებაში და ნებისმიერ შემთხვევაში დაამუშაონ დიდი რაოდენობით

⁹⁷ Coghlan, S., Miller, T. & Paterson, J., Good Proctor or “Big Brother”? Ethics of Online Exam Supervision Technologies, *Philosophy & Technology*, Vol. 34, 2021, 1581–1606.

⁹⁸ The Danish Data Protection Agency, University’s use of supervision program at online exam, 26.01.2021, <<https://bit.ly/3uk7Auw>> [11.06.2022].

პერსონალური მონაცემები. მათ შორის, მოითხოვონ სტუდენტის ბიომეტრიული მონაცემების დამუშავება, გამოცდის დაშვების წინაპირობად⁹⁹ და მოიპოვონ წვდომა გამოცდის მიმდინარეობისას მონაწილის მიერ კომპიუტერში არსებულ აქტივობებზეც.¹⁰⁰ ამ შემთხვევაში გასათვალისწინებელია მონაცემთა მინიმალაციის პრინციპი, რათა შესაძლებელი იყოს სამართლიანი ბალანსის მიღწევა¹⁰¹ სტუდენტის ინტერესებს, პირადი ცხოვრების სფეროსა და საგანმანათლებლო დაწესებულების მიერ დადგენილი მიზნის მიღწევის საშუალებებს შორის. გამოცდის ჩატარების მიზანი სტუდენტის ცოდნის გამოვლენაა, რისი მიღწევაც მხოლოდ თეორიული მასალის გამოკითხვა/დანერის ნაცვლად შესაძლებელია ისეთი დავალების შესრულების გზით, როდესაც სტუდენტს დასჭირდება მიღებული ცოდნის სინთეზი, კრიტიკული აზროვნება, შესაბამისი ინფორმაციის/გარემოებების შეფასება და სხვა უნარები.¹⁰² შესაბამისად, მონაცემთა გადაჭარბებული რაოდენობის დამუშავების თავიდან აცილების მიზნით, როდესაც შესაძლებელია საგანმანათლებლო დაწესებულებებმა გამოცდები ჩაატარონ ზეპირი ფორმით ან სტუდენტს დაავალონ მეტად პრაქტიკული დავალების შესრულება, მინიმუმამდე უნდა იქნეს დაყვანილი მსგავსი პროგრამების პრაქტიკაში გამოყენება. სავსებით დასაშვებია, რომ ასეთი დავალებები კონკრეტული სპეციალობისა და საგნის საგამოცდო მასალის ჩასაბარებლად გარდაუვალი იყოს, ვინაიდან კურსის ფარგლებში დაგროვებული თეორიული ცოდნის შემოწმება იყოს აუცილებელი ან იგი არ იძლეოდა ანალიტიკური ნაშრომის შესრულების შესაძლებლობას. შესაბამისად, უმაღლესი საგანმანათლებლო დაწესებულებების მიერ მსგავსი პლატფორმების გამოყენება, მათი საჭიროებისა და მოსალოდნელი რისკების წინასწარი შეფასების გათვალისწინებით, დასაშვებად უნდა მივიჩნიოთ ზოგიერთი შემთხვევისთვის.

ზემოაღნიშნული მსჯელობიდან გამომდინარე, დასკვნის სახით, შეიძლება ითქვას, რომ დისტანციური სწავლების პროცესში საგანმანათლებლო დაწესებულებები ამუშავებენ სტუდენტის ვინაობის დამდგენ და საკონტაქტო მონაცემებს, საგამოცდო ნაშრომსა და შესრულებულ დავალებებს. ასევე, რიგ შემთხვევებში,

⁹⁹ Kiennert C., De Vos N., Knockaert M., Garcia-Alfaro J., The Influence of Conception Paradigms on Data Protection in E-Learning Platforms: A Case Study, IEEE Access, Vol. 7, 2019, 64110-64119, იხ., <<https://bit.ly/3umsU2a>> [01.07.2022].

¹⁰⁰ Raman, R., Sairam B., Veena G., Vachharajani H., Nedungadi P., Adoption of online proctored examinations by university students during COVID-19: Innovation diffusion study, Education and Information Technologies, Vol. 26, 2021, 7339-7358, იხ., <<https://bit.ly/3NIDZS2>> [15.06.2022].

¹⁰¹ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის №გ-1/043/2015 გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, 5.

¹⁰² განათლების ხარისხის განვითარების ეროვნული ცენტრი, შეფასების ალტერნატიული მეთოდები ელექტრონულ სწავლებაში, თბილისი, 2020, 4-6.

შესაძლოა ამუშავებდნენ სტუდენტის ვიზუალურ გამოსახულებას, ხმას, IP მისამართს და ბიომეტრიული მონაცემებს. ამასთან, მნიშვნელოვანია, რომ უნივერსიტეტს თითოეულ მონაცემთან მიმართებით გააჩნდეს მათი დამუშავების მიზანი, სამართლებრივი საფუძველი და დამუშავება განახორციელოს კანონმდებლობით დადგენილი პრინციპების შესაბამისად.

III. უნივერსიტეტის მოვალეობები დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების დამუშავებისას

1. სტუდენტის თანხმობის საჭიროება მონაცემთა დამუშავებასა და გავრცელებაზე

1.1. სტუდენტის თანხმობა, როგორც პერსონალური მონაცემის დამუშავების საფუძველი

მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავების ერთ-ერთი საფუძველია.¹⁰³ თუმცა, კანონმდებლობაში ასახული დამუშავების საფუძვლები არაა კუმულაციური ხასიათის და რომელიმე მათგანის არსებობაც უკვე საკმარისია, იმისთვის, რომ მონაცემთა დამუშავებელი იყოს უფლებამოსილი, დაამუშაოს სუბიექტის პერსონალური მონაცემები.¹⁰⁴ გარდა სუბიექტის თანხმობისა, მონაცემთა დამუშავების საფუძველი შეიძლება პირდაპირ კანონით იყოს გათვალისწინებული, მათი დამუშავება შეიძლება საჭირო იყოს მონაცემთა დამუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად ან მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად, ან არსებობდეს მონაცემთა კანონიერი დამუშავებისთვის კანონმდებლობით დადგენილი სხვა საფუძვლები.¹⁰⁵

¹⁰³ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Art. 4 para.11; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Art. 5 para. 2; „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის „ა“ ქვეპუნქტი.

¹⁰⁴ Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Josep Lauermaun v. Österreichischer Rundfunk, [CJEU], C-465/00, C-138/01 and C-139/01, 20 May 2003, par.65; Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v Administración del Estado, [CJEU], C-468/10 and C-469/10, 24 November 2011, para.26.

¹⁰⁵ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლი.

მნიშვნელოვანია, რომ საგანმანათლებლო დაწესებულებებმა განასხვაონ სტუდენტის მონაცემთა დამუშავებაზე ინფორმირებული თანხმობის მიღების საჭიროება, მისი მონაცემების დამუშავების თაობაზე ინფორმირების¹⁰⁶ ვალდებულებისგან. ეს უკანასკნელი სტუდენტის, როგორც მონაცემთა სუბიექტის უფლებას წარმოადგენს, რომ იყოს ინფორმირებული იმ პერსონალური მონაცემების ავტომატურ დამუშავებაზე, რომელიც მას შეეხება.¹⁰⁷

აღსანიშნავია, რომ დისტანციური სწავლებისას, მონაცემთა დამუშავების მთავარი საფუძველი, ყოველ კონკრეტულ შემთხვევაში, სტუდენტის თანხმობა არ არის. სტუდენტის თანხმობა არ არის საჭირო თუ უმაღლესი საგანმანათლებლო დაწესებულების მიერ დისტანციურ სწავლების განხორციელება არის გარდაუვალი და ქვეყნის კანონმდებლობა მას პირდაპირ აკისრებს ვალდებულებას სწავლის ასეთი ფორმით გაგრძელების თაობაზე.¹⁰⁸ ამ შემთხვევაში, მონაცემთა დამუშავების პროცესი უფრო მეტად ეფუძნება ისეთ საფუძველებს, როგორიცაა კანონმდებლობით დაკისრებული მოვალეობით გამოწვეული საჭიროება და კანონით გათვალისწინებული შემთხვევები.¹⁰⁹ მოცემულ მსჯელობაზე დაყრდნობით, შეიძლება ითქვას, რომ პერსონალური მონაცემების დამუშავებაზე მონაცემთა სუბიექტის თანხმობა აუცილებელია მხოლოდ მაშინ, როდესაც სწავლების დისტანციური ფორმა სუბიექტის არჩევანია და არა გარდაუვალი აუცილებლობა. თუმცა, მსგავსი მსჯელობაც არამართებულად შეიძლება ჩაითვალოს რამდენიმე გარემოების გამო. უპირველესად, უნდა აღინიშნოს, რომ უმაღლესი საგანმანათლებლო დაწესებულებების მთავარი მიზანია სტუდენტისთვის პროფესიული ცოდნის მიცემა და პროფესიული საქმიანობისათვის მომზადება.¹¹⁰ სტუდენტებისათვის განათლების მინიჭებისათვის ფორმალური საგანმანათლებლო პროცესი კი შეიძლება განხორციელდეს რო-

¹⁰⁶ Ivanova Y., Data Controller, Processor, or Joint Controller: Towards Reaching GDPR Compliance in a Data and Technology-Driven World, in the book: Personal data protection and legal developments in the European Union, edited by Tzanou M., Hershey PA, 2020, 76.

¹⁰⁷ არჩუაძე თ., პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016, 26, იხ. ციტირება: Data Protection and Privacy: Jurisdictional Comparisons, edited by Kuschewsky M., UK, Thompson Reuters, 2012, 141.

¹⁰⁸ Die Datenschutzkonferenz, Orientierungshilfe – Online-Lernplattformen im Schulunterricht, 2018, 5.

¹⁰⁹ შპს „იუაი“- ჩანტლაძე ტ., სულხანიშვილი ე., ცინცქილაძე გ., ჯიშიაშვილი გ., თემატური რეკომენდაციები COVID 19 პანდემიის დროს პერსონალური მონაცემების მართვაზე, ანგარიში დისტანციური სწავლებისას პერსონალურ მონაცემთა დაცვის შესახებ, 2021, 41.

¹¹⁰ Chan, R. Y., Understanding the purpose of higher education: An analysis of the economic and social benefits for completing a college degree, Journal of Education Policy, Planning and Administration, No. 6(5), 2016, 2-3.

გორც შერეული (ჰიბრიდული) სწავლებისას, ასევე დისტანციური და ტრადიციული (პირისპირ) სწავლების დროსაც.¹¹¹ ტექნოლოგიების განვითარებასთან ერთად, იცვლება საგანმანათლებლო პროცესის ფორმა,¹¹² თუმცა, ტრადიციული მეთოდის მსგავსად, სტუდენტისთვის ცოდნის გაზიარების და მისი პროფესიონალად ჩამოყალიბების მიზნის მიღწევას ემსახურება დისტანციური სწავლებაც.¹¹³ შესაბამისად, უცვლელი რჩება უნივერსიტეტის ვალდებულება, შეასრულოს კანონმდებლობით დადგენილი პირობები და ასეთ შემთხვევაში, მნიშვნელობა არ აქვს, დაწესებულება სტუდენტის საკონტაქტო, ვინაობის დამადასტურებელ, აკადემიური მოსწრების აღრიცხვისა თუ აკადემიური ხარისხის მინიჭების შესახებ მონაცემებს დაამუშავებს სწავლების დისტანციური, თუ აუდიტორული ფორმით განხორციელებისას. ცხადია, რომ სწავლების ფორმის ცვლილებისგან განსხვავებით, ასეთი პერსონალური მონაცემების დამუშავების მიზანი არ იცვლება. ამდენად, სწავლების დისტანციური ფორმის არჩევის შემთხვევაში, საგანმანათლებლო დაწესებულებებისთვის პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი და მიზანი, სტუდენტებისგან ამ მონაცემების დამუშავებაზე მხოლოდ თანხმობის მოპოვება არ უნდა იყოს. შესაბამისად, სწავლების ფორმის არჩევის მიუხედავად, თანხმობის საჭიროება არსებობს მხოლოდ იმ პერსონალური მონაცემების დამუშავებაზე, რომელიც არ გამომდინარეობს კანონმდებლობით დაკისრებული მოვალეობების შესრულების ვალდებულებიდან. მაგალითად, სტუდენტის თანხმობა ესაჭიროება ისეთი პერსონალური მონაცემების დამუშავებას, როგორიცაა მისი IP მისამართი, პლატფორმაზე შესვლისა და გასვლის დროები, ელექტრონული პლატფორმის ჩატის ველში განხორციელებულ მიმოწერა და სხვა. ამასთან, თანხმობა თავისთავად არ ნიშნავს იმ ფაქტს, რომ სტუდენტის პერსონალური მონაცემების დამუშავებაზე უმაღლეს საგანმანათლებლო დაწესებულებებს განუსაზღვრელი უფლებამოსილება მიეცემათ.

რაც შეეხება განსაკუთრებული კატეგორიის მონაცემებს, საგანმანათლებლო დაწესებულებისთვის აუცილებელია სტუდენტის თანხმობის მიღება ამ კატეგორიის მონაცემთა დამუშავებისთვის,¹¹⁴ რაც მხოლოდ გამონაკლის და გა-

¹¹¹ New Jersey Administrative Code, Art. 9A:1-1.2; The Pennsylvania Code, Title 22, Chapter 31.2; „უმაღლესი განათლების შესახებ“ საქართველოს კანონის მე-2 მუხლის „პ2“ ქვეპუნქტი.

¹¹² Patru M., Khvilon E., Open and distance learning: trends, policy and strategy considerations; Hamburg, 2002, 7-8.

¹¹³ UNESCO Institute for Lifelong Learning – Carlsen A., Holmberg C., Neghina C., Owusu-Boampong A., Closing the gap: opportunities for distance education to benefit adult learners in higher education, Hamburg, 2016, 41-51.

¹¹⁴ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მეორე პუნქტი.

რდაუვალ შემთხვევებში უნდა განხორციელდეს.¹¹⁵ თუმცა, მსგავსი საჭიროება არ არსებობს სპეციალური საგანმანათლებლო საჭიროების მქონე სტუდენტების დისტანციური სწავლების პროცესში ჩართვის¹¹⁶ შემთხვევისას. მიუხედავად იმისა, რომ ამ დროს უნივერსიტეტი ამუშავებს ინფორმაციას სტუდენტის ჯანმრთელობის მდგომარეობის შესახებ, რაც განსაკუთრებული კატეგორიის მონაცემად ითვლება,¹¹⁷ აღნიშნული წარმოადგენს კანონით გათვალისწინებულ გამონაკლის შემთხვევას და უმაღლესი საგანმანათლებლო დაწესებულება ასეთ დროს უფლებამოსილია დაამუშაოს სტუდენტის განსაკუთრებული კატეგორიის პერსონალური მონაცემი, მისგან თანხმობის მიღების გარეშე. მსგავსი გამონაკლისი არსებობს დისტანციური სწავლების პროცესში ჩართული მსჯავრდებული სტუდენტების¹¹⁸ პერსონალური მონაცემების დამუშავებისთვისაც. ინფორმაცია სტუდენტის სისხლის სამართლის საქმის წარმოებისა და ნასამართლობის შესახებ, ასევე, შესაბამისი უსაფრთხოების ზომები, განსაკუთრებული კატეგორიის მონაცემებია.¹¹⁹ თუმცა, მსჯავრდებულთა განათლების უფლების რეალიზება მისი რესოციალიზაცია/რეაბილიტაციის ნაწილია.¹²⁰ ამ გარემოების გათვალისწინებით, კანონიერია განსაკუთრებული კატეგორიის პერსონალური მონაცემის დამუშავება მონაცემთა სუბიექტის წერილობითი თანხმობის გარეშე.¹²¹ თუმცა, დამუშავებისთვის სამართლებრივი საფუძვლების არსებობის შემთხვევაშიც კი, დაუშვებელია ასეთი ტიპის სტუდენტის პერსონალური მონაცემების გამჟღავნება მესამე პირთათვის.¹²²

¹¹⁵ შპს „იუაი“ – ჩანტლაძე ტ., სულხანიშვილი ე., ცინცქილაძე გ., ჯიშიაშვილი გ., თემატური რეკომენდაციები COVID 19 პანდემიის დროს პერსონალური მონაცემების მართვაზე, ანგარიში დისტანციური სწავლებისას პერსონალურ მონაცემთა დაცვის შესახებ, 2021, 9.

¹¹⁶ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-2 პუნქტის „კ“ ქვეპუნქტი.

¹¹⁷ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Art. 9 para.1; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Article 6; „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის „ა“ ქვეპუნქტი.

¹¹⁸ <<https://bit.ly/3nIFzZz>> [22.06.2022].

¹¹⁹ Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Article 6, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის „ა“ ქვეპუნქტი.

¹²⁰ UNESCO Institute for Lifelong Learning-Cormac B., Education in prison: a literature review, Hamburg, 2021, 40-47.

¹²¹ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-2 პუნქტის „ზ1“ ქვეპუნქტი.

¹²² „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მესამე პუნქტი.

ნებისმიერ შემთხვევაშია აუცილებელი სტუდენტისგან თანხმობის მიღება დისტანციური სწავლებისას ლექციების აუდიო-ვიდეო ჩანერის განხორციელებისას. სინქრონულ რეჟიმში მიმდინარე ლექციის ჩანერა ვერ იქნება უმაღლესი საგანმანათლებლო დაწესებულებისათვის დაკისრებული მოვალეობის – სტუდენტისთვის განათლების გადაცემის აუცილებელი კომპონენტი. აღნიშნული განპირობებულია იმით, რომ სინქრონულ რეჟიმში ლექციების მიმდინარეობისას, სტუდენტები და ლექტორები ერთსა და იმავე დროს სხვადასხვა ადგილებიდან ერთვებიან ლექციას რომელიმე ელექტრონული პლატფორმის გამოყენებით და აქვთ საშუალება მყისიერად დასვან შეკითხვები ან უპასუხონ მათ.¹²³ შესაბამისად, ამ შემთხვევაში აუდიტორული ლექციისგან მხოლოდ ერთი განსხვავებაა, რომ ლექტორი და სტუდენტი ფიზიკურად არ იმყოფებიან ერთსა და იმავე აუდიტორიაში. შესაბამისად, სინქრონული სწავლების დროს მიმდინარე ლექციების ჩანერისას დამუშავებული სტუდენტის პერსონალური მონაცემების საფუძველი ვერ იქნება კანონმდებლობით დაკისრებული მოვალეობებით გამონეული საჭიროება ან/და კანონით გათვალისწინებული შემთხვევები, ისევე, როგორც აუდიტორული ლექციების მსვლელობის აუდიო-ვიდეო ჩანერისას. დისტანციური სწავლების შემთხვევაში, ასეთი გადაწყვეტილების მიღება დამოკიდებულია კონკრეტული დაწესებულების ადმინისტრაციის მიდგომასა და სტუდენტთა გამოხატულ სურვილზე. ამასთან, ჩანერისთვის სწავლების მაქსიმალური ეფექტურობის უზრუნველყოფის სურვილი და განათლების ყველასთვის ხელმისაწვდომობის მიზანიც კი ვერ გადანონის სტუდენტების პირადი ცხოვრების ხელშეუხებლობის უფლებას.¹²⁴ შესაბამისად, ლექციების აუდიო-ვიდეო ჩანერით, სტუდენტის პერსონალური მონაცემების დამუშავება იქნება არაკანონიერი, თუ მას საფუძვლად სტუდენტების თანხმობა არ ექნება. მსგავსად, ლექციების ჩანერისა, თანხმობის მოპოვებაა საჭირო დისტანციურ რეჟიმში მიმდინარე შეხვედრის ფოტოგადაღებისთვისაც (მათ შორის, “Screenshot“-ის გადაღების შემთხვევაშიც¹²⁵).

უნდა აღინიშნოს, რომ საქართველოში დისტანციური სწავლების დაწყების შემდეგ, სოციალურ ქსელში ხშირად ვრცელდებოდა ამ ფორმით ჩატარებული ლექციების, ტრენინგების ან უნივერსიტეტის მიერ ორგანიზებული სხვა ონლაინ ღონისძიებების ფოტო/ვიდეო მასალა.¹²⁶ აღსანიშნავია, რომ პერსონალური

¹²³ „უმაღლესი განათლების შესახებ“ საქართველოს კანონის მე-2 მუხლის „პ2 ქვეპუნქტი.

¹²⁴ Peddy, A. M., *Dangerous classroom app-titude: protecting student privacy from third-party educational service providers*, Brigham Young University Education and Law Journal, No. 1, 2017, 144-145.

¹²⁵ ჯორბენაძე ს., *Covid-19 და პერსონალურ მონაცემთა დაცვა „Zoom-ის“ გამოყენებით დისტანციური სწავლებისას*, „შედარებითი სამართლის ქართულ-გერმანული ჟურნალი“, №5, 2020, 48.

¹²⁶ იქვე, 47.

მონაცემების გამჟღავნება, მონაცემთა გადაცემა, გავრცელება ან სხვაგვარად ხელმისაწვდომად გახდომა პერსონალური მონაცემის დამუშავების ერთ-ერთი ფორმაა.¹²⁷ შესაბამისად, მსგავსი ფოტო/ვიდეო მასალის სოციალურ ქსელში ან სხვა სივრცეში განთავსება, როდესაც პერსონალურ მონაცემებზე წვდომის საშუალება მესამე პირებსაც ეძლევათ, სტუდენტის პერსონალურ მონაცემთა დამუშავებად ჩაითვლება.

გასათვალისწინებელია, რომ სტუდენტის პერსონალური მონაცემების მიმართ განხორციელებული ნებისმიერი ახალი ქმედება საჭიროებს ცალკე სამართლებრივ საფუძველს.¹²⁸ მათ შორის, ამ მონაცემების გამჟღავნებისთვის აუცილებელია იყოს მონაცემთა შეგროვების საფუძვლისგან განსხვავებული, დამატებითი სამართლებრივი საფუძველი.¹²⁹ შესაბამისად, სტუდენტის თანხმობა, მისი პერსონალური მონაცემების მესამე პირებზე გამჟღავნებაზეც აუცილებელია და ასეთ შემთხვევაში, უნივერსიტეტი ვერ დაეყრდნობა მხოლოდ იმ არგუმენტს, რომ მან მონაცემები კანონიერი გზით შეაგროვა.

მიჩნეულია, რომ პირადი ცხოვრების უფლების ერთ-ერთი კომპონენტია პერსონალური მონაცემების დაცვა გამჟღავნებისაგან¹³⁰ და მათი ხელშეუხებლობა ინდივიდის ავტონომიურობის, დამოუკიდებელი განვითარებისა და მისი ღირსების დაცვის წინაპირობაა.¹³¹ ამასთანავე, პირის გამოსახულების გამოქვეყნება მეტად არსებითი ჩარევაა,¹³² ვინაიდან მათ გამჟღავნებას შესაძლოა მძიმე შედეგები ჰქონდეს მონაცემთა სუბიექტისათვის და ამ ინფორმაციის გამჟღავნებით დაირღვეს მისი პირადი ცხოვრების პატივისცემის უფლება.¹³³ სწორედ ამიტომ,

¹²⁷ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „დ“ ქვეპუნქტი.

¹²⁸ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 140; საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაცია უმაღლეს საგანმანათლებლო დაწესებულებებში პერსონალური მონაცემების დამუშავების შესახებ, 2018, 7.

¹²⁹ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 9 მარტის №გ-1/140/2018 გადაწყვეტილება „სსიპ აკაკი წერეთლის სახელმწიფო უნივერსიტეტის შემონმგების დასრულების შესახებ“; საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 7 მარტის №გ-1/136/2018 გადაწყვეტილება „სსიპ საქართველოს ტექნიკური უნივერსიტეტის შემონმგების დასრულების შესახებ“.

¹³⁰ საქართველო საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის გადაწყვეტილება №1/4/693/857 საქმეზე „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“.

¹³¹ საქართველოს საკონსტიტუციო სასამართლოს 2009 წლის 10 ივნისის №1/2/458 განჩინება საქმეზე, „საქართველოს მოქალაქეები – დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ“.

¹³² Verlagsgruppe News GmbH v. Austria, [ECtHR], App. No. 76918/01, 14 December, 2006.

¹³³ Y v. Turkey, [ECtHR], App. no. 648/10, 17 February 2015.

ზოგადი წესის თანახმად, სწორედ მონაცემთა სუბიექტია უფლებამოსილი თავად გადაწყვიტოს, ვის და რა მოცულობით შეიძლება გადაეცეს მისი პერსონალური მონაცემები.¹³⁴ უმაღლესმა საგანმანათლებლო დაწესებულებამ კი მონაცემთა სუბიექტისაგან უნდა მიიღოს თანხმობა ამ მონაცემთა გამჟღავნების თაობაზე, გარდა იმ შემთხვევებისა, თუ არ არსებობს მათი გავრცელების კანონმდებლობით გათვალისწინებული სხვა საფუძველი.¹³⁵ ონლაინ ღონისძიების დროს გადაღებული ფოტო/ვიდეო მასალის გავრცელებისგან განსხვავებით, თანხმობის მიღება არ არის საჭირო, მაგალითად, სტუდენტის პერსონალური მონაცემების სსიპ-განათლების მართვის საინფორმაციო სისტემისთვის გადაცემისას. ვინაიდან, ეს ვალდებულება საგანმანათლებლო დაწესებულებას კანონმდებლობით აქვს დაკისრებული.¹³⁶

პრაქტიკაში ხშირია საგანმანათლებლო დაწესებულებების მიერ სტუდენტთა პერსონალური მონაცემების პოტენციურ დამსაქმებლებისთვის გაზიარების შემთხვევები. აღნიშნული კი შესაძლოა დისტანციური სწავლებისას, შესაბამისი ელექტრონული პლატფორმის მეშვეობითაც ხორციელდებოდეს.¹³⁷ უნდა აღინიშნოს, რომ სტუდენტისაგან თანხმობის არარსებობისას, პერსონალური მონაცემების ამ მიზნით გადაცემა მესამე პირებისთვის არაკანონიერია. ყოველ ადამიანს აქვს მინიჭებული უფლება თავად აირჩიოს შრომითი საქმიანობის ესა თუ ის სფერო¹³⁸ და აირჩიოს სამუშაო რომელსაც შეასრულებს.¹³⁹ შესაბამისად, სტუდენტმა თავად უნდა მიიღოს გადაწყვეტილება სურს თუ არა კონკრეტულ

¹³⁴ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბილისი, 2017, 96.

¹³⁵ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლი.

¹³⁶ „უმაღლესი განათლების შესახებ“ საქართველოს კანონის 862 მუხლის პირველი და მე-2 პუნქტები; „საჯარო სამართლის იურიდიული პირის-განათლების მართვის საინფორმაციო სისტემის შექმნისა და მისი დებულების დამტკიცების შესახებ“ საქართველოს განათლებისა და მეცნიერების მინისტრის 2011 წლის 30 დეკემბრის №229/ნ ბრძანებით დამტკიცებული „საჯარო სამართლის იურიდიული პირის-განათლების მართვისა და საინფორმაციო სისტემის დებულების“ მე-2 მუხლი; საგანმანათლებლო დაწესებულებების რეესტრის წარმოების წესის დამტკიცების შესახებ საქართველოს განათლებისა და მეცნიერების მინისტრის 2011 წლის 22 ივლისის №127/ნ ბრძანებით დამტკიცებული წესის პირველი მუხლის პირველი და მე-2 პუნქტები.

¹³⁷ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 20 აპრილის №1/115/2021 გადაწყვეტილება „სსიპ-ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემომცემების დასრულების შესახებ“

¹³⁸ საქართველოს საკონსტიტუციო სასამართლოს 1998 წლის 3 ნოემბრის №2/80-9 გადაწყვეტილება საქმეზე „ავთანდილ ჭაჭუა საქართველოს პარლამენტის წინააღმდეგ“.

¹³⁹ საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 ოქტომბრის გადაწყვეტილება №2/2-389 საქმეზე „საქართველოს მოქალაქე მაია ნათაძე და სხვები საქართველოს პარლამენტისა და საქართველოს პრეზიდენტის წინააღმდეგ“.

პოტენციურ დამსაქმებელს გაუმჟღავნოს მისი პერსონალური მონაცემები ან გააგრძელოს მასთან ურთიერთობა. მიუხედავად იმისა, რომ დასაქმება სტუდენტისთვის მნიშვნელოვანია და საგანმანათლებლო დაწესებულებასაც შესაძლოა ჰქონდეს ამ საკითხში მისი დახმარების სურვილი, მონაცემთა სუბიექტის ნების გარეშე, პოტენციური დამსაქმებლისთვის, სტუდენტის პერსონალური მონაცემების (რეზიუმეს ან სხვაგვარი ინფორმაციის) გაზიარება დაუშვებელია. შესაბამისად, ასეთი საფუძვლის არარსებობის შემთხვევაში მონაცემების გამჟღავნება ჩაითვლება უკანონოდ.

საინტერესოა იმის გამორკვევაც, რამდენად საჭიროა ყოველი ახალი პოტენციური დასაქმებულისთვის ინფორმაციის გაზიარების შემთხვევაში, სტუდენტისაგან თანხმობის მიღება. აღნიშნულ საკითხზე Deutsche Telekom AG მართლმსაჯულების ევროპული სასამართლოს მსჯელობაზე დაყრდნობით,¹⁴⁰ შესაძლებელია გამოვყოთ ორი შემთხვევა. პირველი, თუ სტუდენტმა თანხმობა განაცხადა მხოლოდ დამუშავების მიზნებზე, რაც გულისხმობს მათი მონაცემების ნებისმიერი პოტენციური დამსაქმებლისათვის გადაცემას და არ ყოფილა დაკონკრეტებული რომელიმე კონკრეტული დაწესებულება, მაშინ სტუდენტის მიერ თანხმობის მიღება ყოველი ახალი შემთხვევისთვის არ არის აუცილებელი. მაგრამ, თუ უნივერსიტეტმა თანხმობა მოითხოვა კონკრეტული დამსაქმებლისათვის ინფორმაციის მიწოდებაზე, მაშინ ყოველი ახალი სუბიექტისთვის მონაცემების გამჟღავნების შემთხვევაში აუცილებელი იქნება სტუდენტისგან თანხმობის მოპოვება. საინტერესო იქნება, თუ აღნიშნულ საკითხზე მსჯელობას განვაზოგადებთ ლექციების აუდიო-ვიდეო ჩანერის განხორციელების შემთხვევაზეც. შედეგად, თუ საგანმანათლებლო დაწესებულება შეიმუშავებს შესაბამის ფორმას და მიიღებს სტუდენტთა ზოგად, „გენერალურ თანხმობას“ დისტანციური სწავლებისას მიმდინარე ლექციების ჩანერაზე, მაშინ აღარ იქნება საჭირო ყოველი შეხვედრის აუდიო/ვიდეო ჩანერის დაწყების წინ მიიღოს ლექციაზე დამსწრე ყველა პირისგან ახალი თანხმობა ასეთი ჩანანერის გაკეთებასა და მის ხელმისაწვდომობასთან დაკავშირებით.

1.2. კანონიერი ძალის მქონე თანხმობის კრიტერიუმები

იმისათვის, რომ სტუდენტების მიერ გამოხატული თანხმობა ჩაითვალოს კანონიერი ძალის მქონედ, საჭიროა იგი რამდენიმე კრიტერიუმს აკმაყოფილებდეს.

მნიშვნელოვანია, თანხმობა იყოს პირის მიერ ნებაყოფლობითი გამოხატული, მის მიერ გამიზნულად გაკეთებული არჩევანის მიხედვით.¹⁴¹ ასეთი არჩევა-

¹⁴⁰ Deutsche Telekom AG v Bundesrepublik Deutschland, [CJEU], C-543/09, 5 May 2011.

¹⁴¹ Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement

ნის შესაძლებლობა პირს ექნება მაშინ, თუ არ იარსებებს მისი მოტყუების, დაშინების ან იძულების რაიმე უარყოფითი საფრთხე იმ შემთხვევებისთვის, თუ იგი უარს იტყვის პერსონალური მონაცემების გაცემაზე.¹⁴² ამასთანავე, დადგენილია, რომ ნებაყოფლობითი თანხმობა საეჭვოა, იმ შემთხვევაში, თუ მონაცემთა დამამუშავებელსა და მონაცემთა სუბიექტს შორის მნიშვნელოვანი ეკონომიკური ან სხვა სახის დისბალანსია.¹⁴³ მართალია, ხშირად ამ შემთხვევაში დამსაქმებლის და დასაქმებულის მაგალითი განიხილება,¹⁴⁴ თუმცა ძალაუფლების დისბალანსზე მსჯელობა შესაძლებელია სტუდენტსა და უნივერსიტეტს შორის არსებული ურთიერთობის შემთხვევაშიც. საგანმანათლებლო დაწესებულებას, მართალია არაკანონიერად, თუმცა, შეუძლია, რომ მონაცემთა სუბიექტზე (სტუდენტზე) გარკვეული ტიპის არასათანადო გავლენა ან ზეწოლა მოახდინოს. აღნიშნული ირიბადაც დასაშვებია,¹⁴⁵ რითაც სტუდენტი პრაქტიკულად იძულებული იქნება დათანხმდეს მისი პერსონალური მონაცემების გამჟღავნებას. დაუშვებელია, უნივერსიტეტმა სტუდენტს დაუდგინოს, რომ დისტანციური სწავლისას ლექციების, სემინარების ან/და პრეზენტაციის მიმდინარეობისას ვიდეოკამერის ჩაერთვებლობის შემთხვევაში მას შეფასება არ დაენერება. მოცემულ შემთხვევაში, უნივერსიტეტი სტუდენტს არ უტოვებს რეალური და ნებაყოფლობითი არჩევანის უფლებას. ასევე, ვიდეოკამერის ჩართვაზე უარის შედეგები სტუდენტისთვის შესაძლოა საკმაოდ მძიმე იყოს, ვინაიდან შეფასებების მიუღებლობით იგი წარმატებით ვერ დაასრულებს საგანს და შეიძლება შეექმნას პრობლემები სწავლების გაგრძელება/დასრულებასთან მიმართებით. აღნიშნული ქმედებით, საგანმანათლებლო დაწესებულება ირიბად აძლევს სტუდენტს, გამოხატოს თანხმობა ისეთი პერსონალური მონაცემების დამუშავებაზე, როგორიცაა მისი სახის გამოსახულება, ხმა და ქცევითი მახასიათებლები.

აუცილებელია, თანხმობის მიღებამდე, საგანმანათლებლო დაწესებულებამ სტუდენტს მისთვის გასაგებ ენაზე მიაწოდოს, ნათელი, ცალსახა და ამომწურავი ინფორმაცია პერსონალური მონაცემების დამუშავების თაობაზე.¹⁴⁶ შესაბამისად,

of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016, Art. 4 para. 11; „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ზ“ ქვეპუნქტი; Van Casteren D.C.J., Consent now and then; Tilburg, 2017, 22-23.

¹⁴² Article 29 Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017, 7.

¹⁴³ იქვე, 6.

¹⁴⁴ იქვე, 7.

¹⁴⁵ European Data Protection Board (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679, 2020, 8-9.

¹⁴⁶ Article 29 Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017, 12-15; Van Casteren D.C.J., Consent now and then; Tilburg, 2017, 23-24; საქა-

სტუდენტი წინასწარ უნდა იყოს ინფორმირებული ყველა სახის პერსონალური მონაცემის დამუშავების შესახებ, მათი დამუშავების მიზნებზე, სამართლებრივ საფუძვლებზე, შენახვის ვადებზე და მხოლოდ ამ ინფორმაციის მიღების შემდეგ უნდა გამოხატოს თანხმობა საკუთარი პერსონალური მონაცემის დამუშავებაზე. ამასთან, თანხმობა საჭიროა თითოეულ მონაცემთან და მონაცემთა დამუშავების თითოეულ მიზანთან მიმართებით.¹⁴⁷

განსაკუთრებული კატეგორიის მონაცემების დამუშავების გარდა,¹⁴⁸ მონაცემთა დამუშავებისას სტუდენტისაგან წერილობითი თანხმობის მიღება აუცილებელი არ არის.¹⁴⁹ საქართველოს კანონმდებლობით თანხმობა უნდა იყოს ნათელი,¹⁵⁰ რაც შეიძლება გამოიხატოს წერილობით, ზეპირსიტყვიერად ან კონკლუდენტური ქმედებით¹⁵¹. ჩვენს ქვეყანაში არსებული მიდგომით, დისტანციური სწავლებისას მიმდინარე ლექცია/სემინარებისა და გამოცდების აუდიო-ვიდეო ჩანერისას, სტუდენტის თანხმობის მიღების ფორმა უმოქმედობით-თანხმობის არ გამოხატვითაც დასაშვებია.¹⁵² მართალია, საქართველოს კანონმდებლობა არ ავალდებულებს საგანმანათლებლო დაწესებულებას პერსონალური მონაცემის დამუშავებაზე თანხმობა აუცილებლად აქტიური ქმედებით მოიპოვოს, თუმცა უმჯობესი იქნება ამ მიმართულებით ევროპის ქვეყნებში გავრცელებული მეტად მაღალი სტანდარტის გათვალისწინება. კერძოდ, დადგენილია, რომ იგი უნდა იყოს მკაფიოდ გამოხატული¹⁵³ და დუმილი ან უმოქმედობა არ შეიძლება ჩაითვალოს ასეთ თანხმობად.¹⁵⁴ შეხვედრის აუდიო/ვიდეო ჩანერაზე ყველა მონაწილის

რთველოს სახელმწიფო ინსპექტორის 2021 წლის 20 აპრილის № 1/115/2021 გადაწყვეტილება „სსიპ-ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

¹⁴⁷ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ, თბილისი, 2018, 8.

¹⁴⁸ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის პირველი პუნქტი.

¹⁴⁹ იქვე, მე-2 მუხლის „ზ“ და „თ“ ქვეპუნქტები.

¹⁵⁰ იქვე.

¹⁵¹ საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2021 წლის 27 მაისის განჩინება №ბს-962(კ-19).

¹⁵² ჯორბენაძე ს., Covid-19 და პერსონალურ მონაცემთა დაცვა „Zoom-ის“ გამოყენებით დისტანციური სწავლებისას, „შედარებითი სამართლის ქართულ-გერმანული ჟურნალი“, №5, 2020, 47; საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 8 ივლისის №გ-1/231/2020 გადაწყვეტილება „განცხადების განხილვის დასრულების შესახებ“.

¹⁵³ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 169.

¹⁵⁴ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, preamble, para. 32.

დათანხმების აუცილებლობა კალიფორნიისა და ფლორიდის შტატებისთვისაც არ არის უცხო, მაშინ, როდესაც ასეთი გაფრთხილების შემდეგ ჩანერის დაწყებას დასაშვებად მიიჩნევენ ჩრდილოეთ კაროლინის შტატი.¹⁵⁵ განსხვავებული პრაქტიკის მიუხედავად, მონაცემთა სუბიექტის თანხმობის აქტიური ქმედებით გამოხატვა გააუმჯობესებს დისტანციური სწავლებისას პერსონალური მონაცემების დამუშავების სტანდარტს. იმ შემთხვევაში, როდესაც სტუდენტებისგან თანხმობის მისაღებად ინფორმაცია და შეკითხვა ერთდროულად სხვა საკითხებთან ერთად ეძლევათ, არსებობს შანსი იმისა, რომ მათ ვერ მოახერხონ ერთმანეთისაგან ინფორმაციული და თანხმობის გამომხატველი საკითხების გამიჯვნა. ამ შემთხვევაში კი თავიანთი უმოქმედობით, გაუთვითცნობიერებლად, გასცენ თანხმობა პერსონალური მონაცემის დამუშავებაზე, ისე რომ არც ჰქონდეთ რეალური წარმოდგენა ამ საკითხზე და მის შედეგებთან მიმართებით. დისტანციური სწავლებისას, მათ შორის, ლექციების ჩანერის განსახორციელებლად, პერსონალური მონაცემების დამუშავებაზე აქტიური ქმედებით დასტურის მოთხოვნისას, ეს რისკები მინიმუმამდე მცირდება. რა თქმა უნდა, აქტიური ქმედების დროს არ უნდა მოვიზნოთ, რომ ყველა სტუდენტი სათითაოდ, ლექციის მიმდინარეობისას დააფიქსირებს თავის პოზიციას. აღნიშნული განსაკუთრებით დიდ დროსთან იქნება დაკავშირებული, განსაკუთრებით მრავალრიცხოვანი აუდიტორიების შემთხვევაში. მსგავსი შედეგის მიღწევა შესაძლებელია, წინასწარ წერილობით დოკუმენტზე ხელისმონერით, ელექტრონულ პლატფორმაზე თავისი აზრის დაფიქსირებით, შეხვედრაზე დასასწრებად ინფორმაციის მიწოდებით, დათანხმების ფუნქციის ლილაკზე აღნიშვნით და სხვა გზების მეშვეობით. აღსანიშნავია ისიც, რომ დავის წარმოშობის შემთხვევაში სწორედ საგანმანათლებლო დაწესებულებას ეკისრება მონაცემთა სუბიექტის თანხმობის ფაქტის არსებობის მტკიცების ტვირთი.¹⁵⁶ შესაბამისად, წინასწარ წერილობით ან სხვა აქტიური ქმედებით გამოხატული თანხმობის შემთხვევაში, კონფლიქტის ან უთანხმოების არსებობის დროს, თანხმობა აღრიცხული ექნება ისე, რომ მარტივად მოხდეს მისი გადამოწმება.¹⁵⁷ ასეთ დროს მონაცემთა დამუშავებელი არ იქნება დამოკიდებული ფაქტობრივი გარემოებების გახსენებაზე და მათ დასამტკიცებლად შესაბამისი მტკიცებულებების მოპოვებაზე.

აღსანიშნავია ისიც, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ახალი პროექტით, იყო დაზუსტებული პერსონალურ მონა-

¹⁵⁵ <<https://bit.ly/3NFfpI9>> [22.06.2022].

¹⁵⁶ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 26-ე მუხლის მე-4 პუნქტი.

¹⁵⁷ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 162.

ცემთა დამუშავებისთვის მონაცემთა სუბიექტის თანხმობის მიღების წესი და კრიტერიუმები. ამ კანონპროექტით, სუბიექტის თანხმობად ჩაითვლება აქტიური მოქმედებით, წერილობით (მათ შორის ელექტრონულად), ან ზეპირად, თავისუფლად და ნათლად გამოხატული ნება.¹⁵⁸ ადრე თუ გვიან, კანონმდებლობაში ცვლილებების შეტანის შემთხვევაში, საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებებს დადგენილი პრაქტიკის შეცვლა აუცილებლად მოუწევთ.

ზოგადად, პერსონალურ მონაცემთა დამუშავებაზე თანხმობის მიღებად შესაძლოა ჩაითვალოს უნივერსიტეტისა და სტუდენტის შორის გაფორმებული ხელშეკრულება, თუ მასში არსებული ჩანაწერები მოიცავს შესაბამის დებულებებს.¹⁵⁹ ამ შემთხვევაში, ხელშეკრულებაზე ხელის მოწერით სტუდენტი აფიქსირებს თავის თანხმობას კონკრეტული მონაცემების დამუშავებაზე. თუმცა, გასათვალისწინებელია ისიც, რომ ასეთ დროს ხელშეკრულებაში მოცემული დებულებები იყოს მკაფიოდ ჩამოყალიბებული, დაწერილი გასაგები ენით, სხვა საკითხებისგან იყოს მარტივად გამორჩევადი და ადვილად აღქმადი.

გარდა ზემოაღნიშნულისა, საგანმანათლებლო დაწესებულებებმა თანხმობის მისაღებად შეიძლება გამოიყენონ ტექნოლოგიური შესაძლებლობები და შეტყობინება სტუდენტებს მიაწოდონ ელექტრონული პლატფორმის მეშვეობით. ამ შემთხვევაში თანხმობად ჩაითვლება მონაცემთა სუბიექტის მხრიდან ინდივიდუალურად და არაავტომატურად თანხმობის გრაფის მონიშვნა/დათანხმება. ასეთი შეტყობინებები უნდა აკმაყოფილებდნენ თანხმობის მიღებისთვის საჭირო ყველა კრიტერიუმს. მათ შორის, ტექსტი უნდა იყოს მკაფიო, გასაგები და ამომწურავი. ხოლო რამდენიმე მონაცემის დამუშავების მოთხოვნის არსებობის შემთხვევაში, პროგრამულადვე იყოს შესაძლებელი თითოეულ მონაცემთან მიმართებით სტუდენტის ნების გამოვლენა.¹⁶⁰

1.3. გაცემული თანხმობის გამოსვლის შესაძლებლობა

ევროპული მიდგომის თანახმად, თანხმობა რომ დასაბუთებულად ჩაითვალოს, მონაცემთა სუბიექტს მისი გამოთხოვის შესაძლებლობაც უნდა გააჩნდეს.¹⁶¹

¹⁵⁸ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 2019 წლის 27 მაისის პროექტის მე-3 მუხლის „მ“ ქვეპუნქტი.

¹⁵⁹ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 8 ივლისის №გ-1/231/2020 გადაწყვეტილება „განცხადების განხილვის დასრულების შესახებ“.

¹⁶⁰ International Association of Privacy Professionals, The UX Guide to Getting Consent, 2017, 3-6; Niemann J. T., Consent as an Appropriate Legal Ground for Processing in the Digital Environment, Analysis Under the Scope of the European General Data Protection Regulation, Edinburgh Student Law Review, 2020, იხ., <<https://bit.ly/3lgz3mC>> [19.06.2022].

¹⁶¹ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 129.

მსგავს შესაძლებლობას საქართველოს კანონმდებლობაც ითვალისწინებს. მონაცემთა სუბიექტს ნებისმიერ დროს, განმარტებების გარეშე, შეუძლია გამოიხმოს თანხმობა მისი პერსონალური მონაცემების დამუშავებასთან მიმართებით.¹⁶² კანონმდებლობით დადგენილი ნორმის საფუძველზე, სტუდენტს ამ უფლების რეალიზება უნდა შეეძლოს ნებისმიერ დროს და საკუთარი შეხედულებისამებრ. ამ შემთხვევაში, უნივერსიტეტი არ არის უფლებამოსილი მოსთხოვოს სტუდენტს ახსნა-განმარტება მის მიერ მიღებულ გადაწყვეტილებაზე. ამასთან, ის უნდა იყოს ისეთივე ადვილი, როგორც მისი გამოხატვა.¹⁶³ ძირითად შემთხვევებში, თანხმობის გამოთხოვა ამ მონაცემთა სამომავლო დამუშავების პრევენციას უზრუნველყოფს.¹⁶⁴ საქართველოსგან განსხვავებით, შესაძლოა ქვეყნის კანონმდებლობა თანხმობის გამოხმობაზე უკუძალის წესის გავრცელებასაც ითვალისწინებდეს.¹⁶⁵ თუმცა, მსგავსი მიდგომა, სტუდენტთა პერსონალური მონაცემების განადგურებისას საკმაოდ ფრთხილ მიდგომას საჭიროებს, რათა ამ ქმედებით, არა მხოლოდ მესამე პირებს, არამედ თავად მონაცემთა სუბიექტის ინტერესებსაც არ მიაღვეთ ზიანი.

მიუხედავად კანონმდებლობით დადგენილი თანხმობის გამოთხოვის შესახებ ნორმისა, ამ უფლების პრაქტიკული რეალიზება დისტანციური სწავლების პროცესში საქართველოში ნაკლებად არის შესაძლებელი.¹⁶⁶ კერძოდ, დისტანციური სწავლების პროცესში ლექცია-სემინარების აუდიო-ვიდეო ჩანერაზე ერთ-ერთმა სტუდენტმა გარკვეული პერიოდის შემდეგ განაცხადა უარი და მოითხოვა მსგავსი ქმედებების შეწყვეტა, გარდა კანონმდებლობით დადგენილი აუცილებელი შემთხვევებისა. მიუხედავად თანხმობის გამოხმობისა, უნივერსიტეტის მიერ ლექციების აუდიო/ვიდეო ჩანერა მაინც გაგრძელდა და სტუდენტს უარი ეთქვა იმ შესაძლებლობაზე, რომ ჩანერა მისი მონაცემების დაშიფვრის გზით გაგრძელებულიყო ან სხვაგვარად არ მომხდარიყო მონაცემების დამუშავება. უნივერსიტეტის ადმინისტრაციის უარი პერსონალურ მონაცემთა დაცვის სამსახურმაც სამართლიანად ცნო და აღნიშნა, რომ ვინაიდან უნივერსიტეტში საკმაოდ ბევრი სტუდენტი სწავლობდა, გაუმართლებელი იქნებოდა მონაცემების დაშიფვრის მოთხოვნა. ამასთან, ჩანერის განხორციელება მიიჩ-

¹⁶² „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 25-ე მუხლი.

¹⁶³ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, preamble, para. 42.

¹⁶⁴ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 171.

¹⁶⁵ Personal Data Protection Act of Estonia, article 12, para. 7.

¹⁶⁶ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 17 აგვისტოს №გ-1/272/2020 გადაწყვეტილება „განცხადების განხილვის დასრულების შესახებ“.

ნიეს კანონიერად მისი სიახლიდან და სხვა პირის ინტერესებიდან გამომდინარე.¹⁶⁷ შესაბამისად, გამოდის, სტუდენტის მიერ თანხმობაც, მასზე უარიც და მისი გამოთხოვაც ფორმალურ ხასიათს ატარებს და არ იწვევს რაიმე შედეგს. ნებისმიერ შემთხვევაში, მნიშვნელოვანია, რომ პერსონალურ მონაცემთა დამუშავებისას სამართლიანი ბალანსი იქნეს დაცული მონაცემთა დამუშავების კანონიერ ინტერესებს და მონაცემთა სუბიექტის პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის უფლებას შორის. ეს ვალდებულება ნარჩუნდება იმ შემთხვევაშიც კი, როდესაც სახეზეა კანონით გათვალისწინებული მონაცემთა დამუშავების რომელიმე საფუძველი.¹⁶⁸ შესაბამისად, ერთი პირის კანონიერი უფლება გამოითხოვოს თავის თანხმობა, არ დაუშვას მისი პერსონალური მონაცემების დამუშავება, როდესაც მათი არდამუშავება უარყოფით ზეგავლენასაც არ მოახდენს სასწავლო პროცესზე და სხვა პირის ინტერესებზე, არ უნდა იქნეს უგულებელყოფილი. გასათვალისწინებელია ის ფაქტიც, რამდენად არის შესაძლებელი, ტექნიკური საშუალებებიდან გამომდინარე, ლექციების აუდიო-ვიდეო მონიტორინგი განხორციელდეს მხოლოდ თანხმობის გამცემი სტუდენტების მიმართ, იმგვარად, რომ მონიტორინგის ქვეშ არ მოექცეს გაცემულ თანხმობაზე უარის განმცხადებელი სტუდენტი. თუმცა, ასეთ შემთხვევებში, იმისათვის, რომ მონაცემთა სუბიექტის უფლებებისა კანონიერი საფუძვლების გარეშე შეზღუდვა არ მოხდეს, შესაძლებელია აშშ-ში ფართოდ დანერგილი პრაქტიკის ჩამოყალიბება. კერძოდ, განმცხადებელი პირის თანხმობაზე უარის დეპერსონალიზაციის ან სხვა გზით დაშიფვრა უკვე არსებულ ჩანაწერზე.¹⁶⁹ ამასთანავე, მითითება უბრალოდ დიდი რაოდენობით სტუდენტებისა და საგნების რაოდენობაზე არარელევანტურია მაშინ, როდესაც მეორე მხარეს ადამიანის პირადი ცხოვრების ხელშეუხებლობის უფლება დგას. გარდა ამისა, აშშ-ს უნივერსიტეტებში, რომლებშიც ზოგიერთ ქართულ უნივერსიტეტზე ბევრად მეტი სტუდენტია, ზემოაღნიშნული მიდგომაა დამკვიდრებული, რითაც უზრუნველყოფენ სტუდენტს პერსონალური მონაცემების დაცვის მაღალი სტანდარტის დანერგვას.

¹⁶⁷ იქვე.

¹⁶⁸ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის №გ-1/043/2015 გადანაცვლებულია შპს „ა“-ს შემონგების დასრულების შესახებ.

¹⁶⁹ University Of Miami, <<https://bit.ly/3nV7iqp>> [25.06.2022]; Loyola University Chicago, <<https://bit.ly/3bOoefk>> [25.06.2022]; The University of Maryland, <<https://bit.ly/3bNatZk>> [25.06.2022].

2. დისტანციური სწავლების პროცესში დამუშავებული პერსონალური მონაცემების შენახვა

2.1. მონაცემთა შენახვის ვადა

მონაცემთა დამუშავებისთვის კანონით გათვალისწინებული საფუძვლის არსებობა, ავტომატურად არ აქცევს მონაცემთა დამუშავების მთლიან პროცესს კანონიერად. აუცილებელია, რომ მონაცემთა დამუშავებელმა განუხრელად დაიცვას მათი დამუშავებისთვის დადგენილი პრინციპებიც.¹⁷⁰

პერსონალურ მონაცემთა დაცვის კანონმდებლობა მინიმიზაციის პრინციპთან ერთად,¹⁷¹ რომელიც მონაცემთა დამუშავებისა და შენახვისთვის აუცილებელი მიზნების არსებობას მოიცავს, ადგენს შენახვის ვადის შეზღუდვის პრინციპსაც.¹⁷² კანონმდებლობის ნორმები არ განსაზღვრავენ დამუშავებული მონაცემების შენახვის ზუსტ, კონკრეტულ ვადას და დისკრეციას მონაცემთა დამუშავებელს ანიჭებენ.¹⁷³ დადგენილია, რომ დამუშავებული მონაცემები, მათი დამუშავების მიზნის მისაღწევად აუცილებელი ვადით უნდა იქნეს შენახული, რის შემდეგაც ისინი უნდა დაიბლოკოს, წაიშალოს, განადგურდეს ან შენახულ უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით.¹⁷⁴ დაუშვებელია, რომ უმაღლესმა საგანმანათლებლო დანესებულებებმა დაამუშაონ და შეინახონ მონაცემები მხოლოდ იმ მიზნით რომ მომავალში ისინი შეიძლება სასარგებლო და გამოსადეგი აღმოჩნდეს.¹⁷⁵ ამასთანავე, კანონდარღვევად ითვლება მონაცემთა შეუზღუდავი დროით დამუშავებაც.¹⁷⁶ პერსონალური მონაცემების

¹⁷⁰ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 10 ივლისის №1/234/2020 გადაწყვეტილება „სსიპ-სოხუმის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

¹⁷¹ Neves A., Protection of Personal Data Regulation and Public Liberties: A Polyhedron With Unexpected Effects, in the book: Personal data protection and legal developments in the European Union, edited by Tzanou M., Hershey PA, 2020, 4.

¹⁷² Georgiou E., GDPR in Between Profiles and Decision-Making: How the General Data Protection Principles Under Article 5 GDPR Are Engaged with Profiling, in the book: Personal data protection and legal developments in the European Union, edited by Tzanou M., Hershey PA, Hershey PA, 2020, 96.

¹⁷³ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Art. 5 para.1; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Article 5 para. 4E; „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „ე“ ქვეპუნქტი.

¹⁷⁴ იქვე.

¹⁷⁵ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 140.

¹⁷⁶ იქვე.

გაუმართლებლად ხანგრძლივი დროის განმავლობაში შენახვის თავიდან ასაცილებლად მნიშვნელოვანია, საგანმანათლებლო დაწესებულებებს წინასწარ ჰქონდეთ განსაზღვრული მონაცემთა შესაბამისი სახეების შენახვისთვის საჭირო და პროპორციული ვადები.

უმალესი საგანმანათლებლო დაწესებულებები საკმაოდ დიდი რაოდენობით პერსონალურ მონაცემებს ამუშავებენ როგორც დისტანციური, ასევე, არადისტანციური სწავლების მიმდინარეობისას.¹⁷⁷ წარმოუდგენელია, საკანონმდებლო დონეზე განისაზღვროს თითოეული მონაცემის სახეობის შენახვის ოპტიმალური ვადა. მონაცემთა დამუშავებელს შეუძლია თავად შეაფასოს მონაცემის დამუშავების მიზანი და ამ მიზნის მიღწევისთვის მათი შენახვის პერიოდი. მაგალითისთვის, უმაღლესი საგანმანათლებლო დაწესებულება ვალდებულია კონკრეტულ საგანმანათლებლო პროგრამაზე სწავლის გაგრძელების მსურველთათვის დაანესოს გამოცდა შესაბამის სპეციალობაში¹⁷⁸ და უფლება-მოსილია, დაანესოს დამატებითი გამოცდები სხვა საგნებშიც.¹⁷⁹ გამოცდაზე მიღებული შედეგები კი უნივერსიტეტების ოფიციალურ საიტებზე ქვეყნდება.¹⁸⁰ ამ მონაცემების დამუშავებისა და ვებ-გვერდზე განთავსების ვადა შეზღუდული უნდა იყოს უმაღლეს საგანმანათლებლო დაწესებულებაში სწავლის გაგრძელების შესახებ გადაწყვეტილების მიღებისათვის დადგენილი ვადის დროით, რომელიც განსხვავებული იქნება ყველა დაწესებულებაში. ასევე, განსხვავებული შენახვის ვადა უნდა იყოს დადგენილი სტუდენტის ფინანსური დავალიანების შესახებ ინფორმაციის, როგორც მისი პერსონალური მონაცემის¹⁸¹ დამუშავებისა და შენახვისას. ფინანსური დავალიანების დაფარვისა და ბალანსის გასწორების შემდეგ, ინფორმაცია დავალიანების შესახებ უნდა წაიშალოს, თუ კანონმდებლობით სხვა რამ არ არის განსაზღვრული.

¹⁷⁷ Borgman, C. L., Open data, grey data, and stewardship: universities at the privacy frontier, *Berkeley Technology Law Journal*, Vol. 33(2), 2018, 368.

¹⁷⁸ „სამაგისტრო გამოცდების ჩატარების დებულებისა და სახელმწიფო სასწავლო სამაგისტრო გრანტის განაწილების წესის დამტკიცების შესახებ“ საქართველოს განათლებისა და მეცნიერების მინისტრის 2009 წლის 22 აპრილის №227 ბრძანებით დამტკიცებული სამაგისტრო გამოცდების ჩატარების დებულების მე-5 მუხლის მერვე პუნქტი.

¹⁷⁹ იქვე, მეცხრე პუნქტი.

¹⁸⁰ სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 10 აგვისტოს №1/266/2020 გადაწყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“, სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 31 ივლისის №1/253/2020 გადაწყვეტილება „სსიპ – ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

¹⁸¹ სახელმწიფო ინსპექტორის სამსახურის 2018 წლის 7 მარტის №1/136/2018 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემონმების დასრულების შესახებ“.

აღსანიშნავია ისიც, რომ პერსონალურ მონაცემთა დაცვის სამსახურის განმარტებით, კურსდამთავრებულის სტატუსის მინიჭების, ან/და სტუდენტის სტატუსის შეწყვეტის შემდეგ, შესაძლოა აღარ იყოს საჭირო კურსდამთავრებულის ან/და შეწყვეტილი სტატუსის მქონე სტუდენტის პერსონალური მონაცემების იმავე მოცულობით და ფორმით დამუშავება, როგორც ეს აქტიური ან/და შეჩერებული სტატუსის მქონე პირის შემთხვევაშია.¹⁸² მაგალითად, აღარ იყოს საჭირო ლექციაზე დასწრების მონაცემების ან ცალკეულად დავალებებსა და გამოცდებში მიღებული ქულების შენახვა და სხვა.

გარდა ზემოაღნიშნულისა, განსხვავებული მიზანი აქვს დისტანციური სწავლებისას შესრულებული დავალებებისა და საგამოცდო ნაშრომების დამუშავებას. მათი დანიშნულება სტუდენტის ცოდნის შემოწმებაა, რაშიც მას შესაბამისი შეფასება ეწერება. ამ პერსონალური ინფორმაციის შენახვის საჭიროება დამუშავებისთვის არსებული მიზნის მიღწევის შემდეგ აღარ იარსებებს და უნდა წაიშალოს.¹⁸³ კერძოდ, ისინი უნდა წაიშალოს ელექტრონული ბაზიდან ან ლექტორის ელექტრონული ფოსტიდან დავალების/გამოცდის შესწორების, ქულის ელექტრონულ ჟურნალში ასახვისა და დაწერილი შეფასების გასაჩივრების ვადის ამოწურვის შემდეგ. ეს ვადები თითოეულ უმაღლეს საგანმანათლებლო დაწესებულებაში შიდა ორგანიზაციული დოკუმენტებით უნდა რეგულირდებოდეს.¹⁸⁴

ასევე, განსხვავებული შენახვის ვადა უნდა იყოს დადგენილი სტუდენტის ხმისა და ვიზუალური გამოსახულების დამუშავებისას. ეს მონაცემები უმეტესწილად დისტანციური სწავლებისას მუშავდება, ლექციების ან/და გამოცდების ჩანერით. ამასთან, ვინაიდან, სინქრონულ რეჟიმში მიმდინარე ლექციების ჩანერა ემსახურება ლექტორის მიერ ახსნილი მასალის სტუდენტებისთვის ხელმისაწვდომობისა და მათთვის კურსის განმავლობაში ცოდნის გაზიარების მიზანს,¹⁸⁵ ისინი სტუდენტისთვის სასწავლო კურსის ხანგრძლივობის პერიოდით უნდა იყოს ხელმისაწვდომი. მიზნის მიღწევის შემდეგ, კი ეს ჩანაწერები უნდა წაიშალოს. წინააღმდეგ შემთხვევაში დარღვეული იქნება მონაცემთა კანონიერად დამუშავების საფუძვლები.¹⁸⁶ რაც შეეხება საგამოცდო პროცესის აუდიო-ვიდეო ჩანაწერე-

¹⁸² შპს „იუაი“ – ჩანტლაძე ტ., სულხანიშვილი ე., ცინცვილაძე გ., ჯიშიაშვილი გ., თემატური რეკომენდაციები COVID 19 პანდემიის დროს პერსონალური მონაცემების მართვაზე, ანგარიში დისტანციური სწავლებისას პერსონალურ მონაცემთა დაცვის შესახებ, 2021, 28.

¹⁸³ იქვე, 37.

¹⁸⁴ იქვე, 48.

¹⁸⁵ Makarem S. C., Using Online Video Lectures to Enrich Traditional Face-to-Face Courses, *International Journal of Instruction*, Vol. 8, No.2, 2015, 156-159.

¹⁸⁶ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 25 მაისის №გ-1/286/2017 გადაწყვეტილება, „შპს „ა“-ს შემოწმების დასრულების შესახებ“.

ბს, აქაც მნიშვნელოვანია, მონაცემები ინახებოდეს მათი შემოწმების, ქულების შეტანის და გასაჩივრებისთვის დადგენილი ვადის განმავლობაში.

საქართველოში სკოლის მოსწავლეებისთვის პირადი საქმეების შენახვის მაქსიმალურ ვადად 74 წელია განსაზღვრული.¹⁸⁷ თუმცა, უნივერსიტეტმა ამ ვადის გამოყენების შემთხვევაშიც უნდა განსაზღვროს და მიუთითოს სტუდენტის ვინაობის, ჩაბარების და გამოშვების წელის, ასევე მინიჭებული ხარისხის შესახებ მონაცემების შენახვის მიზანი. ხოლო, სხვა ტიპის პერსონალური მონაცემები უმჯობესია შედარებით უფრო მოკლე პერიოდის განმავლობაში ინახებოდეს, მაგალითად, ინგლისში ასეთად 6 წელია მიჩნეული¹⁸⁸.

ზემოაღნიშნულიდან გამომდინარე, ცხადია, რომ თითოეული მონაცემის დამუშავებას განსხვავებული მიზანი აქვს. შესაბამისად, უნივერსიტეტმა წინასწარ უნდა განსაზღვროს შიდა ორგანიზაციული აქტით ამ მონაცემთა დამუშავების მიზანი და შენახვის ვადაც თითოეულ პერსონალურ მონაცემთან ან მონაცემთა ჯგუფთან მიმართებით.¹⁸⁹ ის, რომ მონაცემთა დამუშავების ვალდებულებას წარმოადგენს სტუდენტის პერსონალური მონაცემების შენახვის ვადის განსაზღვრა, დადგენილია არა მხოლოდ საქართველოსა და ევროკავშირის კანონმდებლობით, არამედ, ეს წესი მოქმედებს ამერიკის შეერთებულ შტატებშიც.¹⁹⁰

აღსანიშნავია ისიც, რომ დაუშვებელია სტუდენტის საქმეების ან/და ელექტრონულ პლატფორმაში ასახული პერსონალური მონაცემების შეუზღუდავად, უვადოდ შენახვა.¹⁹¹ ამასთან, არ აქვს მნიშვნელობა გამოიყენებს თუ არა მონაცემთა დამუშავებელი პირის პერსონალურ მონაცემებს მისი დამუშავების მიზნის მისაღწევად მიჩნეული გონივრული ვადის შემდეგ. მიჩნეულია, რომ მათი შენახვა გავლენას ახდენს ინდივიდის პირადი ცხოვრების ინტერესებზე.¹⁹² პირის

¹⁸⁷ საქართველოს განათლებისა და მეცნიერების მინისტრის 2013 წლის 22 აგვისტოს №113/6 ბრძანება „მოსწავლის პირადი საქმის ფორმისა და ზოგადსაგანმანათლებლო დაწესებულებაში მოსწავლის პირადი საქმის წარმოების წესის დამტკიცების თაობაზე“, დანართი 1, მუხლი 2(6)

¹⁸⁸ For how long will the University keep my personal data? University of Portsmouth, <<https://bit.ly/3NFE8pE>> [20.06.2022]; The University of Manchester, <<https://bit.ly/3bODfO0>> [20.06.2022]; Data Retention Periods, The University of Edinburgh, <<https://bit.ly/3bRQkq9>> [20.06.2022].

¹⁸⁹ Record Retention Table, Boston University, <<https://bit.ly/3ycnx73>> [20.06.2022]; Data Retention Periods, The University of Edinburgh, <<https://bit.ly/3bRQkq9>> [20.06.2022]; RM Framework Guidance Document: Student Records Storage and Retention, The University of Nottingham, <<https://bit.ly/3bODxV6>> [20.06.2022].

¹⁹⁰ C., Privacy Considerations in Higher Education Online Learning, Washington, 2020, 8.

¹⁹¹ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 140.

¹⁹² S. and Marper v. the United Kingdom, [ECtHR], Apps. nos. 30562/04 and 30566/04, 4 December 2008, par. 121.

პერსონალური მონაცემების შემცველი ინფორმაციის ბლანკეტურად, მუდმივი შენახვა არ წარმოადგენს მითითებული ლეგიტიმური მიზნის მიღწევის აუცილებელ საშუალებას.¹⁹³ განსაკუთრებით ხანგრძლივი დროით პირის პერსონალური მონაცემების დამუშავება, საქმეში წარმოდგენილი ფაქტობრივი გარემოებების მიხედვით, შეიძლება ჩაითვალოს პირის პირად ცხოვრებაში გაუმართლებელ ჩარევად.¹⁹⁴ გარდა ამისა, მათი განუსაზღვრელი დროით შენახვა საკმაოდ არაპრაქტიკულია საგანმანათლებლო დაწესებულებისთვისაც, რადგანაც მათი შენახვა და უსაფრთხოების უზრუნველყოფა საკმაოდ დიდ ადამიანურ და ფინანსურ რესურსთანაც არის დაკავშირებული. ამიტომაც, მნიშვნელოვანია, რომ მონაცემთა დამმუშავებელმა, უმაღლესმა საგანმანათლებლო დაწესებულებამ სწორად შეაფასოს და განისაზღვროს სტუდენტთა პერსონალურ მონაცემთა შენახვის და დაარქივების წესი. ვინაიდან უნივერსიტეტმა, რომელიც ამუშავებს დიდი მოცულობით მონაცემს, უნდა უზრუნველყოს სამართლიანი ბალანსის დაცვა მონაცემთა დამუშავების კანონიერ ინტერესებს, მონაცემთა სუბიექტის პირადი ცხოვრების ხელშეუხებლობასა და მონაცემების დაცვის უფლებას შორის¹⁹⁵.

2.2. მონაცემთა სისწორის დაცვა

მონაცემთა დამუშავების აუცილებლობისა და მათი შენახვის პროპორციული ვადის განსაზღვრა, მიზნის მიღწევის პროპორციულად, მრავალი პრობლემის თავიდან აცილების საშუალებას იძლევა. განსაკუთრებით მაშინ, როდესაც მონაცემთა დამმუშავებელს ზუსტი და სწორი მონაცემების შენახვის ვალდებულება გააჩნია.¹⁹⁶ მიჩნეულია, რომ მონაცემთა დამუშავების ვადაზე ადრე ნაშლა, ისევე, როგორც მათი განსაკუთრებით დიდი ხნით შენახვა, შესაძლოა იყოს რისკის შემცველი და პრობლემების წარმოშობის საფუძველი, რადგანაც დროის გასვლასთან ერთად მათი სიზუსტის დადგენაც უფრო რთული ხდება.¹⁹⁷

¹⁹³ საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 9 თებერვლის N1/2/622 გადაწყვეტილება საქმეზე „საქართველოს მოქალაქე ედიშერ გოდუაძე საქართველოს შინაგან საქმეთა მინისტრის წინააღმდეგ“.

¹⁹⁴ Brunet v. France, [EctHR], App. No. 21010/10, 18 September 2014.

¹⁹⁵ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 10 ივლისის №1/234/2020 გადაწყვეტილება „სსიპ-სოხუმის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

¹⁹⁶ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Art. 5 para. 1 d; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Art. 5 para. 4 d, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „დ“ ქვეპუნქტი.

¹⁹⁷ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბი-

საგანმანათლებლო დაწესებულებაც, როგორც მონაცემთა დამმუშავებელი, ვალდებულია მიიღოს ყველა საჭირო ზომა, რათა უზრუნველყოს სტუდენტთა პერსონალური მონაცემების ნამდვილობა და სიზუსტე. ამ პრინციპის უზრუნველსაყოფად ზოგიერთ შემთხვევაში შესაძლოა საჭირო იყოს სტუდენტის მხრიდან გარკვეული ქმედების განხორციელებაც, მაგრამ ვალდებულება მათი ზუსტი შენახვისათვის იმპერატიულად მაინც საგანმანათლებლო დაწესებულებას ეკისრება.¹⁹⁸ სწორედ, ამ უკანასკნელმა უნდა მიიღოს გადანაცვები, არაზუსტი მონაცემების შესწორების, წაშლის ან დაბლოკვის შესახებ.¹⁹⁹

საქართველოსა და ევროკავშირის კანონმდებლობა არ ადგენს, რა შეიძლება იყოს არაზუსტი და არანამდვილი ინფორმაცია და როგორ უნდა გადაამოწმოს მონაცემთა დამმუშავებელმა მათი სიზუსტე. ინგლისის პერსონალურ მონაცემთა დაცვის აქტი კი პირდაპირ უთითებს, რომ არაზუსტია ნებისმიერი არასწორი ან შეცდომაში შემყვანი ინფორმაცია კონკრეტულ პერსონალურ მონაცემთან მიმართებით.²⁰⁰ მიუხედავად ჩანაწერის არარსებობისა, მიჩნეულია, რომ იგი კონკრეტულ ფაქტებთან მიმართებით უნდა გადამოწმდეს,²⁰¹ და ყოველ კონკრეტულ შემთხვევაში გათვალისწინებული უნდა იქნეს მათი შეგროვების მიზანიც.²⁰² აღნიშნულიდან გამომდინარე, თუ სტუდენტის ელექტრონულ ჟურნალში შეტანილი იქნა მცდარი შეფასება, მიუხედავად ამ უკანასკნელის მომართვისა, საგანმანათლებლო დაწესებულებამ მხედველობაში უნდა მიიღოს ამ მონაცემების დამუშავების მიზანი და გაასწოროს სტუდენტის ელექტრონული შეფასება.

მნიშვნელოვანია ისიც, რომ არაზუსტი ან არასწორი მონაცემების ჩასწორება არ გულისხმობს რომ ისინი ყველა შემთხვევაში უნდა წაიშალოს და განადგურდეს.²⁰³ მაგალითად, თუ სტუდენტმა წარმატებით ვერ დაასრულა რომელიმე კურსი და ერთი ან რამდენიმე საგნის გავლა თავიდან მოუწია, მათი წარმატებით დასრულების შემდეგ აუცილებელი არ არის „ძველი“ მონაცემები მყისიერად წაიშალოს. ყოველ კონკრეტულ შემთხვევაში საგანმანათლებლო დაწესებულებ-

ლისი, 2017, 79, იხ. ციტირება: პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო, 2013, 21.

¹⁹⁸ Bygrave L., *Data Privacy Law: An International Perspective*, Oxford University Press, 2014, 164.

¹⁹⁹ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერტი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 145.

²⁰⁰ The Data Protection Act 2018, Article (1).

²⁰¹ Hallinan D., Zuiderveen Borgesius F., *Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle*, *International Data Privacy Law*, Vol. 10, Iss. 1, 2020, 20.

²⁰² Peter Nowak v Data Protection Commissioner, [CJEU], C-434/16, 20 December 2017, para. 53.

²⁰³ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერტი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 146.

ბამ უნდა შეაფასოს მონაცემთა სისწორე და სიზუსტე და მიიღოს გადაწყვეტილება რა ტექნიკური ზომები უნდა განახორციელოს ამ ვალდებულების შესასრულებლად.²⁰⁴ მაგალითად, ხშირია შემთხვევები, როდესაც სტუდენტი იცვლის საკონტაქტო ტელეფონის ნომერს ან ელექტრონული ფოსტის მისამართს (შიდაორგანიზაციული ფოსტის არარსებობისას). ასეთ დროს, ელექტრონულ პლატფორმაზე, უნივერსიტეტს შეუძლია თავად გაასწოროს ეს მონაცემები ან სტუდენტს მისცეს უფლება თავად შეცვალოს და დააზუსტოს აღნიშნული ინფორმაცია, ხოლო უნივერსიტეტმა უზრუნველყოს ამ ცვლილებების აღრიცხვა.

მონაცემთა დამმუშავებლის მიერ ინფორმაციის ნამდვილობისა და სიზუსტის უზრუნველყოფის ვალდებულება ემსახურება როგორც სუბიექტების ინტერესების დაცვის მიზანს, ასევე საგანმანათლებლო დაწესებულებების ინტერესებსაც.²⁰⁵ ვინაიდან სტუდენტის შესახებ სწორი და ზუსტი ინფორმაციის არსებობა, მათ შორის, მისი საკონტაქტო მონაცემების თაობაზე, უმნიშვნელოვანესია საგანმანათლებლო დაწესებულებისთვის, სტუდენტთა ინფორმირებულობისა და სასწავლო პროცესის ეფექტიანად წარმართვის უზრუნველყოფის მიზნებისთვის.

2.3. მონაცემთა ნაშლა/განადგურება

პერსონალურ მონაცემთა დაცვის კანონმდებლობა განსაზღვრავს, რომ მონაცემთა დამმუშავების მიზნის მიღწევის შემდეგ, მონაცემთა სუბიექტის მიერ თანხმობის გამოთხოვის ან/და დამმუშავების სხვა საფუძვლების აღარ არსებობის შემთხვევაში, მონაცემთა დამმუშავებელმა დამმუშავებული მონაცემები უნდა წაშალოს, გაანადგუროს ან/და შეინახოს არაიდენტიფიცირებადი ფორმით.²⁰⁶ სწორედ მონაცემთა დამმუშავებელი ვალდებულია წინასწარ შეაფასოს და განსაზღვროს ვადა, რა ვადით დაამუშავებს პირის პერსონალურ მონაცემებს და ასევე დაადგინოს მათი განადგურების/წაშლის და დეპერსონალიზაციის მექანიზმები.²⁰⁷

ზემოაღნიშნულიდან გამომდინარე, იმისათვის, რომ დაცული იყოს კანონმდებლობით გათვალისწინებული პრინციპები, მნიშვნელოვანია, საგანმანათლებლო დაწესებულებამ შეაფასოს და შიდაორგანიზაციული დოკუმენტით

²⁰⁴ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 145-146.

²⁰⁵ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 28 სექტემბრის №გ-1/340/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემომების დასრულების შესახებ“.

²⁰⁶ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „ე“ ქვეპუნქტი.

²⁰⁷ Georgiou E., GDPR in Between Profiles and Decision-Making: How the General Data Protection Principles Under Article 5 GDPR Are Engaged with Profiling, in the book: Personal data protection and legal developments in the European Union, edited by Tzanou M., Hershey PA, 2020, 98.

განსაზღვროს მის მიერ პირდაპირ ან შესაბამისი პლატფორმების მეშვეობით დამუშავებული სტუდენტების მონაცემების ელექტრონულ ბაზაში შენახვის საჭიროება, ფორმა, ვადა და ნაშლის მექანიზმები.²⁰⁸ მართალია დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების უმრავლესობა ავტომატური საშუალებით გროვდება და შესაბამის ელექტრონულ ბაზაზე ინახება, თუმცა ეს არ გამორიცხავს მათი მატერიალური სახით შენახვის შესაძლებლობასაც.²⁰⁹ ამიტომაც აუცილებელია, რომ მონაცემთა განადგურების მექანიზმებიც წინასწარ იყოს განსაზღვრული. ამგვარად შესაძლებელი იქნება ყველა ფორმაში შენახული მონაცემების განადგურების/ნაშლის ან დეპერსონალიზაციის მიღწევა, რაც გამორიცხავს მონაცემთა უკანონო შენახვასა და გამოყენებას.

მნიშვნელოვანია მონაცემები ნაიშალოს ისე, რომ უზრუნველყოფილი იყოს მესამე პირებისთვის უკანონო წვდომის შეუძლებლობა.²¹⁰ ხშირ შემთხვევაში მონაცემთა დამუშავებლებს ელექტრონულ ბაზებზე არსებული მონაცემების მიმართ აქვთ შემუშავებული ისეთი მექანიზმი, რომელიც უზრუნველყოფს პირის პერსონალური მონაცემების ავტომატურად ნაშლას გარკვეული პერიოდის შემდეგ.²¹¹ სწორედ მსგავსი მექანიზმის შემოღება შეუძლიათ უმაღლეს საგანმანათლებლო დაწესებულებებს ელექტრონულ ბაზებში არსებულ სტუდენტთა პერსონალურ მონაცემებთან მიმართებითაც. მაგალითისთვის, საგანმანათლებლო დაწესებულების მიერ წინასწარ განსაზღვრული დროის შემდეგ ავტომატურად ნაიშალოს სტუდენტის ელექტრონული ჟურნალი, მისი პირადი ინტერნეტ პლატფორმის ვებ-გვერდი/კაბინეტი და სხვა.

სტუდენტის პერსონალური მონაცემების ნაშლის საკითხი განსაკუთრებით აქტუალურია ტექნოლოგიებისა და ინტერნეტის ეპოქაში, როდესაც ინტერნეტში განთავსებული პერსონალური ინფორმაცია შესაძლოა არამიზნობრივად დიდი დროის განმავლობაში დარჩეს ხელმისაწვდომი სხვა პირებისთვის და ამით დაირღვევს მონაცემთა კანონიერი დამუშავებისათვის აუცილებელი პრინციპები და ადამიანის პირადი ცხოვრების ხელშეუხებლობის უფლება.²¹² ხშირ

²⁰⁸ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 14 ივნისის №გ-1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემონმების დასარულების შესახებ“, 12.

²⁰⁹ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 14 ივნისის №გ-1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემონმების დასარულების შესახებ“.

²¹⁰ Wang X., Personal data security Technichal Guide for Online Education Platforms, Morcow, 2020, 11-12.

²¹¹ Progin-Theuerkauf S., Zoetewij M., Turhan C., Smart Borders and Data Protection, in the book: Personal data protection and legal developments in the European Union, edited by Tzanou M., Hershey PA, 2020, 98.

²¹² Google Spain vs AEPD and Mario Costeja Gonzalez [CJEU], C-131/12, 13 May 2014.

შემთხვევაში, სტუდენტების პერსონალური ინფორმაციები საგანმანათლებლო დაწესებულებების ვებ-გვერდებზეც ქვეყნდება, რა დროსაც მნიშვნელოვანია, რომ მათ უზრუნველყონ ამ ფაილების გამოქვეყნება მხოლოდ მანამ, სანამ არსებობს მონაცემთა დამუშავების საჭიროება²¹³ და ნაშალონ ისინი ისე, რომ მონაცემები აღარსად ინახებოდნენ „ქეშირებული“ (დამახსოვრებული) სახით.²¹⁴ შესაბამისად, საგანმანათლებლო დაწესებულებამ, არსებული ტექნოლოგიებისა და ხარჯების გათვალისწინებით, უნდა აცნობოს ინფორმაციის ნაშლის შესახებ სხვა ორგანიზაციებს, რომლებიც ამავე მონაცემებს ამუშავებენ.²¹⁵ აღნიშნული, მეტად არის გასათვალისწინებელი ონლაინ შეხვედრების უზრუნველსაყოფად გამოყენებული ელექტრონული პლატფორმების მიმართაც. საგანმანათლებლო დაწესებულება ვალდებულია თავადაც ნაშალოს დამუშავებული პერსონალური მონაცემები და დარწმუნდეს, რომ ამ ვადის გასვლის შემდეგ არც იმ ელექტრონული პლატფორმების პროვაიდერ კომპანიებში ინახება სტუდენტების პერსონალური მონაცემები.

უნდა აღინიშნოს ისიც, რომ შესაძლებელია არსებობდეს შემთხვევები, როდესაც მონაცემები აღარ არის საჭირო იმ მიზნის მისაღწევად, რისთვისაც მოხდა მათი შეგროვება ან დამუშავება, მაგრამ მოხდეს გარკვეული ინფორმაციის შენახვა დეპერსონალიზირებული სახით. მაგალითად, უნივერსიტეტმა არ ნაშალოს ინფორმაცია რომელიმე სასწავლო წელს მიღებულ ან/და კურსდამთავრებულ სტუდენტებთან მიმართებით და შეინახოს ისინი, როგორც სტატისტიკური მონაცემები, იმგვარად, რომ არ იდენტიფიცირდებოდეს კონკრეტული სტუდენტების ვინაობა.

როგორც აღინიშნა, გაუმართლებელია მონაცემთა უვადოდ ან მისი მიზნის არაპროპორციულად დიდი ხნის ვადით შენახვა და აუცილებელია, ვადის გასვლის შემდეგ მათი ნაშლა/განადგურება. დაუშვებელია, რომ ეს მიდგომა შეიცვალოს და საგანმანათლებლო დაწესებულებამ მიმართოს მხოლოდ წვდომის

²¹³ სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 10 აგვისტოს №1/266/2020 გადაწყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“; საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 30 ივლისის №გ-1/252/2019 გადაწყვეტილება „სსიპ ილიას სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“; საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 10 ივლისის № 1/234/2020 გადაწყვეტილება „სსიპ-სოხუმის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

²¹⁴ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 14 ივნისის №გ-1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემონმების დასრულების შესახებ“; საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 31 ივლისის №1/253/2020 გადაწყვეტილება „სსიპ – ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

²¹⁵ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ, თბილისი, 2018, 11.

შეზღუდვის პრინციპს. ეს უკანასკნელი თავისი არსით, სულ სხვა მიზანს ემსახურება და არ წარმოადგენს სამართლიან ბალანსს, ვიანიდან პერსონალურ მონაცემთა მიმღებ პირებს უნდა ჰქონდეთ მონაცემებზე დაშვების უფლება, არა მხოლოდ ახლანდელი, არამედ წარსული დროის მიმართაც.²¹⁶ მონაცემთა წაშლა კი თავისი არსით სრულიად უნდა განსხვავდებოდეს მათი დაარქივებისგან და შემდგომში გამოყენების რამენაირი შესაძლებლობიდან და გულისხმობს ისეთ მდგომარეობას, როდესაც პერსონალური მონაცემები არანაირი ფორმით აღარ არის ხელმისაწვდომი.²¹⁷

გარდა იმისა, რომ მონაცემთა დამმუშავებელი ვალდებულია თავად უზრუნველყოს დამუშავებულ პერსონალურ მონაცემთა წაშლა/განადგურება, პერსონალურ მონაცემთა დაცვის კანონმდებლობა მონაცემთა სუბიექტს ანიჭებს შესაძლებლობას, მოითხოვოს მათი წაშლა.²¹⁸ თუმცა, ეს უფლება აბსოლუტური არ არის და კანონმდებლობით გათვალისწინებულ შემთხვევებში, საგანმანათლებლო დაწესებულება უფლებამოსილია უარი განაცხადოს მონაცემთა წაშლაზე.²¹⁹ მაგალითად, დისტანციური სწავლების დროს ჩანერილი ლექციების შემთხვევაში, საგანმანათლებლო დაწესებულებამ უარი შეიძლება უთხრას სტუდენტს ამ ჩანაწერების ვადაზე ადრე წაშლის მოთხოვნაზე, რადგან ამით ზიანი შეიძლება მიაღწეს იმ სალექციო კურსის ფარგლებში მყოფ სხვა სტუდენტებს.

3. ფაილური სისტემის კატალოგის წარმოება

ფაილური სისტემა მონაცემთა სტრუქტურულიზებული წყებაა, რომელშიც პირის პერსონალური მონაცემები, მათზე ხელმისაწვდომობის მიზნით, გარკვეული კრიტერიუმის მიხედვით არის დალაგებული.²²⁰ ფაილური სისტემის კატალოგი ე.წ. „მონაცემთა ბაზა“, რომელიც შეიძლება არსებობდეს როგორც ელექტრონული ასევე მატერიალური სახითაც. საგანმანათლებლო დაწესებუ-

²¹⁶ College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, [CJEU], C-553/07, 7 May 2009, para. 70.

²¹⁷ Information Commissioner's Office, Deleting personal data, 2014, 4-5.

²¹⁸ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Article 17; „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 22-ე მუხლი.

²¹⁹ იქვე, 24-ე მუხლი.

²²⁰ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Article 2 para. 1; „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ნ“ ქვეპუნქტი.

ლებებში მსგავსი სისტემის კატალოგები შეიძლება არსებობდეს სტუდენტთა პირად საქმეებთან მიმართებით, უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონულ ბაზაში ასახულ პერსონალურ ინფორმაციებთან და სხვა ნებისმიერ პერსონალურ მონაცემთა სტრუქტურის მქონე ნაწილებთან მიმართებით. ასეთი მონაცემთა ბაზების გამოყენების შემთხვევაში კი მონაცემთა დამმუშავებელი ვალდებულია აწარმოოს ფაილური სისტემის კატალოგი.²²¹ შესაბამისად, იმ შემთხვევაში, თუ საგანმანათლებლო დაწესებულებები, იყენებენ პერსონალურ მონაცემთა შემცველ სტრუქტურის მქონე ბაზებს, მაშინ ისინი ვალდებული არიან აწარმოონ ფაილური სისტემის კატალოგები საქართველოს კანონმდებლობით დადგენილი წესის მიხედვით.

საქართველოს კანონმდებლობითვეა დადგენილი ის მონაცემები, რომლებიც ფაილური სისტემის კატალოგის აუცილებელი კომპონენტებია.²²² მათ შორისაა, ინფორმაცია მონაცემთა დამმუშავებელი სუბიექტის და უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში), დამუშავების სამართლებრივი საფუძვლებისა და მიზნების, შენახვის ვადისა და უსაფრთხოების ზოგადი წესის, მონაცემთა სუბიექტის უფლების შეზღუდვის ფაქტი და საფუძვლების, ასევე დამმუშავებელი მონაცემების კატეგორიისა და მათი სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემის შესახებ და ასეთი გადაცემის სამართლებრივი საფუძვლების შესახებ. ამასთანავე, თითოეულ ფაილური სისტემის კატალოგს უნდა ჰქონდეს თავისი სახელწოდება.²²³

გარდა იმისა, რომ უმაღლესი საგანმანათლებლო დაწესებულება ვალდებულია აწარმოოს ფაილური სისტემის კატალოგი, მას კანონმდებლობით აქვს დაკისრებული მოვალეობა, შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს ინფორმაცია ასეთი სისტემის შექმნამდე ან მასში ახალი კატეგორიის მონაცემთა შეტანამდე.²²⁴ აღსანიშნავია ისიც, რომ კანონმდებლობა მონაცემთა დამმუშავებელს ავალდებულებს შექმნას ვიდეოჩანანერების შენახვისთვის განკუთვნილი ფაილური სისტემა. ეს უკანასკნელი კი უნდა შეიცავდეს ინფორმაციას მონაცემთა დამმუშავების თარიღის, ადგილისა და დროის შესახებ, ასევე დამმუშავებელ ჩანაწერებს, მათ შორის ხმასა და ვიზუალურ გამოსახულებას.²²⁵ აღნიშნული ვალდებულება კიდევ უფრო აქტუალური გახდა დისტანციური სწავლების პირობებში, როდესაც საგანმანათლებლო დაწესებულების მიერ სინქრონული თუ

²²¹ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-19 მუხლის პირველი პუნქტი.

²²² იქვე.

²²³ იქვე.

²²⁴ იქვე, მე-20 მუხლის პირველი და მე-2 პუნქტები.

²²⁵ იქვე, მე-12 მუხლის მე-6 პუნქტი.

ასინქრონული სწავლებისას, მიმდინარე ლექციების, სემინარების, გამოცდების ან სხვა ონლაინ ღონისძიების ჩანერა ხორციელდება. ასეთი ვიდეოჩანაწერები გარკვეული ვადით ინახება უნივერსიტეტის მიერ შესაბამის ელექტრონულ ბაზაზე/ან პლატფორმაზე და კატეგორიების მიხედვითაც შეიძლება იყოს სტრუქტურული-ზებულის. მაგალითად, დალაგებული იყოს ღონისძიების კატეგორიების, საგნებისა თუ ჯგუფების მიხედვით. ასეთ დროს, კი უნივერსიტეტს, როგორც მონაცემთა დამმუშავებელს უნდა დაეკისროს ვალდებულება, აწარმოოს ფაილური სისტემის კატალოგი, სისტემატურად განაახლოს მასში შეყვანილი ინფორმაცია და წარუდგინოს იგი პერსონალურ მონაცემთა დაცვის სამსახურს. ასეთი ვალდებულების შეუსრულებლობა კი უნივერსიტეტის მიმართ ადმინისტრაციული პასუხისმგებლობის დაკისრების საფუძველიც შეიძლება გახდეს²²⁶.

უნდა აღინიშნოს, რომ ფაილური სისტემის კატალოგის წარმოებას და შეტყობინების ვალდებულებას მხოლოდ ფორმალური ხასიათის დატვირთვა არ უნდა ჰქონდეს. იგი რეალურად, საწინდარია მონაცემთა დაცვისთვის გასატარებელ ორგანიზაციულ ტექნიკური ზომების მისაღებად. ასევე, იგი უზრუნველყოფს პერსონალურ მონაცემთა დაცვის სამსახურის მხრიდან ეფექტიანი კონტროლის განხორციელების შესაძლებლობას.²²⁷ ასეთი კატალოგების შექმნა, უზრუნველყოფს, რომ მონაცემთა დამმუშავებელმა წინასწარ განსაზღვროს და გაიაზროს, რა სახის პერსონალურ მონაცემებს ამუშავებს დაწესებულება და როგორ აქვს ისინი სისტემატიზებული კატეგორიებად. საგანმანათლებლო დაწესებულება ასევე შეიძლება განსაზღვროს, შეიცავენ თუ არა მონაცემები სენსიტიურ ინფორმაციას და რა ტიპის ტექნიკური თუ ორგანიზაციული ზომების მიღება იქნება საჭირო მათ დასაცავად.

4. მონაცემთა უსაფრთხოების უზრუნველყოფა

მონაცემთა დამმუშავების კანონიერებისათვის, მნიშვნელოვანია, რომ მონაცემთა დამმუშავების საფუძვლების არსებობის და პრინციპების განუხრელი დაცვის პარალელურად, მონაცემთა დამმუშავებელმა უზრუნველყოს მონაცემთა უსაფრთხოების წესების დაცვა დამმუშავების მთელი პროცესის განმავლობაში.²²⁸ პერსონალურ მონაცემთა დაცვის კანონმდებლობა ადგენს, რომ აუცილებელია,

²²⁶ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 25 მაისის გადაწყვეტილება №გ-1/286/2017 „შპს „ა“-ს შემონმების დასრულების შესახებ“.

²²⁷ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბილისი, 2017, 98-99.

²²⁸ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 148.

მონაცემთა დამმუშავებელმა მიიღოს შესაბამისი ორგანიზაციულ-ტექნიკური ზომები და უზრუნველყოს მონაცემთა სათანადო უსაფრთხოება, მათ შორის, უკანონო და უნებართვო დამმუშავების, შემთხვევითი განადგურების და ზარალის თავიდან ასაცილებლად.²²⁹ ხაზგასასმელია ისიც, რომ უსაფრთხოების დაცვა-სთან დაკავშირებული მოთხოვნების შეუსრულებლობის დადგენისთვის აუცილებელი არ არის, რომ მონაცემების უკანონო დამმუშავების შედეგი დადგეს, არამედ საკმარისია ისიც, თუ მონაცემთა დამმუშავებელი არ ან ვერ გაითვალისწინებს მონაცემთა დამმუშავებასთან დაკავშირებულ რისკებს და თავისი ქმედებით ან უმოქმედობით შეუქმნის ასეთ საფრთხეს მონაცემთა დამმუშავებას.²³⁰ ამასთანა-ვე, არ აქვს მნიშვნელობა საგანმანათლებლო დაწესებულების ქმედება განზრახ, თუ გაუფრთხილებლობით იქნება გამოწვეული.²³¹ აღსანიშნავია, ისიც, რომ პერ-სონალურ მონაცემთა დაცვის უსაფრთხოების უზრუნველყოფა საგანმანათ-ლებლო დაწესებულებებისთვის უდიდეს გამოწვევას წარმოადგენს, არა მხოლოდ საქართველოსათვის,²³² არამედ სხვა ქვეყნებისთვისაც,²³³ მათ შორის, დისტანცი-ური სწავლების განმავლობაშიც.

უსაფრთხოების შესაბამისი ზომების შემუშავება და დანერგვა ყოველ კონ-კრეტულ შემთხვევაში განსხვავებულად უნდა შეფასდეს²³⁴ და დამოკიდებულია დაწესებულების ზომაზე, მონაცემთა დამმუშავების პროცესებზე, დამმუშავებუ-ლი მონაცემების კატეგორიებზე და სხვა გარემოებებზე. მნიშვნელოვანია ისიც, რომ შეუძლებელია მონაცემთა უსაფრთხოება უზრუნველყოფილი იყოს მხო-ლოდ ტექნიკური ან მხოლოდ ორგანიზაციული წესების შემოღებისას. ამიტომ, იგი კომპლექსურ მიდგომას საჭიროებს.²³⁵ შესაბამისად, თითქმის წარმოუდგენე-

²²⁹ Regulation 2016/679 of the European Parliament and of the Council 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), 27 April 2016, Articles 5 para.1 and art. 39; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, Art. 7, „პერ-სონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლი.

²³⁰ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 26 დეკემბ-რის გადაწყვეტილება სს „ა“-ს შემონმების დასრულების შესახებ, საქმე №გ-1/701/2018, 9; Decision №DI-2019-9432 of Swedish Authority for Privacy Protection on the supervision of UMEA's university, 10 December 2020.

²³¹ საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 30 ივლისის №გ-1/252/2019 გადა-წყვეტილება „სსიპ ილიას სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“

²³² სახელმწიფო ინსპექტორის სამსახურის 2021 წლის საქმიანობის ანგარიში, 40-41.

²³³ Smith, C., Diaz, A., & Sterns, R., Data breach at university: preparing our networks, National Security Law Journal, No. 5(1), 2016, 121-126.

²³⁴ Huth D., Matthes F., Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements, Cancun, 2019, 3.

²³⁵ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერტი მ., მონაცემთა დაცვის ევროპული სამა-რთლის სახელმძღვანელო, ლუქსემბურგი, 2018, 189.

ლია, რომ ერთი კონკრეტული მიდგომა შემუშავდეს ყველა ტიპის დანესებულებისთვის, რაც მათ ინტერესებზე და საჭიროებებზე იქნება მორგებული. თუმცა, შესაძლებელია რამდენიმე ძირითადი საკითხის გამოყოფა, რომელთაც შესაბამის ქვეთავებში განიხილება.

4.1. შეზღუდული წვდომა დამუშავებულ მონაცემებზე

მონაცემთა უსაფრთხოების უზრუნველყოფის ერთ-ერთი მნიშვნელოვანი კრიტერიუმი პასუხისმგებლობის მკაფიო გადანაწილება და უფლებამოსილება ნათლად გამოიყვანა.²³⁶ ამასთან, ვინაიდან პერსონალური მონაცემების დაცვა კერძო ცხოვრების ხელშეუხებლობის ნაწილია და კონსტიტუციური ბუნება აქვს,²³⁷ დაუშვებელია რომ მასზე წვდომა ნებისმიერ პიროვნებას განუსაზღვრელად გააჩნდეს, რაც კიდევ უფრო მარტივი ხდება ავტომატურად დამუშავებული მონაცემების შემთხვევაში.²³⁸ შესაბამისად, იმის განსაზღვრა, თუ ვის, როდის და რა კრიტერიუმების საფუძველზე ექნება წვდომა პერსონალურ მონაცემებთან, პერსონალური მონაცემების დამუშავებისა და დაცვის ქვაკუთხედი.²³⁹ ამიტომაც მნიშვნელოვანია, რომ საგანმანათლებლო დანესებულებას ჰყავდეს შესაბამისი, წინასწარ განსაზღვრული პირობები, რომლებსაც ექნებათ წვდომა სტუდენტების პერსონალურ მონაცემებზე. რა თქმა უნდა, სხვადასხვა ტიპის მონაცემებზე საგანმანათლებლო დანესებულებაში დასაქმებულ სხვადასხვა პიროვნებას შეიძლება გააჩნდეს წვდომა. აღნიშნული კი შესაბამისი საჭიროების მიხედვით უნდა შეფასდეს. მაგალითისთვის, ფაკულტეტების მდივნებს შეეძლოთ ელექტრონულ ჟურნალში ჩარიცხული სტუდენტების შესახებ მიღებული ინფორმაციის შევსება/დამატება/რედაქტირება.²⁴⁰ ამ შემთხვევაში მნიშვნელოვანია, მათ წვდომა შეზღუდული ჰქონდეთ მხოლოდ მათი ფაკულტეტის ხელთ არსებულ მონაცემებზე. ასევე, ცხადია, რომ საგანმანათლებლო დანესებულების ფინანსური განყოფილების თანამშრომელს უნდა ჰქონდეს წვდომა სტუდენტის ფინანსურ ბარათზე და მის გადახდებზე, იმისთვის, რომ შეასრულონ მათზე დაკისრებული მოვალეობები. შეზღუდული წვდომის ფარგლებში,

²³⁶ იქვე, 190.

²³⁷ საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2013 წლის 30 მაისის განჩინება საქმეზე №ბს-527-518(კ-12).

²³⁸ Cha S. -C., Yeh K. -H., A Data-Driven Security Risk Assessment Scheme for Personal Data Protection, IEEE Access, Vol. 6, 2018, 50510, იხ., <<https://bit.ly/3yGceWf>> [30.06.2022].

²³⁹ Borgman, C. L., Open data, grey data, and stewardship: universities at the privacy frontier, Berkeley Technology Law Journal, No. 33(2), 2018, 395.

²⁴⁰ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 10 მაისის №გ-1/141/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

მნიშვნელოვანია, რომ ლექტორებს/პროფესორებს წვდომა ჰქონდეთ მხოლოდ თავიანთ სასწავლო ჯგუფებში შემავალი სტუდენტების მონაცემებზე და ანალოგიურად, სტუდენტებსაც მხოლოდ თავიანთ მონაცემებზე წვდომის უფლება უნდა გააჩნდეთ. დისტანციური სწავლების მიმდინარეობისას მნიშვნელოვანია ისიც, რომ კონკრეტულ ლექცია/სემინარზე დასწრება მხოლოდ მასზე რეგისტრირებულ სტუდენტებს შეეძლოთ. აგრეთვე, აუცილებელია საგანმანათლებლო დაწესებულებამ არ გაასაჯაროოს შეხვედრის ელექტრონული ლინკი მესამე პირებზე და შეხვედრების ჩანაწერები არ გახადოს ხელმისაწვდომი არავისთვის, გარდა სალექციო კურსში ჩართული პირებისა. ასევე უნდა შეზღუდოს ამ სალექციო მასალების პერსონალურ კომპიუტერში ჩამოწერის შესაძლებლობა.²⁴¹ ეს ყოველივე უზრუნველყოფს პირის პერსონალური მონაცემების მესამე პირებზე გამჟღავნების რისკების თავიდან აცილებას.

ცხადია, რომ საგანმანათლებლო დაწესებულებამ ყოველ კონკრეტულ შემთხვევაში უნდა შეაფასოს თუ ვის და რა დოზით მიანიჭებს სტუდენტის პერსონალურ მონაცემებზე წვდომას და როგორ უზრუნველყოფს ელექტრონული საშუალებებით პერსონალურ მონაცემებზე ავტომატიზებული და შეზღუდული წვდომის წესების იმპლემენტირებას. ასევე, გადანყვებილების მიღებისას მან უნდა გაითვალისწინოს ორივე მხარის ინტერესები, რათა არ შეექმნას საფრთხე საგანმანათლებლო პროცესის ეფექტურად წარმართვას და სტუდენტის პირადი ცხოვრების უფლებაში გაუმართლებელ ჩარევას.

4.2. მონაცემთა დამუშავებაზე პასუხისმგებელი პირი, რისკის ანალიზი და თვითმონიტორინგი

საქართველოსა და ევროკავშირის კანონმდებლობა არ ადგენს მონაცემთა დაცვისათვის კონკრეტული უსაფრთხოების ზომებს. უსაფრთხოების პრინციპის იმპლემენტირება აგებულია რისკების განსაზღვრისა და შეფასების პრინციპზე.²⁴²

მიჩნეულია, რომ მონაცემთა უსაფრთხოების უზრუნველსაყოფად პირველი ეტაპი მონაცემთა დამუშავებასთან დაკავშირებული რისკების გამოვლენაა.²⁴³ ამ მიზნების მისაღწევად, მნიშვნელოვანია, საგანმანათლებლო დაწესებულებამ განსაზღვროს შეგროვებულ პერსონალურ მონაცემთა სახეები და მათი სამართლებრივი საფუძვლები, მათი შეგროვების მიზანი და იმ პირების სია, ვისაც

²⁴¹ სახელმწიფო ინსპექტორის სამსახური, რეკომენდაცია-პერსონალური მონაცემების დამუშავება დისტანციური სწავლების პროცესში, 2022, 6.

²⁴² Cha S. -C., Yeh K. -H., A Data-Driven Security Risk Assessment Scheme for Personal Data Protection, IEEE Access, Vol. 6, 2018, 50510, იხ., <<https://bit.ly/3yGceWf>> [30.06.2022].

²⁴³ Decesion №ZSOŚS.421.25.2019 of The President of the Personal Data Protection Office of Poland on inspection of Warsaw University of Life Sciences (SGGW), 21 August 2020.

ამ მონაცემებზე ექნება წვდომა (როგორც ადმინისტრაციული პერსონალის, ისე სტუდენტების და დამხმარე პერსონალისთვის), მათი გამჟღავნების ტიპური შემთხვევები და პოტენციური ინციდენტები.²⁴⁴ ასევე, დეტალურად უნდა შეფასდეს თითოეული ტიპური ინციდენტით გამოწვეული სავარაუდო შედეგებიც. მაგალითად, დისტანციური სწავლებისას ჩანერილი ლექციების მესამე პირებზე გამჟღავნებისას, რა საფრთხე შეიძლება შეექმნას ვიდეოჩანანერში მყოფ სტუდენტებს. მაგალითისთვის, შესაძლებელია ამას მოჰყვეს კონკრეტული პირის მიმართ დამცინავი კომენტარები ან სხვაგვარი დისკრიმინაცია. სტუდენტების ვინაობის დასადგენი ინფორმაციის გამჟღავნება, შეიძლება შემდეგში გამოყენებული იყოს დანაშაულებრივი მიზნებისთვისაც. მეტად საყურადღებოა განსაკუთრებული კატეგორიის პერსონალური მონაცემების უკანონო ხელყოფით ან გამჟღავნებით მიყენებული ზიანიც.

აღსანიშნავია ისიც, რომ გერმანიაში ფართოდ არის გავრცელებული მონაცემთა დამუშავების ზეგავლენის შეფასების დოკუმენტის შემუშავება.²⁴⁵ მასში უნდა აისახოს მონაცემთა კატეგორიები, მათი დამუშავების მიზნები და პროპორციულობა, ასევე მათი დამუშავების პროცესი და საფუძვლები.²⁴⁶ გარდა ამისა, ასეთ დროს უნდა მოხდეს ადამიანის ძირითადი უფლებების შელახვის შესაძლო საფრთხეების შეფასებაც და განისაზღვროს მათი დაცვისთვის საჭირო ორგანიზაციულ-ტექნიკური ზომები.²⁴⁷ აღნიშნული პრინციპის დანერგვა, მნიშვნელოვნად შეამცირებს უმაღლეს საგანმანათლებლო დაწესებულებებში პერსონალური მონაცემების არამიზნობრივ დამუშავებას და უზრუნველყოფს სტუდენტთა უფლებების მაქსიმალურად დაცვასაც.

რისკების და შედეგების განსაზღვრისას, ნათლად იკვეთება, რაოდენ დიდი ზიანი შეიძლება მიაღგეს მონაცემთა სუბიექტს. ამ რისკების სწორად შეფასებისთვის კი მნიშვნელოვანია, წინასწარ დადგინდეს და გაიწეროს საგანმანათლებლო დაწესებულების მიერ სტუდენტთა პერსონალური მონაცემების დამუშავების პროცესი, მათ შორის, დისტანციური სწავლებისას. აუცილებელია დადგინდეს, თუ რომელი ტექნიკური ზომები იქნება ეფექტური, დაწესებულებაში რისკის შესაბამისი უსაფრთხოების დონის უზრუნველსაყოფად და როგორ უნდა განხორციელდეს ინციდენტებზე რეაგირება, განისაზღვროს პასუხისმგებელი პირის უფლებამოსილებები და სხვა მნიშვნელოვანი დებულებები. დოკუმენტის შემუ-

²⁴⁴ Cha S. -C., Yeh K. -H., A Data-Driven Security Risk Assessment Scheme for Personal Data Protection, IEEE Access, Vol. 6, 2018, 50512-50513, იხ., <<https://bit.ly/3yGceWf>> [30.06.2022].

²⁴⁵ European Data Protection: Law and Practice, edited by Ustaran E., Portsmouth, 2019, 131.

²⁴⁶ იქვე.

²⁴⁷ იქვე, 131-133.

შავება და დადგენილი წესების დაცვით მისი აღსრულებაც მნიშვნელოვნად გაამარტივებს საგანმანათლებლო დაწესებულებაში მონაცემთა უსაფრთხოების პოლიტიკის უზრუნველყოფას.

სწორედ, ამიტომ, პერსონალური მონაცემების უსაფრთხოების უზრუნველყოფის მიზნით, საგანმანათლებლო დაწესებულებებმა უნდა გამოყოფონ მონაცემთა დამუშავებასა და კანონიერებაზე/უსაფრთხოებაზე პასუხისმგებელი პირი/პირები.²⁴⁸ მათ მუდმივად უნდა უზრუნველყონ მონაცემთა დამუშავების მონიტორინგი, იყვნენ ორიენტირებულნი მონაცემთა დამუშავების კანონიერების აღსრულებასა და პროცესის მაქსიმალურად დახვეწაზე. ამ მხრივ, ასევე, საინტერესოა ევროკავშირის ქვეყნებში არსებული პრაქტიკა, როდესაც საგანმანათლებლო დაწესებულებებს ჰყავთ განსაზღვრული მონაცემთა დაცვის ოფიცრები.²⁴⁹ ხშირად ისინი მოიაზრებიან როგორც შიდა პოლიციელები,²⁵⁰ რომლებიც უწევენ მონიტორინგს პერსონალურ მონაცემთა დამუშავების პროცესში კანონმდებლობის მოთხოვნების შესრულებას, უზრუნველყოფენ დაწესებულების ინფორმირებასა და კონსულტაციას პერსონალურ მონაცემთა დაცვის კანონმდებლობისა და მისი მოთხოვნების შესახებ.²⁵¹ ასევე, განსაზღვრავენ მნიშვნელოვან პროცედურებს პერსონალურ მონაცემთა დაცვისთვის და ეხმარებიან დაწესებულებებს მათ იმპლემენტაციაში.²⁵² აღსანიშნავია ისიც, რომ გერმანიაში ასევე დადგენილია შიდა აუდიტის წესებიც, რომლებიც პერსონალურ მონაცემთა დაცვის ოფიცერს ან/და სხვა პასუხისმგებელ პირს ეხმარება პერსონალური მონაცემების დამუშავების მაღალი სტანდარტის დანერგვაში.²⁵³ რაც შეეხება საქართველოს, პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუტის საგანმანათლებლო დაწესებულებებში დანერგვა, იმის გათვალისწინებით, რომ უნივერსიტეტები ძალიან დიდი რაოდენობით პერსონალურ მონაცემებს ამუშავებენ, მხოლოდ ხელს შეუწყობს მონაცემთა უსაფრთხოების ხარისხის ამაღლებას.

ასევე, უნდა აღინიშნოს, რომ დისტანციური სწავლებისას, ხშირ შემთხვევაში, საგანმანათლებლო დაწესებულებებში მონაცემთა დამუშავება უფლებამოსილი

²⁴⁸ შპს „იუაი“ – ჩანტლაძე ტ., სულხანიშვილი ე., ცინცკილაძე გ., ჯიშიაშვილი გ., თემატური რეკომენდაციები COVID 19 პანდემიის დროს პერსონალური მონაცემების მართვაზე, ანგარიში დისტანციური სწავლებისას პერსონალურ მონაცემთა დაცვის შესახებ, 2021, 29.

²⁴⁹ < <https://bit.ly/3AlbhnR> > [25.06.2022]; < <https://bit.ly/3yCsyXZ> > [25.06.2022].

²⁵⁰ გუგავა ნ., განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დაცვის სტანდარტები საქართველოში და საერთაშორისო გამოცდილება, სადისერტაციო ნაშრომი, თბილისი, 2017, 151.

²⁵¹ Article 29 Working Party, Guidelines on Data Protection Officers, 13 December 2016, 5-9.

²⁵² იქვე.

²⁵³ Fischer P., Data Protection Audit: The German Experience, in the book: Beyond Data Protection Strategic Case Studies and Practical Guidance, edited by Noriswadi E., Lee E., Cieh Y., springer, e-book, 2013, 233-235.

პირების მეშვეობით მიმდინარეობს.²⁵⁴ შესაძლებელია, უნივერსიტეტმა დაიქირაოს პირი, ელექტრონული ჟურნალის შესაქმნელად და სამართავად, დისტანციური სწავლებისთვის საჭირო პროგრამის შესაქმნელად და სანარმოებლად, ან სხვა მომსახურების გასაწევად. თუმცა, ამ შემთხვევაში მნიშვნელოვანია, უმაღლესი საგანმანათლებლო დაწესებულება დარწმუნდეს, რომ ეს უკანასკნელი დაიცავს მონაცემთა დამუშავებისთვის დადგენილ წესებს, ვინაიდან სწორედ მას ეკისრება ვალდებულება გაითვალისწინოს, მონაცემთა კანონიერი დამუშავებისა და უსაფრთხოების შესახებ დებულებები მხარეთა შორის გაფორმებულ ხელშეკრულებაში და გაუწიოს მონიტორინგი უფლებამოსილი პირების მიერ მონაცემთა დამუშავებას, მის მიერ უსაფრთხოების ზომების მიღებას და ხელშეკრულებით გათვალისწინებული ვალდებულებების შესრულებას.²⁵⁵ ამრიგად, საგანმანათლებლო დაწესებულებამ, თუ თავად არ აქვს შექმნილი დისტანციური სწავლებისას გამოსაყენებელი პლატფორმა, წინასწარი შერჩევით, პერსონალურ მონაცემთა დაცვის პოლიტიკის გათვალისწინებით, უნდა შეარჩიოს მესამე პირის მიერ შექმნილი პლატფორმა. ხოლო, მხარეთა შორის გაფორმებული ხელშეკრულება უნდა იყოს ნათელი და სრულად უნდა იყოს გათვალისწინებული პერსონალურ მონაცემთა დაცვისთვის საჭირო რეგულაციები.

4.3. პერსონალურ მონაცემებთან დაკავშირებული ქმედებების აღრიცხვა

დამუშავებულ მონაცემთა უსაფრთხოებისთვის, აუცილებელია, რომ აღირიცხებოდეს მონაცემთა მიმართ შესრულებული ყველა ქმედება თუ ისინი ელექტრონული ფორმით არის შენახული.²⁵⁶ დისტანციური სწავლების მიმდინარეობისას, ცხადია, სტუდენტთა პერსონალური მონაცემების უდიდესი ნაწილი მუშავდება ავტომატური საშუალებით და ინახება ელექტრონულად. შესაბამისად, მონაცემთა უსაფრთხოებისთვის არსებითია, რომ ელექტრონულ სისტემას გააჩნდეს მონაცემთა მიმართ შესრულებული ნებისმიერი ქმედების აღრიცხვის შესაძლებლობა.²⁵⁷ მათ შორის, ელექტრონული ჟურნალის დათვალიერება, ელექტრონულ ჟურნალში ან ფინანსურ ბარათში შესული ცვლილება დროისა და ცვლილების

²⁵⁴ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-16 მუხლი.

²⁵⁵ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 21 აპრილის №გ-1/210/2017 გადაწყვეტილება „მ. ა.-ს განცხადებასთან დაკავშირებული განხილვის დასრულების შესახებ“.

²⁵⁶ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის მეორე პუნქტი.

²⁵⁷ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 10 მაისის №გ-1/141/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემოწმების დასრულების შესახებ“, 12.

განმახორციელებელი პირის მითითებით და ნებისმიერი სხვა პერსონალური მონაცემების ცვლილებასთან დაკავშირებული ქმედების დაფიქსირებით²⁵⁸.

აღსანიშნავია, რომ საგანმანათლებლო დაწესებულების მიერ მონაცემთა მიმართ შესრულებულ ყველა მოქმედების აღრიცხვა ხელს შეუშლის ელექტრონული ფორმით შენახული მონაცემების უკანონო მოპოვებას, გამჟღავნებას, განადგურებას ან სხვაგვარ გამოყენებას. ამასთანავე, აღრიცხვის გარეშე შეუძლებელი იქნება მონაცემთა უკანონო დამუშავების შემთხვევებში ფაქტზე ადეკვატური რეაგირება და პასუხისმგებელი პირის იდენტიფიცირებაც. ასეთი აღრიცხვა ასევე საქმეს გაუადვილებს მონაცემთა დამუშავებაზე მონიტორინგის განმახორციელებელ პირსაც და გაამარტივებს მონაცემთა დამუშავებლის მიერ ანგარიშვალდებულების პრინციპით გათვალისწინებული მოვალეობების შესრულებასაც²⁵⁹.

4.4. მონაცემთა უსაფრთხოებისთვის საჭირო დამატებითი ზომები

მონაცემთა უსაფრთხოების უზრუნველსაყოფად უმნიშვნელოვანესია, ორგანიზაციამ შეიმუშაოს შიდაორგანიზაციული სახელმძღვანელო დოკუმენტი, რომელიც განსაზღვრავს დისტანციური სწავლების პროცესში ელექტრონულ სისტემაში დაცულ მონაცემებზე წვდომის, წვდომაზე უფლების მქონე პირების უფლებამოსილებების, მონაცემთა უსაფრთხოების დაცვის, მონაცემების დამუშავების კანონიერების მონიტორინგს, გამოვლენილ დარღვევებზე ადეკვატური რეაგირების საკითხებს და სხვა მნიშვნელოვან საკითხებს.²⁶⁰ აქვე შეიძლება იყოს გათვალისწინებული სტუდენტთა მონაცემების ფსევდონიმიზაციის ან დეპერსონალიზაციის²⁶¹ გამოყენების შესაძლებლობა და სხვა კონკრეტული შემთხვევებიც. სწორედ ეს დოკუმენტი არის პირველი წინ გადადგმული ნაბიჯი იმისათვის, რომ მინიმუმამდე იქნეს დაყვანილი მონაცემთა არამართლზომიერი დამუშავება. აღნიშნული დოკუმენტის შესამუშავებლად კი მნიშვნელოვანი იქნება წინასწარვე განისაზღვროს მონაცემთა ის სახეები, რომლებსაც დაამუშავებს უმაღლესი საგანმანათლებლო დაწესებულება. ეს ემსახურება იმის დადგენასაც, თუ რა კატეგორიის მონაცემებს ამუშავებს დაწესებულება, უწევს თუ არა მას განსაკუთ-

²⁵⁸ იქვე.

²⁵⁹ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 152.

²⁶⁰ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 14 ივნისის №გ-1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემონმების დასრულების შესახებ“, 12; Decesion №ZSOŚS.421.25.2019 of The President of the Personal Data Protection Office of Poland on inspection of Warsaw University of Life Sciences (SGGW), 21 August 2020.

²⁶¹ European Data Protection: Law and Practice, edited by Ustaran E., Portsmouth, 2019, 52.

რებული კატეგორიის მონაცემების დამუშავება და რა შესაბამისი ტექნიკური ზომების მიღებაა აუცილებელი მათ დასაცავად.

ყურადსაღებია ის პროცესიც, თუ როგორ მიაწვდის და განათავსებს უნივერსიტეტი სტუდენტთა პერსონალურ მონაცემებს ელექტრონულ სერვერებზე. მაგალითისთვის, დაუშვებელია, რომ სერვერებზე შესანახად სტუდენტთა განსაკუთრებული კატეგორიის მონაცემები პირდაპირ დაუშიფრავი მეილით გაიგზავნოს.²⁶² ასევე, უმჯობესია პლატფორმაზე ავტორიზაციისას გამოყენებული პაროლები სერვერზე ინახებოდეს დაშიფრული სახით.²⁶³ მონაცემთა დაშიფვრა, რომელიც უსაფრთხოების ერთ-ერთი მთავარი მახასიათებელია,²⁶⁴ ხელს შეუწყობს მონაცემთა არამართლზომიერი დამუშავების რისკების გამორიცხვას. თუმცა, გარდა პაროლების განთავსებისა, საგანმანათლებლო დაწესებულებას შეუძლია შეიმუშაოს შესაბამისი კრიპტოგრაფიული ალგორითმები, რომლებიც მაქსიმალურად უზრუნველყოფენ მონაცემთა ანონიმიზაციას/დაშიფვრას, ორმაგ ავთენტიფიკაციას და სხვა მსგავსი ზომების მიღებას.²⁶⁵ შესაბამისად, მაშინაც, თუ ეს მონაცემები უკანონოდ აღმოჩნდება მესამე პირის ხელში, მისთვის საკმაოდ დიდ სირთულეებთან იქნება დაკავშირებული სტუდენტის პერსონალურ ანგარიშზე წვდომის მოპოვება და რაიმე ცვლილების განხორციელება.

უნდა აღინიშნოს ისიც, რომ მონაცემთა უსაფრთხოების პრინციპის უზრუნველსაყოფად, მნიშვნელოვანია არა მხოლოდ მონაცემთა დამუშავების კანონმდებლობის მცოდნე ადამიანის ორგანიზაციაში არსებობა არამედ ტექნიკური მხარდაჭერის განმახორციელებელი პირების მაქსიმალური ჩართულობაც. ვინაიდან, სწორედ მათ უნდა განსაზღვრონ, თუ რა სახის უსაფრთხოების უზრუნველყოფის და თავდაცვის სისტემას შეიმუშავენ ელექტრონულად, რათა თავიდან იქნეს აცილებული მოსალოდნელი კიბერშეტევები. მათვე უნდა შეიმუშაონ რეკომენდაციები სტუდენტებისთვის, რათა მათ შეძლონ დისტანციური სწავლების ძირითადი სისტემების უსაფრთხოდ გამოყენება. საბოლოოდ კი ზემოაღნიშნული ღონისძიებების დანერგვითა და აღსრულებით შესაძლებელი იქნება სტუდენტთა პერსონალური მონაცემების უსაფრთხოების მაქსიმალური დაცვის უზრუნველყოფა.

²⁶² Decision №DI-2019-9432 of Swedish Authority for Privacy Protection on the supervision of UMEA's university, 10 December 2020.

²⁶³ საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 10 მაისის №გ-1/141/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემონემების დასრულების შესახებ“

²⁶⁴ ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 141.

²⁶⁵ Wang X., Personal data security Technical Guide for Online Education Platforms, Moscow, 2020, 12.

IV. კვლევა საქართველოში აკრედიტებული უმაღლესი საგანმანათლებლო დაწესებულებების მიერ დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების დამუშავების თაობაზე

1. კვლევის მიზანი და მეთოდოლოგია

უმაღლესი საგანმანათლებლო დაწესებულებებისთვის ახალი საკითხი არაა სტუდენტთა პერსონალური მონაცემების დამუშავება და დაცვა. თუმცა, განათლების დისტანციური სწავლების ფორმატზე გადასვლის აუცილებლობით გამოწვეულმა პერსონალური მონაცემების დაცვის რისკების გაზრდამ, მნიშვნელოვანი გახადა, იმის გარკვევა კანონმდებლობით დადგენილი წესის შესაბამისად ახორციელებენ თუ არა უმაღლესი საგანმანათლებლო დაწესებულებები სტუდენტების პერსონალური მონაცემების დამუშავებას და რა სახის ორგანიზაციულ-ტექნიკურ ზომებს ატარებენ დამუშავებული მონაცემების დასაცავად. შესაბამისად, ჩატარებული კვლევის მიზანს წარმოადგენდა საქართველოში აკრედიტებულ უმაღლეს საგანმანათლებლო დაწესებულებებში დისტანციური სწავლებისას, სტუდენტთა პერსონალური მონაცემების დამუშავებისა და დაცვის კუთხით არსებული მდგომარეობისა და პრაქტიკის გამოკვლევა. უფრო კონკრეტულ მიზანს წარმოადგენდა შემდეგი საკითხების შესწავლა:

1. სტუდენტთა იმ პერსონალური მონაცემების დადგენა, რომლებსაც ამუშავებენ კონკრეტული უმაღლესი საგანმანათლებლო დაწესებულებები, მათ შორის დისტანციური სწავლების მეთოდის გამოყენების პირობებში;
2. კანონმდებლობით გათვალისწინებული მონაცემთა დამუშავების საფუძვლების განსაზღვრა;
3. მონაცემთა დამუშავების საშუალების დადგენა;
4. შიდასამართლებრივი აქტის (ბრძანება, ინსტრუქცია, დებულება) არსებობა, მისი კანონმდებლობასთან შესაბამისობის დადგენა და იმის შეფასება, რამდენად ასახავს დოკუმენტი დისტანციური სწავლებისას პერსონალური მონაცემების დამუშავების წესებს;
5. საგანმანათლებლო დაწესებულების იმ სტრუქტურული ერთეულის დადგენა, რომელიც ახორციელებს პერსონალურ მონაცემთა დამუშავებაზე მონიტორინგს;
6. დისტანციური სწავლების მეთოდის გამოყენების პერიოდში საგანმანათლებლო დაწესებულების მიერ ლექციის ჩანერის შესაძლებლობა,

ჩანერის მიზანი, ხელმისაწვდომობა და აღნიშნულ საკითხზე სტუდენტების მიერ გამოხატული თანხმობის არსებობა;

7. დამუშავებულ სტუდენტთა თითოეულ მონაცემთან მიმართებით შენახვის ვადის არსებობა;
8. სტუდენტთა პერსონალური, მათ შორის, დისტანციური სწავლებისას მოპოვებული მონაცემების უსაფრთხოებისთვის აუცილებელი, ადეკვატური ორგანიზაციული და ტექნიკური ზომების არსებობა;
9. პერსონალურ მონაცემთა დაცვის სამსახურის დროული ინფორმირება ფაილური სისტემის კატალოგის წარმოებასთან დაკავშირებით.

კვლევის ფარგლებში ასევე მნიშვნელოვანი იყო იმის დადგენა, თუ რა პრაქტიკა არსებობს უმაღლეს საგანმანათლებლო დაწესებულებებში განხორციელებული პერსონალურ მონაცემთა დამუშავების კანონიერების ზედამხედველობის კუთხით. ამ მიზნით, შესაბამისი კითხვარით ინფორმაცია გამოთხოვილ იქნა პერსონალურ მონაცემთა დაცვის სამსახურიდან, კერძოდ, 2013-2022 წლების, მათ შორის, დისტანციური სწავლების პერიოდში იმ შემთხვევების/განცხადებების განხილვის სტატისტიკა და გადაწყვეტილების ასლები, რომლებშიც მონაწილე მხარეს წარმოადგენდნენ უმაღლესი საგანმანათლებლო დაწესებულებები.

ასევე, კვლევის ფარგლებში, საქართველოში აკრედიტებულ 63 უმაღლეს საგანმანათლებლო დაწესებულებას (15.05.2022-ის მდგომარეობით) დაეგზავნა ჩემს მიერ შედგენილი სპეციალური კითხვარი. ამასთანავე, უნივერსიტეტებს განემარტათ, რომ გამოკითხვის შედეგების გადმოცემა მოხდებოდა მხოლოდ განზოგადებული სახით. საბოლოოდ, კვლევაში მონაწილეობა მიიღო და კითხვარი შეავსო 5-მა უმაღლესმა საგანმანათლებლო დაწესებულებამ, მათ შორისაა:

1. სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი²⁶⁶;
2. სსიპ – ილიას სახელმწიფო უნივერსიტეტი²⁶⁷;
3. სსიპ – გორის სახელმწიფო უნივერსიტეტი²⁶⁸;
4. შპს – სულხან-საბა ორბელიანის უნივერსიტეტი²⁶⁹;
5. შპს – კავკასიის საერთაშორისო უნივერსიტეტი²⁷⁰.

²⁶⁶ სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის 2022 წლის 2 ივნისის №MES 2 22 0000581982 წერილი.

²⁶⁷ სსიპ – ილიას სახელმწიფო უნივერსიტეტის 2022 წლის 24 მაისის №35/3086 წერილი.

²⁶⁸ სსიპ – გორის სახელმწიფო უნივერსიტეტის 2022 წლის 27 მაისის №MES 9 22 0000551676 და 2022 წლის 4 ივლისის № MES 6 22 0000753570 წერილები

²⁶⁹ შპს – სულხან-საბა ორბელიანის უნივერსიტეტის 2022 წლის 27 მაისის წერილი.

²⁷⁰ შპს – კავკასიის საერთაშორისო უნივერსიტეტის 2022 წლის 26 მაისის წერილი.

2. კვლევის შედეგად მიღებული პასუხები

2.1. საგანმანათლებლო დაწესებულებებისგან მიღებული პასუხები

კვლევაში მონაწილე ყველა უნივერსიტეტმა წარმოადგინა შევსებული კითხვარი და პერსონალურ მონაცემთა დამუშავების მარეგულირებელი შიდა სამართლებრივი აქტების ასლები (არსებობის შემთხვევაში). მართალია, კითხვარში დასმულ შეკითხვას თითქმის სრულად უპასუხა კითხვარის შემვსებმა ყველა მონაწილემ, მაგრამ მიღებული პასუხები გარკვეულ შემთხვევებში არასრული, ზოგადი და აბსტრაქტული შინაარსის შემცველი იყო.

2.1.1. დამუშავებული პერსონალური მონაცემები და ონლაინ ლექციების ჩანერა

მიღებული პასუხების მიხედვით, დადგინდა, რომ უნივერსიტეტები ამუშავებენ სტუდენტების ისეთ პერსონალურ მონაცემებს, როგორიცაა მათი სახელი, გვარი, მამის სახელი, დაბადების თარიღი, პირადი ნომერი, ტელეფონი, ელ-ფოსტა, ფოტოსურათი, ფაქტობრივი და იურიდიული მისამართი, სქესი, მოქალაქეობა, საშუალო საგანმანათლებლო დაწესებულება და მისი დამთავრების თარიღი, ატესტატის მონაცემები (მათ შორის, ნომერი, გაცემის თარიღი), სოციალური სტატუსი (არსებობის შემთხვევაში), ინფორმაცია მისი ჩარიცხვისა (მათ შორის, ბრძანების) და გრანტის მოპოვების შესახებ, ფაკულტეტი, საფეხური, კურსი, სემესტრი, ჯგუფი, აკადემიური მოსწრება, სწავლის საფასური, ინფორმაცია სტუდენტის სტატუსის შესახებ (მათ შორის, ბრძანების ნომერი სტუდენტის სტატუსის შეჩერების შესახებ ან სტუდენტის სტატუსის შეწყვეტის შესახებ), სტუდენტის დიპლომის და დიპლომის დანართი. რაც შეეხება დისტანციური სწავლებისას დამუშავებულ სტუდენტთა პერსონალურ მონაცემებს, კვლევაში მონაწილე ყველა უნივერსიტეტმა აღნიშნა, რომ დისტანციური სწავლებისას მათი საგანმანათლებლო დაწესებულება არ ამუშავებს მათ მიერ უკვე მითითებული მონაცემებისგან განსხვავებულ პერსონალურ მონაცემებს. მხოლოდ ერთმა უნივერსიტეტმა აღნიშნა, რომ დისტანციური სწავლებისას არ ამუშავებდა სტუდენტის პირად ნომერს, ტელეფონსა და ელ-ფოსტის მისამართს. თუმცა, ამავე უნივერსიტეტის მიერ თავის ოფიციალურ ვებ-გვერდზე გამოქვეყნებულია დისტანციური სწავლების ფორმაზე გადასვლისას უნივერსიტეტში არსებული ელექტრონულ პლატფორმაზე წვდომის მოსაპოვებლად საჭირო გზამკვლევი. უნივერსიტეტის მიერ შემუშავებულ გზამკვლევში მითითებულია, რომ სტუდენტს აუცილებლად უნდა ჰქონოდა აქტიური ელექტრონული ფოსტა, რომლის საშუალებითაც შევიდოდა ელექტრონულ პლატფორმაზე, ასევე, პლატფორმაზე არსებულ მის

პირად გვერდზე უნდა განეხილებინა ინფორმაცია ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის შესახებ.²⁷¹ გარდა ამისა, ამ უნივერსიტეტში ჩატარებული შემონმების შედეგად დადგინდა, რომ ლექციები დისტანციური სწავლებისას Google-meet-ის პროგრამის საშუალებით ტარდებოდა, რა დროსაც შეხვედრაზე დასასწრებად სტუდენტები ორგანიზატორის მიერ წინასწარ არიან მოწვეულნი მათივე ელექტრონული ფოსტის მისამართის გამოყენებით.²⁷² შესაბამისად, შეიძლება ჩაითვალოს, რომ სტუდენტთა პერსონალური მონაცემის აღნიშნული სახე, ამ უნივერსიტეტის მიერ დისტანციური სწავლების მიმდინარეობისასაც ჩვეულებრივად მუშავდებოდა. ამიტომაც, გაუგებარია, რა მიზნით მიუთითა საგანმანათლებლო დაწესებულებამ ისეთი პერსონალური მონაცემის (ელექტრონული ფოსტის მისამართი და ტელეფონის ნომერი) არდამუშავების პრაქტიკაზე, რომელსაც დისტანციური სწავლების პროცესშიც აქტიურად ამუშავებდა. შესაძლოა ეს გამომწვეული იყო იმ ფაქტით, რომ საგანმანათლებლო დაწესებულება სრულად ვერ აანალიზებდა, სტუდენტის რომელ პერსონალურ მონაცემებს ამუშავებდა დისტანციური სწავლებისას.

აქვე, უნდა აღინიშნოს, რომ კვლევაში მონაწილე მხოლოდ ერთმა საგანმანათლებლო დაწესებულებამ აღინიშნა, რომ სტუდენტის თანხმობით ამუშავებს მისი ფოტოსურათისა და დაბადების თარიღის შესახებ ინფორმაციას. დანარჩენ შემთხვევებში არ იყო ხაზგასმული მონაცემთა დამუშავებისთვის სტუდენტისაგან თანხმობის მიღების საფუძვლით მონაცემთა ამ ორი სახის დამუშავების თაობაზე. ეს, რა თქმა უნდა, უპირობოდ არ მიუთითებს იმ ფაქტზე, რომ კვლევაში მონაწილე რომელიმე სხვა დაწესებულება სტუდენტის პერსონალურ მონაცემებს სამართლებრივი საფუძვლის გარეშე ამუშავებს და საჭიროების შემთხვევაში სტუდენტისაგან თანხმობას არ იღებს, ვინაიდან სტუდენტის მხოლოდ სახელისა და გვარის დამუშავება არ არის საკმარისი მისი იდენტიფიკაციისათვის. თუმცა, სტუდენტის დაბადების თარიღისა და ფოტოსურათის დამუშავება მის პირად ნომერთან ერთად, მხოლოდ სტუდენტის ვინაობის დადგენის მიზნით, ვერ იქნება მიზნის მიღწევის პროპორციული საშუალება, ვინაიდან თითოეული ადამიანის პირადი ნომერი უნიკალურია და მას იდენტიფიკაციისთვის სხვა დამატებითი მონაცემის დამუშავება არ ესაჭიროება. სწორედ ამიტომ, ამ უნივერსიტეტის მიერ, დაბადების თარიღისა და ფოტოსურათის დამუშავებისას, სტუდენტთა ნებასა და გამოხატულ თანხმობაზე ყურადღების გამახვილება, საკმაოდ დადებითად უნდა შეფასდეს.

²⁷¹ < <https://bit.ly/3RbUYPC> > [01.07.2022].

²⁷² საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 10 მაისის №გ-1/141/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემონმების დასრულების შესახებ“.

ასევე, უნდა აღინიშნოს, რომ კვლევაში მონაწილე უნივერსიტეტები თითქოს ცოტაოდენი შიშით ეპყრობიან დისტანციური სწავლებისას მიმდინარე ლექციების აუდიო-ვიდეო ჩანერის საკითხს, რომელიც ცალსახად არ არის პერსონალური მონაცემების უკანონო დამუშავების მაგალითი. კვლევის შედეგად დადგინდა, რომ მხოლოდ ორი საგანმანათლებლო დაწესებულება იწერდა სინქრონულ რეჟიმში მიმდინარე ლექციებს. ორივე შემთხვევაში ჩანერა მიმდინარეობდა სტუდენტების თანხმობით, რომელიც ზეპირი ფორმით იყო გამოხატული ლექციის დასაწყისშივე, მიმდინარე შეხვედრის ჩანანერის გასაკეთებლად. ორივე შემთხვევაში, ლექციების ჩანანერი ხელმისაწვდომი იყო მხოლოდ იმ სალექციო კურსზე დარეგისტრირებული სტუდენტებისთვის, შესაბამისი პლატფორმის მეშვეობით. თუმცა, მხოლოდ ერთ შემთხვევაში იყო განსაზღვრული სალექციო ჩანანერების ხელმისაწვდომობის ვადა, რომელიც სტუდენტებისათვის მხოლოდ იმ კურსის ფარგლებში მიმდინარე სემესტრის განმავლობაში იყო ხელმისაწვდომი. ამასთანავე, ამ ორიდან არცერთ შემთხვევაში, საგანმანათლებლო დაწესებულებას არ აღუნიშნავს, რომ დისტანციური სწავლების მიმდინარეობისას ამუშავებდნენ სტუდენტის ვიზუალურ გამოსახულებასა და ხმას.

დასკვნის სახით შესაძლოა ითქვას, რომ საგანმანათლებლო დაწესებულებებმა რამდენიმე შემთხვევაში არასრულად მიუთითეს იმ მონაცემებზე, რომელსაც ისინი ამუშავებდნენ. თუმცა, კვლევის ინტერესის საგანს არა ზოგადად ყველა მონაცემის აღნიშვნა, არამედ დისტანციური სწავლებისას დამუშავებული პერსონალური მონაცემების კონკრეტული სახეების განხილვა წარმოადგენდა. ამ მხრივ კი, მხოლოდ ერთმა საგანმანათლებლო დაწესებულებამ მიუთითა დისტანციური სწავლებისას სტუდენტის ელექტრონული ფოსტის მისამართის არდამუშავების პრაქტიკაზე, რაც თავისთავად ეწინააღმდეგება დისტანციური სწავლების მართვის პროცესს, მით უფრო, რომ ეს საგანმანათლებლო დისტანციური სწავლებისას დაწესებულება იყენებდა ისეთ პლატფორმას, რომლის მეშვეობითაც სტუდენტის პლატფორმაზე დაშვების საფუძველს მის მიერ ელექტრონული ფოსტის მისამართის გამოყენება წარმოადგენდა, ამასთანავე, სტუდენტის ვიზუალური გამოსახულებისა და ხმის დამუშავების შესახებ მონაცემების დამუშავებაზე არ მიუთითა ორმა დაწესებულებამ, მიუხედავად იმ ფაქტისა, რომ ისინი ონლაინ შეხვედრების (ლექციების) აუდიო/ვიდეო ჩანერას ახორციელებდნენ. აღნიშნულის გათვალისწინებით, კი გამოიკვეთა, რომ კვლევაში მონაწილე უნივერსიტეტებს სწავლების დისტანციური ფორმის განხორციელებისას შესაძლოა ბოლომდე არ ჰქონდათ გააზრებული იმ პერსონალური მონაცემების კონკრეტული სახეების შესახებ ინფორმაცია, რომელსაც ამუშავებდნენ. მაშინ, როცა დისტანციური სწავლებისას სტუდენტთა დამუშავებული

პერსონალური მონაცემების სახეების, მიზნებისა და ფარგლების განსაზღვრა პირველი ნაბიჯია მათი დაცვის უზრუნველყოფისა და კანონიერად დამუშავებისთვის.

2.1.2. მონაცემთა დამუშავების საშუალება და სამართლებრივი საფუძვლები

უნდა აღინიშნოს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება ვრცელდება „საქართველოს ტერიტორიაზე ავტომატური და ნახევრად ავტომატური საშუალებებით მონაცემთა დამუშავებაზე, ასევე არაავტომატური საშუალებებით იმ მონაცემთა დამუშავებაზე, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შეტანის მიზნით მუშავდება“.²⁷³ ხოლო მონაცემთა დამუშავებელია ის საჯარო დაწესებულება, ფიზიკური თუ იურიდიული პირი, რომელიც ინდივიდუალურად ან სხვებთან ერთად, უშუალოდ ან სხვა უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას, განსაზღვრავს მათი დამუშავების მიზნებსა და საშუალებებსაც.²⁷⁴ ვინაიდან, უმაღლესი საგანმანათლებლო დაწესებულება ნებისმიერ შემთხვევაში არის საჯარო სამართლის იურიდიული პირი ან „მენარმეთა შესახებ“ საქართველოს კანონის შესაბამისად შექმნილი იურიდიული პირი, რომელიც ამუშავებს, სტუდენტთა პერსონალურ მონაცემებს, ამასთან, განსაზღვრავს მათი დამუშავების მიზნებსა და საშუალებებს. კანონმდებლობის შესაბამისად, ის არის მონაცემთა დამუშავებელი. კვლევის ფარგლებში, იმის დასადგენად, ვრცელდებოდა თუ არა უმაღლეს საგანმანათლებლო დაწესებულებაზე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება, კითხვარი ითვალისწინებდა კითხვას, რომელი საშუალებით (ავტომატური, ნახევრად ავტომატური თუ არაავტომატური საშუალებით) ამუშავებდა საგანმანათლებლო დაწესებულება სტუდენტების პერსონალურ მონაცემებს. მიღებული პასუხების მიხედვით დადგინდა, რომ ორი უნივერსიტეტი მონაცემებს ამუშავებს სამივე (ავტომატური, ნახევრად ავტომატური და არაავტომატური) საშუალებით, ორი მხოლოდ ავტომატური საშუალებით, ხოლო ერთმა უნივერსიტეტმა, ავტომატური დამუშავების მნიშვნელობის არცოდნის გამო, ვერ მიუთითა, რომელ საშუალებას იყენებდა სტუდენტთა პერსონალური მონაცემების დასამუშავებლად. თუმცა, ამ უკანასკნელმა კითხვარში ერთ-ერთ პასუხად მიუთითა, რომ უნივერსიტეტში შექმნილი აქვთ ფაილური სისტემა, სტუდენტთა და პერსონალის პირადი ინფორმაციის დამუშავებაზე. შესაბამისად, იმ შემთხვევაშიც კი, თუ ისინი არაავტომატური საშუალებებით

²⁷³ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის პირველი პუნქტი.

²⁷⁴ იქვე, „ი“ ქვეპუნქტი.

ბებით ამუშავებენ სტუდენტების პერსონალურ მონაცემებს, ფაილური სისტემის კატალოგის წარმოებით და პერსონალურ მონაცემთა დაცვის აპარატისთვის მისი წარდგენის აღნიშვნით, ქმნიან საფუძველს, ვივარაუდოთ, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება კვლევაში მონაწილე ყველა უმაღლეს საგანმანათლებლო დაწესებულებაზე ვრცელდება.

უნდა აღინიშნოს, რომ ნებისმიერ შემთხვევაში მონაცემთა კანონიერად დამუშავებისთვის აუცილებელია, მონაცემთა დამმუშავებელი აკმაყოფილებდეს საქართველოს კანონმდებლობით გათვალისწინებული სამართლებრივი საფუძველბიდან ერთ-ერთს მაინც.²⁷⁵ ამასთანავე, შესაძლებელია, რომ უნივერსიტეტების მიერ მუშავდებოდეს სტუდენტთა განსაკუთრებული კატეგორიის პერსონალური მონაცემებიც, რომელთა დამუშავება, გამონაკლისი შემთხვევების გარდა, დაუშვებელია.²⁷⁶ მოცემული საკითხების გათვალისწინებით, უნივერსიტეტებისათვის დაგზავნილი კითხვარი შეიცავდა კითხვას, მონაცემთა დამუშავებისათვის კანონმდებლობით გათვალისწინებული საფუძველების მითითების თაობაზე. თუმცა, აღნიშნულ კითხვაზე ერთმა უნივერსიტეტმა მიუთითა, რომ მათ წინასწარ აქვს განსაზღვრული სტუდენტთა პერსონალური მონაცემები, რომლებსაც ისინი დაამუშავებენ. აღნიშნული მონაცემების დამუშავების საფუძველად კი მითითებულია კანონმდებლობით დადგენილი საფუძველი, ხოლო იმ პერსონალურ მონაცემებს, რომლის დამუშავების საფუძველები არ არის კანონით განკარგული, უნივერსიტეტი ამუშავებს მონაცემთა სუბიექტის თანხმობით. კვლევაში მონაწილე დანარჩენი საგანმანათლებლო დაწესებულებები შემოიფარგლნენ ზოგადი პასუხით და მიუთითეს საკანონმდებლო აქტების დასახელებები და თავიანთი შიდაორგანიზაციული დოკუმენტები, რომელთა საფუძველზეც ისინი სტუდენტების პერსონალურ მონაცემებს ამუშავებდნენ. მათ შორის, მიუთითეს საქართველოს ზოგად ადმინისტრაციულ კოდექსზე, „პერსონალურ მონაცემთა დაცვის შესახებ“ და „უმაღლესი განათლების შესახებ“ საქართველოს კანონებზე და ერთ შემთხვევაში ასევე მითითებული იყო „სხვა კანონქვემდებარე აქტებიც“.

უნივერსიტეტების მიერ გამოგზავნილი შიდა ორგანიზაციული დოკუმენტების ტექსტის ანალიზი ცხადყოფს, რომ პერსონალურ მონაცემთა დაცვის შესახებ დებულებები, ძირითად შემთხვევაში, კანონმდებლობის ანალოგს წარმოადგენს. დოკუმენტებში, იმის ნაცვლად, რომ დეტალურად ჰქონდეთ განკარგული თავიანთ საგანმანათლებლო დაწესებულებაში არსებული შიდა პოლიტიკა, მხოლოდ კანონმდებლობით გათვალისწინებული ნორმების ამოკითხვაა შესაძლებელი. ეს

²⁷⁵ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაცია, პერსონალური მონაცემების დაცვა – გზამკვლევი დამწყები ბიზნესისათვის, 2018, 6-7.

²⁷⁶ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის პირველი და მე-2 პუნქტები.

უკანასკნელი, კი ისედაც სავალდებულო ხასიათისაა და მათი მოქმედება ვრცელდება დისტანციური სწავლისას პერსონალურ მონაცემთა დამუშავების კანონიერად უზრუნველყოფისთვის. რა თქმა უნდა, არ შეიძლება სრულად გამოირიცხოს მსგავსი თეორიული ნაწილების უნივერსიტეტების დებულებებში ასახვა. თუმცა, მხოლოდ ზოგადი ხასიათის ნორმებით და ასევე ზოგადად საკანონმდებლო აქტების ჩამონათვალის მითითებით, რთულია იმის დადგენა კანონიერია თუ არა ის საფუძვლები რასაც უნივერსიტეტი სტუდენტთა მონაცემების დამუშავებისთვის იყენებს. მაგალითად, არცერთ შემთხვევაში კონკრეტულად არ იყო განსაზღვრული, რომ დისტანციური სწავლებისას ლექციების ჩაწერისთვის სტუდენტის თანხმობა უნდა გათვალისწინებულიყო, ან ის ფაქტი, რომ დაუშვებელია სტუდენტის მიერ დისტანციური სწავლებისას პროგრამაში კინობითი ან სხვა სახელის მითითება, ვინაიდან სტუდენტი სახელისა და გვარის დამუშავება ემსახურება მისი იდენტიფიკაციის მიზანს და აუცილებელია საგანმანათლებლო დაწესებულებისთვის მასზე დაკისრებული მოვალეობების შესასრულებლად. ცხადია, წარმოდგენილია ყოველ კონკრეტულ შემთხვევაში სტუდენტთა ყველა პერსონალური მონაცემის დამუშავების საფუძვლის წინასწარ გამოვლენა. თუმცა, კანონმდებლობის მხოლოდ ჩამონათვალის მითითებით, უნივერსიტეტის მიერ მონაცემთა დამუშავების საფუძვლების კანონიერების შეფასებაც შეუძლებელია. აღსანიშნავია, რომ რაც უფრო მეტად კონკრეტულად იქნება განსაზღვრული სტუდენტის პერსონალური მონაცემების დამუშავების სახეები და საფუძვლები, მონაცემთა დამუშავების პროცესი იქნება უფრო გამჭვირვალე და მონაცემთა სუბიექტიც მეტად ინფორმირებული, მისი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით. გასათვალისწინებელია ისიც, რომ საგანმანათლებლო დაწესებულებამ შეიძლება თავიდანვე ამომწურავად ვერ განსაზღვროს ყველა პერსონალური მონაცემის სახე, რომელსაც დაამუშავებს, რადგან შესაძლოა სწავლების პროცესში შემხვედრი გარემოებების საპასუხოდ ახალი სახეობის მონაცემის დამუშავება გახდეს საჭირო. თუმცა, სავსებით შესაძლებელია, რომ წინასწარ განისაზღვროს ის მონაცემები, რომლებსაც დაწესებულებები მუდმივად ამუშავებენ და რასაც ადასტურებს კიდევ ერთ-ერთი უნივერსიტეტის პრაქტიკა, სადაც შიდა დოკუმენტით სხვა დებულებებთან ერთად განსაზღვრულია, რომ არასრულწლოვან პირთა მონაცემებს უნივერსიტეტი მხოლოდ კანონიერი წარმომადგენლის თანხმობის საფუძველზე დაამუშავებს, ასევე ის, რომ მონაცემები შეიძლება დამუშავდეს პლაგიატის პრევენციისა და მისი გამოვლენის მიზნით და ა.შ.

დასკვნის სახით შეიძლება ითქვას, რომ ზოგად საკანონმდებლო აქტებზე მითითებით შესაძლოა, უნივერსიტეტებმა თავი აარიდეს კონკრეტული პასუხის

გაცემას, რამაც შეიძლება გვაფიქრებინოს, რომ ისინი სათანადოდ ვერ აღიქვამენ იმ ფაქტს, რომ წარმოადგენენ მონაცემთა დამმუშავებლებს, და მათზე დაკისრებულ მოვალეობებს მოქმედი კანონმდებლობის დაცვით უნდა ახორციელებდნენ. ამდენად, უარყოფითად უნდა შეფასდეს კვლევაში მონაწილე უნივერსიტეტების უმრავლესობის მიერ დაფიქსირებული ზოგადი პასუხები და მათსავე დოკუმენტებში კონკრეტულის მოკლებული პასუხები. დაუშვებელია უნივერსიტეტებმა პირდაპირ ჩათვალონ, რომ სამართლებრივი საფუძვლის გარეშე სტუდენტთა პერსონალური მონაცემების დამუშავება, დაკისრებული მოვალეობების შესრულების მიზნით მათთვის ავტომატურად ნებადართულია.

2.1.3. პერსონალურ მონაცემთა დამუშავების მარეგულირებელი მიდორგანიზაციული დოკუმენტის არსებობა

უმაღლესი საგანმანათლებლო დაწესებულებები საკმაოდ დიდი რაოდენობით პერსონალურ მონაცემებს ამუშავებენ და შესაძლოა საკმაოდ მსხვილ დამმუშავებლებად ჩაითვალონ. მიუხედავად არსებული საკანონმდებლო ნორმებისა, უმჯობესი იქნება, თუკი ორგანიზაციას ექნება შიდასამართლებრივი აქტი, რომლითაც განსაზღვრული იქნება უმაღლეს საგანმანათლებლო დაწესებულებაში პერსონალური მონაცემების დამუშავება/დაცვის წესები, მათ შორის, დისტანციური სწავლების წარმართვის პროცესში. აღნიშნული ორგანიზაციებს მისცემს შესაძლებლობას თავიდან აირიდონ მონაცემთა არამიზნობრივი და არაპროპორციული დამუშავება. შესაბამისად, უმაღლესი საგანმანათლებლო დაწესებულებისთვის დაგზავნილი დოკუმენტი შეიცავდა კითხვას იმის თაობაზე, არსებობდა თუ არა მათ დაწესებულებაში პერსონალურ მონაცემთა დამუშავების მარეგულირებელი რაიმე შიდა სამართლებრივი აქტი (ბრძანება, ინსტრუქცია, დებულება)? ასეთის არსებობის შემთხვევაში კი, ასახავდა თუ არა ეს დოკუმენტი დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების დამუშავების წესებს. უნივერსიტეტებიდან მიღებული პასუხების მიხედვით გამოიკვეთა რომ, პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტი შემუშავებული აქვს კვლევაში მონაწილე ორ უნივერსიტეტს. ერთი დოკუმენტი ასახავს საკანონმდებლო ნორმებს თუ რა პრინციპებზე დაყრდნობით უზრუნველყოფს უნივერსიტეტი პერსონალური მონაცემების დამუშავებას, მონაცემთა დამუშავების საფუძვლებს, მონაცემთა გამჟღავნების და მესამე პირთათვის გადაცემის და მათი დაცვის საკითხებს, ფაილური სისტემის კატალოგის წარმოების წესს და პერსონალურ მონაცემთა დაცვის ინსპექტორისთვის შეტყობინების საკითხს, პერსონალისა და სტუდენტის პასუხისმგებლობის საკითხს და ასევე მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდების წესს. ხოლო მეორე დოკუმენტში პერსონალურ მონაცემთა დაცვის წესები საქართველოს კანონმდებლო-

ბით დადგენილი ნორმების ანალოგიურია. ამასთანავე, ორივე უნივერსიტეტის მიერ განსაზღვრულია იმ პირთა/დეპარტამენტთა ჩამონათვალი, რომლებსაც სტუდენტების პერსონალურ მონაცემებზე აქვთ წვდომა. სამუხაროდ, მხოლოდ ერთი უნივერსიტეტის შემთხვევაშია დადგენილი მონაცემთა შენახვის ვადები.

უნდა აღინიშნოს, რომ მოცემული დოკუმენტები არ ასახავენ განცალკევებით დისტანციური სწავლებისას პერსონალური მონაცემების დამუშავების წესს. ერთ-ერთი უნივერსიტეტის მითითებით, ისინი ხელმძღვანელობენ სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციის შესაბამისად („პერსონალური მონაცემების დამუშავება დისტანციური სწავლების პროცესში“). აღსანიშნავია, რომ აღნიშნულ უნივერსიტეტში სწავლა მიმდინარეობდა ჰიბრიდულ რეჟიმში, რა დროსაც ლექციების აუდიო/ვიდეო ჩანერა 2019-2020 წლის გაზაფხულის სემესტრიდან 2021-2022 წლის გაზაფხულის სემესტრამდე მიმდინარეობდა, რათა სტუდენტებისთვის ჩანაწერი ყოფილიყო ხელმისაწვდომი, ასინქრონულ რეჟიმშიც. მართალია, პერსონალურ მონაცემთა დაცვის სამსახური დასაშვებად მიიჩნევს ასეთი ჩანაწერების განხორციელების შესაძლებლობას, თუმცა არ იძლევა კონკრეტულ მითითებას, რა ვადით უნდა იყოს ისინი ხელმისაწვდომი. საგანმანათლებლო დაწესებულებას კი, ასეთი ჩანაწერის შენახვის ვადა მათ მიერ მითითებული დოკუმენტით არ აქვთ გათვალისწინებული. ამასთანავე, უნივერსიტეტის მიერ დასახელებული რეკომენდაციები სახელმწიფო ინსპექტორის აპარატის მიერ შემუშავებულია 2022 წლის 20 იანვარს. არსებობს, კიდევ ერთი რეკომენდაცია, რომელიც მომზადებულია შპს „იუაი“-ს მიერ „ეი არ დი ინკისთვის“, დემოკრატიული მმართველობის ინიციატივა (GGI) 2021 წლის 11 ოქტომბერს, რომელიც სახელმწიფო ინსპექტორის მიერ გაცემული რეკომენდაციის შინაარსის მსგავსად მსჯელობს ზემოაღნიშნულ საკითხზე. შესაბამისად, მაშინ, როდესაც უნივერსიტეტმა დაიწყო პრაქტიკაში ლექციების აუდიო/ვიდეო ჩანერა და ამ გზით სტუდენტთა განსხვავებული პერსონალური მონაცემების დამუშავება (2020 წლიდან) მათ შიდაორგანიზაციულ დოკუმენტში არ ჰქონდათ განსაზღვრული ნორმები/წესები მსგავსი მონაცემების დამუშავების შესახებ. მოცემულ შემთხვევაში მითითება ერთი წლის შემდეგ გამოქვეყნებულ რეკომენდაციებზე არარელევანტურია. თუმცა, აღნიშნული ფაქტი *a priori* არ განსაზღვრავს, რომ მოცემული საგანმანათლებლო დაწესებულება არღვევდა პერსონალური მონაცემების დამუშავების წესებს და მოცემული საკითხი სხვა კომპონენტებთან ერთად კუმულაციურად განხილვით უნდა იქნეს გამოკვლეული.

კვლევაში მონაწილე ერთი უნივერსიტეტის შემთხვევაში, პერსონალურ მონაცემთა დამუშავების წესი გათვალისწინებულია შინაგანანესით, თუმცა იგი

მოიცავს მხოლოდ ზოგად დებულებებს (რომელი მონაცემები მუშავდება და რომელი სტრუქტურული ერთეული ამუშავებს მათ). ამ შინაგანანესით არ არის დადგენილი მათი დამუშავების საფუძვლები, შენახვის ვადები, დაცვის მიზნით განხორციელებული ქმედებები და სხვა საკითხები. არამედ, დოკუმენტში გვხვდება მითითება მხოლოდ მონაცემთა დაცვის კანონმდებლობის დაცვის აუცილებლობაზე. ასევე, უნივერსიტეტის შინაგანანესი არ შეიცავდა პერსონალურ მონაცემთა დამუშავების წესებს, დისტანციური სწავლების მიმდინარეობისას, თუმცა, აღსანიშნავია, რომ მათ შემუშავეს ელექტრონული სწავლების წესი, რომელშიც მითითებულია ელექტრონული სწავლების პროცესში პერსონალური მონაცემების დამუშავების პრინციპებისა და დაცვის აუცილებლობაზე.

უნდა აღინიშნოს ისიც, რომ კვლევაში მონაწილე ერთ-ერთ უნივერსიტეტში არ არსებობს პერსონალურ მონაცემთა დამუშავების, მათ შორის, დისტანციური სწავლების ფარგლებში მონაცემების დამუშავებისთვის რაიმე შიდამარეგულირებელი აქტი. მათ შორის, არც შინაგანანესი მოიცავს დებულებას პერსონალურ მონაცემთა დამუშავებისა და დაცვის მარეგულირებელ საკითხებთან დაკავშირებით. შესაბამისი შიდაორგანიზაციული დოკუმენტი არც მეხუთე უნივერსიტეტში არ არის განსაზღვრული, თუმცა მათი მითითებით, საკითხის მარეგულირებელი დებულებები გათვალისწინებული აქვთ სტუდენტებთან გაფორმებულ ხელშეკრულებებში, ასევე სხვადასხვა მარეგულირებელი საკითხები ნორმების სახით ჩანერილია უნივერსიტეტის წესებსა და ინსტრუქციებში. ამასთანავე, დისტანციური სწავლებისას მონაცემების დამუშავების შესახებ ცალკე დოკუმენტი უნივერსიტეტს არ შეუმუშავებია.

დასკვნის სახით შეიძლება ითქვას, რომ არცერთ შემთხვევაში არ არის განსაზღვრული დისტანციური სწავლების პროცესში მონაცემთა დამუშავებასთან დაკავშირებული საკითხები, მათ შორის აუდიტორული სწავლებისგან განსხვავებული მონაცემების დამუშავების შემთხვევაში, მათი შენახვის ვადები, გამოვლენილ დარღვევებზე რეაგირების ფორმები და სხვა მნიშვნელოვანი საკითხები. მხოლოდ ერთ შემთხვევაში, მონაცემთა დაცვის პოლიტიკის დოკუმენტი ითვალისწინებს, რომ პერსონალური მონაცემების დამუშავების შესახებ დადგენილი წესების დარღვევა არის უნივერსიტეტის პერსონალის მიმართ დისციპლინური დევნის დაწყების საფუძველი. აღნიშნული კი გვაძლევს იმის ვარაუდის საფუძველს, რომ ძირითად შემთხვევებში კვლევაში მონაწილე უნივერსიტეტებს უჭირთ, ან საჭიროდ არ მიიჩნევენ პოლიტიკის დოკუმენტებში განსაზღვრონ დისტანციური სწავლების პროცესში დამუშავებული პერსონალური მონაცემების დაცვის მიზნით კონკრეტული დებულებები.

2.1.4. სტუდენტთა პერსონალური მონაცემების შენახვის ვადა და მონიტორინგი მონაცემების დამუშავება/დაცვაზე

საქართველოს კანონმდებლობა ადგენს წესებს, პრინციპებს, საფუძვლებსა და უსაფრთხოების ზომებს, რომელთა დაცვაც აუცილებელია ფიზიკური პირების მონაცემების დამუშავებისას. იმისთვის, რომ მონაცემები კანონიერად დამუშავდეს, მხოლოდ საფუძვლის არსებობა საკმარისი არ არის და აუცილებელია კონკრეტული პრინციპების დაცვა. მათ შორის, დადგენილია რომ პერსონალური მონაცემები უნდა ინახებოდეს კანონით განსაზღვრული ვადით ან იმ ვადით, რაც აუცილებელია მიზნის მისაღწევად. მიზნის მიღწევის შემდეგ, ისინი უნდა წაიშალოს, ან შეინახოს პირის იდენტიფიცირების გამომრიცხავი ფორმით. შესაბამისად, საგანმანათლებლო დაწესებულებს დაესვათ კითხვა დისტანციური სწავლებისას დამუშავებული პერსონალური მონაცემების ვადებთან დაკავშირებით. უნივერსიტეტებმა აღნიშნეს, რომ ისინი დისტანციური სწავლებისას განსხვავებულ პერსონალურ მონაცემებს არ ამუშავებენ. კვლევაში მონაწილე ორმა უნივერსიტეტმა, მიუთითა, რომ სტუდენტთა დამუშავებულ პერსონალურ მონაცემებს ისინი უვადოდ ინახავენ. ერთ უნივერსიტეტს ბრძანებით აქვს წინასწარ განსაზღვრული მონაცემთა შენახვის ვადა თითოეულ შემთხვევაში, რომელიც განსხვავებულია პერსონალური მონაცემების მიხედვით. აღსანიშნავია, რომ კვლევაში მონაწილე მეოთხე უნივერსიტეტის მიერ მონაცემთა შენახვის ერთიანი – 25 წლიანი ვადაა დადგენილი. კვლევაში მონაწილე კიდევ ერთი უნივერსიტეტის მითითებით კი, მონაცემები ინახება მხოლოდ გონივრული ვადით, რაც განისაზღვრება რექტორის ბრძანებით, კონკრეტულ შემთხვევაში. კვლევაში მონაწილე უნივერსიტეტების მიდგომა ზოგიერთ შემთხვევაში პერსონალური მონაცემების აშკარა დარღვევაზე მიუთითებს, რადგან დაუშვებელია სტუდენტების პერსონალური მონაცემების უვადოდ შენახვა. ამასთანავე, ნაკლებ სავარაუდოა, რომ სტუდენტების ყველა პერსონალური მონაცემის შენახვისათვის ერთნაირი ვადა იყოს გონივრული და პროპორციული. მნიშვნელოვანია, უნივერსიტეტებს დაენერგათ ინდივიდუალური მიდგომა თითოეულ მონაცემთან მიმართებითაც. ამიტომაც, დადებითად უნდა შეფასდეს კვლევაში მონაწილე ორი უნივერსიტეტის მიერ ასეთი პრაქტიკის დანერგვა. ამასთანავე, უნდა აღინიშნოს, რომ ჩვენი კვლევის საგანს არ წარმოადგენს გონივრული ვადების განსაზღვრა ყველა ტიპის სტუდენტის პერსონალურ მონაცემთან მიმართებით.

ამასთანავე, კვლევაში მონაწილე არცერთი საგანმანათლებლო დაწესებულების შიდა ორგანიზაციული დოკუმენტი არ მოიცავს წესებს მონაცემთა განადგურებისა და დაარქივების თაობაზე.

საქართველოს კანონმდებლობა ორგანიზაციას ავალდებულებს მონიტორინგი გაუწიოს უფლებამოსილი პირის მიერ მონაცემთა დამუშავებას. თუმცა, კანონმდებლობით არ არის განსაზღვრული, რომ აუცილებელია ამისთვის ცალკე სტრუქტურული ერთეულის არსებობა ორგანიზაციის შიგნით. კვლევის შედეგად დადგინდა, რომ საგანმანათლებლო დაწესებულებებში არ არსებობს ცალკე სტრუქტურული ერთეული, რომელიც პერსონალურ მონაცემთა დამუშავებაზე მონიტორინგს ახორციელებს. აღნიშნული ფუნქცია შეთავსებული აქვს ძირითადად იურისტს/იურიდიულ სამსახურს. ერთ უნივერსიტეტში აღნიშნული ფუნქცია ასევე შეთავსებული აქვს პერსონალის მართვის და მონიტორინგის სამსახურს. კვლევაში მონაწილე ერთ-ერთ უნივერსიტეტის მითითებით აღნიშნული ფუნქცია მინიჭებული აქვს მხოლოდ საინფორმაციო ტექნოლოგიების უზრუნველყოფის განყოფილებას. ხოლო ერთ-ერთმა საგანმანათლებლო დაწესებულებამ არ მიუთითა იმ სტრუქტურის ან თანამდებობის პირის დასახელება, რომელიც მონაცემთა დამუშავების მონიტორინგის ფუნქციას შეითავსებდა. შესაბამისად, კვლევის შედეგად დადგინდა რომ იურიდიული სამსახურის გარდა პერსონალურ მონაცემთა დამუშავებაზე მონიტორინგს ახორციელებენ სხვა პირებიც, რომლებიც ნაკლებად სავარაუდოა, რომ კარგად იცნობდნენ პერსონალურ მონაცემთა დაცვის კანონმდებლობას. მაგალითად, რთულად წარმოსადგენია, რომ საინფორმაციო ტექნოლოგიების უზრუნველყოფის განყოფილების თანამშრომლები ისეთივე წარმატებით ერკვეოდნენ ამ საკითხებში, როგორც შესაბამისი დარგის სპეციალისტი. ამიტომაც, ეჭვქვეშ დგება კვლევაში მონაწილე უნივერსიტეტებში ჩატარებული მონიტორინგის ეფექტურობის საკითხი. მონაწილეების მიერ დაფიქსირებული პასუხების მიხედვით, შეიძლება ვივარაუდოთ, რომ კვლევაში მონაწილე ზოგიერთ დაწესებულებაში მონიტორინგი მხოლოდ ფორმალურ ხასიათს ატარებს და მონაცემთა დამუშავების პროცესის დახვეწისთვის შედეგიანი ვერ იქნება.

2.1.5. მონაცემთა დაცვისათვის განხორციელებული ორგანიზაციულ-ტექნიკური ზომები

გარდა იმისა, რომ მონაცემები უნდა დამუშავდეს კანონმდებლობით დადგენილი წესების შესაბამისად, საქართველოს კანონმდებლობა განსაზღვრავს მონაცემთა დამუშავებლის ვალდებულებას, მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისგან, შეცვლისგან, გამჟღავნებისგან, მოპოვებისგან ან ნებისმიერი სხვა ფორმით უკანონო გამოყენებისგან. ასევე შემთხვევითი ან უკანონო დაკარგვისგან.²⁷⁷ მართალია, რთულია გამოვლინდეს უსაფრთხოე-

²⁷⁷ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის პირველი პუნქტი.

ბის სტანდარტის დამდგენი ყველა საშუალება, ვინაიდან სხვადასხვა სახისა და მოცულობის მონაცემებს განსხვავებული უსაფრთხოების სისტემა ესაჭიროებათ. თუმცა ნაშრომში უკვე განხილულია რამდენიმე მნიშვნელოვანი საკითხი, რომლებიც ასეთი უსაფრთხოების შექმნისთვის აუცილებელია.

უმაღლეს საგანმანათლებლო დანესებულებებში სტუდენტების პერსონალური მონაცემების დაცვისთვის მიღებული ორგანიზაციულ-ტექნიკური ზომების გამოსაკვლევად, დაგზავნილი კითხვარი აღნიშნულ საკითხთან დაკავშირებულ კითხვასაც შეიცავდა. უნივერსიტეტებისგან მიღებული პასუხებით დადგინდა, რომ კვლევაში მონაწილე ყველა უნივერსიტეტში სტუდენტთა პერსონალური მონაცემების უსაფრთხოების უზრუნველსაყოფის მიზნით, მკაცრად არის შეზღუდული იმ პირების სია, ვისაც ხელი მიუწვდება ამგვარ პერსონალურ ინფორმაციაზე. ამასთანავე, ერთ-ერთმა უნივერსიტეტმა აღნიშნა, რომ მიღებული აქვთ ტექნიკური ზომები და ბაზებზე მხოლოდ ავტორიზებული წვდომაა დაშვებული. ერთი უნივერსიტეტის მითითებით, ელექტრონულ ჟურნალში ყველა სტუდენტს აქვს თავისი ელექტრონული გვერდი და ის ხედავს მხოლოდ თავის მონაცემებს, ხოლო ლექტორები ხედავენ მხოლოდ თავიანთ ჯგუფებს და სტუდენტებს მათი პირადი ნომრების გარეშე.

კვლევაში მონაწილე ორ უნივერსიტეტში, შესაბამისი სტრუქტურული ერთეული „ინფორმაციული ტექნოლოგიების სამსახური“ უზრუნველყოფს მონაცემების უსაფრთხოების დაცვას. ხოლო, ერთ-ერთის მითითებით, თუ სტუდენტების მონაცემებს ამუშავებს უფლებამოსილი პირი, მაშინ მასთან დადებული აქვთ შესაბამისი ხელშეკრულება პერსონალური მონაცემების დაცვის გარანტიების შესახებ.

ასევე უნდა აღინიშნოს, რომ კვლევაში მონაწილე ერთმა უნივერსიტეტმა წარმოადგინა ინფორმაციული ტექნოლოგიების მართვის დოკუმენტი, რომლის მიხედვითაც ინფორმაციული ტექნოლოგიების განყოფილება პასუხისმგებელი მონაცემთა უსაფრთხოების დაცვისთვის ეფექტური მექანიზმის შექმნაზე, ინფორმაციული საფრთხის შემცველ ინციდენტზე რეაგირებასა და მართვაზე. მეორე უნივერსიტეტი, რომელსაც ასევე აქვს შემუშავებული ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დოკუმენტი, არ მოიცავს პერსონალურ მონაცემთა დამუშავებისა და დაცვის მარეგულირებელ საკითხებს და მხოლოდ ზოგადი დებულებებით არის განსაზღვრული ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის აუცილებლობა. თუმცა არცერთი უნივერსიტეტის შემთხვევაში არ იყო განსაზღვრული დისტანციური სწავლების პროცესში მონაცემთა დამუშავებასთან დაკავშირებული საკითხები.

უნდა აღინიშნოს, რომ კვლევაში მონაწილე ერთ-ერთმა უნივერსიტეტმა, რომელსაც შემუშავებული აქვს ინფორმაციული ტექნოლოგიების მართვის პო-

ლიტიკის დოკუმენტი, დეტალურად აღწერა, რომ წვდომა ბაზაზე ინტერნეტიდან დაცულია HTTPS SSL სერტიფიკატის მეშვეობით. ასევე, ელექტრონულ სისტემაში მიმდინარეობს გარკვეული მონაცემების, მაგალითად, მომხმარებელთა პაროლების, დაკავშირების პარამეტრების შიფრაცია. შიფრაციის მიზნით გამოიყენება ასიმეტრიული კრიპტოგრაფია. მონაცემთა უსაფრთხოების ამაღლების მიზნით მონაცემების დამუშავება ძირითადად ხორციელდება უნივერსიტეტის განცალკევებულად გამოყოფილ შიდა ქსელში. უნივერსიტეტის სერვერები განთავსებულია საიმედოდ დაცულ, ჩაკეტილ ოთახში, რომელიც არ არის ხელმისაწვდომი უცხო პირებისთვის. ამასთანავე, ისინი სისტემის უსაფრთხოების მიზნით სხვა ანტივირუსულ საშუალებებსაც იყენებენ და შემუშავებული აქვს დაცვის სისტემა კიბერშეტევებისგან მაქსიმალურად თავდასაცავად. აღსანიშნავია, რომ ამავე უნივერსიტეტს მკაფიოდ აქვს გაწერილი იმ პირთა უფლებამოსილებები და წვდომის ფარგლები, რომლებსაც ხელი მიუწვდებათ ან/და ცვლილების შეტანა შეუძლიათ სტუდენტების პერსონალურ მონაცემებში. უნდა აღინიშნოს, რომ ამგვარი სისტემური მიდგომა ცალსახად დადებითად უნდა შეფასდეს. თუ მათ მიერ გამოყენებული პლატფორმების მეშვეობით შესაძლებელია პერსონალურ მონაცემებთან დაკავშირებული ნებისმიერი ქმედების აღრიცხვა, მაშინ შეიძლება იმის ვარაუდი, რომ ამ უნივერსიტეტში პერსონალურ მონაცემთა დაცვისათვის აუცილებელი ორგანიზაციულ-ტექნიკური ზომები სათანადოდ აქვთ მიღებული.

კვლევაში მონაწილე არცერთ დანესებულებას არ დაუსახელებია, რომ ხორციელდებოდა ავტომატურად ყველა იმ ქმედების აღრიცხვა, რაც პერსონალურ მონაცემებთან მიმართებით მიმდინარეობდა. მაგალითად, ცვლილებები, მესამე პირზე გამჟღავნების შემთხვევები და სხვა ნებისმიერი ქმედება.

მიღებული პასუხებისა და დოკუმენტების გაანალიზების შედეგად შეუძლებელია ცალსახად იმის მტკიცება, რომ უსაფრთხოების ზომები კვლევაში მონაწილე სხვა სუბიექტებს არ აქვთ მიღებული. თუმცა, მოწოდებული მასალის გაანალიზების საფუძველზე, შეიძლება ითქვას, რომ მათ მიერ მიღებული ღონისძიებები უფრო მეტად ორგანიზაციული ხასიათისაა, ვიდრე უსაფრთხოების დაცვის უზრუნველყოფის მიზნებისთვის გატარებული. მონაცემთა დაცვის მექანიზმი სუსტი და არასაკმარისია იმ შემთხვევაში, სადაც არ არიან ძლიერი ინფორმაციული უსაფრთხოების მართვის სპეციალისტები, რომლებიც უზრუნველყოფენ მონაცემთა დაშიფვრასა და იმგვარად შენახვას, რომ დაიცვას მათი უსაფრთხოება შესაბამისი ანტივირუსული და კიბერშეტევებისგან. შესაბამისად, მიუხედავად იმისა, რომ დადებითად უნდა შეფასდეს უნივერსიტეტებში გარკვეული შიდაორგანიზაციული დოკუმენტის არსებობა, კვლევაში მონაწილე

ზოგიერთი უნივერსიტეტის მიერ გატარებული ზომების საფუძველზე, შეიძლება ითქვას, რომ ისინი სათანადოდ ვერ უზრუნველყოფენ სტუდენტების პერსონალური მონაცემების უსაფრთხოების დაცვას.

2.1.6. ფაილური სისტემის კატალოგის წარმოება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, უნივერსიტეტი ვალდებულია, თითოეულ ფაილურ სისტემასთან დაკავშირებით, აწარმოოს ფაილური სისტემის კატალოგი, რაც გულისხმობს ფაილური სისტემის სტრუქტურისა და შინაარსის დეტალურ აღწერილობას.²⁷⁸ ამასთან, უნივერსიტეტი როგორც მონაცემთა დამმუშავებელი, ასევე ვალდებულია, შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს ინფორმაცია, ერთი მხრივ, ფაილური სისტემის შექმნამდე და მასში ახალი კატეგორიის მონაცემთა შეტანამდე, ხოლო მეორე მხრივ, ფაილური კატალოგის ცვლილებისას, მისი შეტანიდან არაუგვიანეს 30 დღისა.²⁷⁹ შესაბამისად, კვლევის ფარგლებში დაგზავნილი კითხვარით გამოთხოვილ იქნა აღნიშნულზე ინფორმაცია, რომელზეც სამმა მონაწილემ მიუთითა ზოგადი პასუხი იმის თაობაზე, რომ უნივერსიტეტი აწარმოებს ფაილური სისტემის კატალოგს და ამის თაობაზე განაცხადი გაკეთებული აქვთ კანონის შესაბამისად. ხოლო, ერთმა მონაწილემ აღნიშნა, რომ ისინი ფაილური სისტემის კატალოგს საერთოდ არ აწარმოებენ.

უნდა აღინიშნოს, რომ პერსონალურ მონაცემთა სამსახურისგან მოწოდებული ინფორმაციის საფუძველზე დადგინდა, რომ კვლევაში მონაწილე ორ სუბიექტს მხოლოდ ერთი ტიპის ფაილური სისტემის კატალოგი აქვს 2015 წელს წარდგენილი შესაბამისი სამსახურისთვის. ხოლო მესამე უნივერსიტეტს რამდენიმე ფაილური სისტემის კატალოგი აქვს წარდგენილი პერსონალურ მონაცემთა დაცვის სამსახურისთვის 2019 წელს. ამ ვადების შემდეგ კი კვლევაში მონაწილე არცერთ უნივერსიტეტს არ წარუდგენია შესაბამისი ფაილური სისტემის კატალოგები, რაც გვაძლევს საფუძველს ვივარაუდოთ, რომ კვლევაში მონაწილე უნივერსიტეტებს არ შეუტანიათ ცვლილებები ფაილური სისტემის კატალოგში ან შეიტანეს, თუმცა აღნიშნული არ შეატყობინეს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსს კანონმდებლობით დადგენილი წესის შესაბამისად.

²⁷⁸ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 19.

²⁷⁹ იქვე, მუხლი 20.

2.2 პერსონალურ მონაცემთა დაცვის სამსახურისგან მიღებული ინფორმაცია

2.2.1. სტატისტიკური ინფორმაცია

საქართველოში პერსონალურ მონაცემთა დამუშავების კანონიერებაზე კონტროლის განმახორციელებელი ორგანო პერსონალურ მონაცემთა დაცვის სამსახურია,²⁸⁰ რომლისგანაც გამოთხოვილ იქნა სტატისტიკური ინფორმაცია საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებების შემოწმებისა და მოქალაქეთა განცხადებების განხილვის შესახებ და ასევე, მიღებული გადაწყვეტილებების ასლებიც.²⁸¹ კვლევის განსაკუთრებული ყურადღების საგანს დისტანციური სწავლებისას ჩატარებული ინსპექტირებები და განცხადებების განხილვის შედეგები წარმოადგენს.

პერსონალურ მონაცემთა დაცვის სამსახურისგან გამოთხოვილი საჯარო ინფორმაცია კანონით დადგენილი ვადის შესაბამისად გამოიგზავნა. მიღებული შედეგებით, გაირკვა, რომ 2013 წლიდან 2022 წლის 1 აპრილის ჩათვლით, პერსონალურ მონაცემთა დაცვის სამსახურმა განახორციელა 12 უმაღლესი საგანმანათლებლო დაწესებულებების ინსპექტირება. მათგან:

დისტანციური სწავლებისას უმაღლეს საგანმანათლებლო დაწესებულებებში პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების მიზნით 2020 წლის 1 აპრილიდან 2022 წლის 1 აპრილის ჩათვლით ინსპექტირებულია მხოლოდ 2 დაწესებულება. რაც შეეხება დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების დამუშავების კანონიერების მოთხოვნით პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მოქალაქეთა განცხადებების განხილვას, აქაც მხოლოდ 2 განცხადება იქნა შემოსული და განხილული 2020 წლის საანგარიშო პერიოდში. შემდგომ 2021-2022 წლის პირველი აპრილის ჩათვლით, სტრუქტურაში ამ მიმართულებით არცერთი განცხადება აღარ შესულა და განხილულა. აღნიშნული მონაცემების საფუძველზე, შეიძლება ითქვას, რომ არც ისე ძლიერი კონტროლი ხორციელდება უნივერსიტეტების შემოწმების მი-

²⁸⁰ 2022 წლის პირველი მარტიდან გაუქმდა სახელმწიფო ინსპექტორის სამსახური და სახელმწიფო ინსპექტორის თანამდებობა. ამ პერიოდიდან სახელმწიფო ინსპექტორის სამსახურის ორ ნაწილად – პერსონალურ მონაცემთა დაცვის სამსახურად და სპეციალურ საგამოძიებო სამსახურად გაიყო. ჩემს მიერ გამოთხოვილი გადაწყვეტილებები მიღებულია 2022 წლის პირველ მარტამდე. შესაბამისად, გადაწყვეტილების მიმღები სახელმწიფო ინსპექტორია. იხ., „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე საქართველოს კანონი, 1312-VIIრ-ს-Xმპ, საქართველოს საკანონმდებლო მაცნე, 13.01.2022; საქართველოს საკონსტიტუციო სასამართლოს 2022 წლის 28 თებერვლის N1/1/1673 საოქმო ჩანაწერი საქმეზე „ლონდა თოლორაია საქართველოს პარლამენტის წინააღმდეგ“.

²⁸¹ პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის 3 მაისის №PDPS 1 22 00001573 წერილი.

მართულებით, რამაც შესაძლოა უფრო მეტად წაახალისოს მონაცემთა შედარებით დაბალი დაცვის სტანდარტის არსებობა, ვიდრე ეს იქნებოდა აქტიური შემოწმებების შედეგად.

აღსანიშნავია ისიც, რომ 2020 წლის 1 აპრილიდან 2022 წლის 1 აპრილის ჩათვლით, დისტანციური სწავლებისას, სტუდენტთა პერსონალური მონაცემების დამუშავების კანონიერების შემოწმებების (ინსპექტირების) საფუძველზე მიღებული გადაწყვეტილებებიდან, სასამართლოში გასაჩივრდა მხოლოდ 1 გადაწყვეტილება, რომლის სასამართლო განხილვაც ჯერ არ დასრულებულა.

ამასთანავე, პერსონალურ მონაცემთა დაცვის სამსახურისგან გამოთხოვილ იქნა ფაილური სისტემის კატალოგის რეესტრის მონაცემები იმ უმაღლესი საგანმანათლებლო დაწესებულებების შესახებ, რომლებმაც სამსახურში წარადგინეს ფაილური სისტემის კატალოგები. აღნიშნული ინფორმაცია ასევე ხელმისაწვდომია ორგანიზაციის ვებ-გვერდზეც. დადგინდა, რომ 2015-2020 წლების განმავლობაში საქართველოში აკრედიტებული უმაღლესი საგანმანათლებლო დაწესებულებებიდან ფაილური სისტემის კატალოგი პერსონალურ მონაცემთა დაცვის სამსახურს მიაწოდა მხოლოდ 10-მა საგანმანათლებლო დაწესებულებამ. ამასთანავე, წერილში აღნიშნულია, რომ კატალოგების გაგზავნა ძირითად შემთხვევაში ერთჯერად ხასიათს ატარებს და არ ასახავს რეალურად უმაღლესი საგანმანათლებლო დაწესებულებების მიერ სანარმოებელი ფაილური სისტემის კატალოგების სრულყოფილ ვერსიას. ამასთანავე, მიუხედავად კანონით დადგენილი მოთხოვნისა, ბოლო ფაილური სისტემის კატალოგი მხოლოდ 2020 წელშია ატვირთული ერთი უნივერსიტეტის მიერ. 2021-2022 წლებში კი არცერთმა აკრედიტებულმა უმაღლესმა საგანმანათლებლო დაწესებულებამ პერსონალურ მონაცემთა დაცვის სამსახურს არ მიაწოდა ინფორმაცია ფაილური სისტემის კატალოგის წარმოების თაობაზე. აღნიშნული იძლევა იმის მტკიცების საშუალებას, რომ ფაილური სისტემის კატალოგის წარმოება და აღნიშნულზე პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირების ვალდებულება უნივერსიტეტებისთვის ფორმალურ ხასიათს ატარებს. მიუხედავად საქართველოს კანონმდებლობით გათვალისწინებული ვალდებულებისა და ამ ვალდებულების დარღვევის შემთხვევაში, შესაბამისი ადმინისტრაციული პასუხისმგებლობისა, უნდა ითქვას, რომ საგანმანათლებლო დაწესებულებები აღნიშნულ საკითხს ნაკლები პასუხისმგებლობით ეკიდებიან და დიდ ყურადღებას არ აქცევენ.

2.2.2. მიღებული გადაწყვეტილებების ანალიზის შედეგად გამოვლენილი ძირითადი მიგნებები

პერსონალურ მონაცემთა დაცვის სამსახურმა 2020 წლის 1 აპრილიდან 2022 წლის 1 აპრილის ჩათვლით შეამოწმა ორი უმაღლესი საგანმანათლებლო დაწესებულება, დისტანციური სწავლებისას სტუდენტების პერსონალური მონაცემების დამუშავების პროცესის, დამუშავების საფუძვლების, მათი პრინციპებთან შესაბამისობის და მიღებული ორგანიზაციულ-ტექნიკური ზომების გამოკვლევის მიზნით. შესწავლის შედეგად გამოიკვეთა რამდენიმე დარღვევა. ყველაზე ფართოდ გავრცელებული დარღვევა პერსონალურ მონაცემთა უსაფრთხოებისთვის დაცვისათვის კანონმდებლობით დადგენილი ტექნიკური ზომების არასრულყოფილად და არაეფექტურად დანერგვა იყო. უმეტესწილად არ აღირიცხებოდა სტუდენტების მონაცემების მიმართ შესრულებული ყველა მოქმედება და მომხმარებლების პაროლები არ ინახებოდა დაშიფრული ფორმით.²⁸² ამასთანავე, ერთ-ერთ უნივერსიტეტში არ არსებობდა პერსონალურ მონაცემთა დამუშავების კანონიერებაზე პასუხისმგებელი პირი.²⁸³ პერსონალურ მონაცემთა დაცვის სამსახურმა გამოავლინა ნაკლოვანება მონაცემთა შენახვის საჭიროების, ვადების და ნაშლის ავტომატური მექანიზმების დანერგვასთან მიმართებითაც.²⁸⁴

აღნიშნულმა მაკონტროლებელმა დაწესებულებამ 2020 წლის 1 აპრილიდან 2022 წლის 1 აპრილის ჩათვლით შეამოწმა ორი უმაღლესი საგანმანათლებლო დაწესებულების ელექტრონული პლატფორმის გამოყენებით მონაცემების დამუშავება, რომელიც როგორც აუდიტორული, ასევე დისტანციური სწავლების პერიოდშიც გამოიყენებოდა. აღნიშნული გადაწყვეტილებების ანალიზის საფუძველზე²⁸⁵ ირკვევა, რომ უმაღლეს საგანმანათლებლო დაწესებულებებში არ არის დანერგილი პერსონალურ მონაცემთა უსაფრთხოების დაცვისთვის კანონმდებლობით დადგენილი ეფექტური ორგანიზაციულ-ტექნიკური ზომები და არ აღირიცხება სტუდენტების მონაცემების მიმართ შესრულებული ყველა მოქმედება. გამოწვევაა, სტუდენტებისა და კურსდამთავრებულების პერსონალური

²⁸² საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 10 მაისის №გ-1/141/2021 გადაწყვეტილება „სსიპ – თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

²⁸³ იქვე, ასევე, საქართველოს სახელმწიფო ინსპექტორის 2021 წლის 14 ივნისის №გ-1/202/2021 გადაწყვეტილება „სსიპ – საქართველოს ტექნიკური უნივერსიტეტის შემოწმების დასრულების შესახებ“.

²⁸⁴ იქვე.

²⁸⁵ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 20 აპრილის №1/115/2021 გადაწყვეტილება „სსიპ – ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“, სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №1/205/2021 გადაწყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემოწმების დასრულების შესახებ“.

მონაცემების გაზიარების საჭიროება, მიზანი და სტუდენტების თანხმობის არარსებობაც. ამასთანავე, პრობლემატურია მონაცემთა დამუშავების ფორმების და ვადების შესახებ შიდა რეგულაციების არარსებობა და იმ სტუდენტთა პერსონალური მონაცემების უსაფუძვლო და არამიზნობრივი შენახვა, რომლებიც აქტიურ შემხებლობაში აღარ არიან უნივერსიტეტთან. გარდა ამისა, გამოვლინდა სტუდენტების პერსონალურ მონაცემთა რამდენიმე სახეობის არამიზნობრივი დამუშავება. მაგალითად, როგორიცაა სტუდენტის ოჯახური მდგომარეობა, ფოტოსურათი, პირადობის მოწმობის ნომერი²⁸⁶ და IP მისამართი.²⁸⁷

პერსონალურ მონაცემთა დაცვის სამსახურმა იმავე საანგარიშო პერიოდში დისტანციური სწავლებისას, სტუდენტთა პერსონალური მონაცემების დამუშავების კანონიერების მოთხოვნით მოქალაქის 2 განცხადება განიხილა და დადგინდა, რომ დაწესებულებას არ დაურღვევია პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით გათვალისწინებული დებულებები.²⁸⁸ მოცემულ გადანყვეტილებათა ანალიზის შედეგად შეგვიძლია აღვნიშნოთ, რომ დისტანციური არხების მეშვეობით ლექციების აუდიო/ვიდეო ჩანერა დასაშვებია, როდესაც უნივერსიტეტის მიერ პროგრამულად უზრუნველყოფილია მუდმივი გაფრთხილება ლექციის ჩანანერის თაობაზე. ასევე დასაშვებია დისტანციური არხების მეშვეობით ჩაბარებული გამოცდების აუდიო/ვიდეო ჩანერა, ვინაიდან აღნიშნული სტუდენტსა და უნივერსიტეტს შორის გაფორმებული ხელშეკრულებითაცაა გათვალისწინებული. მნიშვნელოვანია, მხოლოდ, რომ ჩანერას წინ უნდა უძღოდეს მის განხორციელებაზე გაფრთხილება და დამსწრეთა თანხმობის მიღება, რომელიც კონკლუდენტური ქმედებითაც გამოიხატება. ამასთანავე, ჩანანერის გარკვეული ვადით შენახვა სტუდენტის ინტერესების დაცვასაც ემსახურება, სადავო გარემოებების წამოჭრის შემთხვევაში. ნებისმიერ შემთხვევაში დაუშვებელია ჩანანერების სხვა სხვა პირებზე უკანონოდ გამჟღავნებაც. პერსონალურ მონაცემთა დაცვის სამსახურმა დაადგინა, რომ საქართველოში ლექციების ჩანანერებთან მიმართებით, სტუდენტს არ წარმოეშობა მოთხოვნა, დაიშიფროს ლექტორისა და სტუდენტის კომუნიკაციის ნაწილი, იმ ფაქტორის გათვალისწინებით, როდესაც უნივერსიტეტში სტუდენტთა, აკრედიტებულ პროგრამათა და საგანთა რაოდენობა საკმაოდ დიდი მოცულობისაა.

²⁸⁶ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 15 ივნისის №1/205/2021 გადანყვეტილება „სსიპ – ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

²⁸⁷ სახელმწიფო ინსპექტორის სამსახურის 2021 წლის 20 აპრილის №1/115/2021 გადანყვეტილება „სსიპ – ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტის შემონმების დასრულების შესახებ“.

²⁸⁸ საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 17 აგვისტოს №გ-1/272/2020 გადანყვეტილება „განცხადების განხილვის დასრულების შესახებ“; საქართველოს სახელმწიფო ინსპექტორის 2020 წლის 8 ივლისის №გ-1/231/2020 გადანყვეტილება „განცხადების განხილვის დასრულების შესახებ“.

V. რეკომენდაციები

კორონავირუსის ("Covid-19") გავრცელებამ მთელი მსოფლიოს მასშტაბით უფრო პოპულარული გახადა დისტანციური სწავლების მეთოდი. არსებობს მოლოდინი, რომ იგი მომავალში საგანმანათლებლო პროცესის განუყოფელი ნაწილიც იქნება.²⁸⁹ ჩატარებული კვლევის შედეგად, შესაძლებელია გამოვყოთ რამდენიმე მნიშვნელოვანი რეკომენდაცია, რომელიც ხელს შეუწყობს უმაღლეს საგანმანათლებლო დაწესებულებებს პრაქტიკაში დანერგონ პერსონალურ მონაცემთა დაცვის უფრო მაღალი სტანდარტი.

პირველ რიგში, უმჯობესია საგანმანათლებლო დაწესებულებებმა გაიაზრონ და იდენტიფიცირება მოახდინონ სტუდენტის იმ პერსონალური მონაცემებისა, რომელთაც ისინი ამუშავებენ, მათ შორის, ცალკე გამოყონ ის მონაცემები, რომელთაც დისტანციური სწავლების პროცესში ამუშავებენ. ასევე, ცალკე გამოყონ განსაკუთრებული კატეგორიის პერსონალური მონაცემები, ასეთის არსებობის შემთხვევაში. ამასთან, მნიშვნელოვანია, რომ თითოეული მონაცემთან მიმართებაში განსაზღვრონ მისი დამუშავების მიზნები და დამუშავების სამართლებრივი საფუძველი. მიუთითოს, მათი დამუშავებისათვის გამოყენებული ელექტრონული სისტემები/მონაცემების დაცვის პოლიტიკა, ამასთანავე, მნიშვნელოვანია, რომ განსაზღვრონ დამუშავებულ მონაცემთა შენახვისათვის განსაზღვრული ვადები და ამ ვადის გასვლის შემდეგ მონაცემთა განადგურებისა და არქივირების დეტალური წესი.

გარდა აღნიშნულისა, საგანმანათლებლო დაწესებულებებმა უნდა შეაფასონ მათ მიერ დამუშავებულ პერსონალურ მონაცემებთან დაკავშირებული რისკები. ამ მხრივ, კი მნიშვნელოვანია განსაზღვრონ მონაცემთა უსაფრთხოების უზრუნველსაყოფად გასატარებელი ღონისძიებები და შეიმუშაონ ზეგავლენის დოკუმენტი. ასევე, საგანმანათლებლო დაწესებულებებმა უნდა შეიმუშაონ მონაცემთა დაცვის კონკრეტული პოლიტიკა, რომელშიც აღნიშნული იქნება მონაცემთა დამუშავების მიზნები, საფუძვლები და საშუალებები, მათი შენახვის ვადები, განადგურების წესი და სხვა პრაქტიკული საკითხები, მათ შორის ელექტრონული სწავლების წარმართვის შემთხვევაში და ეს დოკუმენტაცია თავისუფლად ხელმისაწვდომი უნდა იყოს სტუდენტებისათვის და პერსონალისათვის, რათა წინასწარ იყოს განჭვრეტადი მათი მონაცემების დამუშავების საფუძვლები და პროცესი.

ამასთანავე, უნივერსიტეტმა ყურადღებით უნდა აარჩიოს დისტანციური სწავლებისთვის გამოსაყენებელი პლატფორმა და მისი გამოყენებისას შეზღუ-

²⁸⁹ Crawford J., Butler-Henderson K., Rudolph J., Malkaw B., Glowatz M., Burton R., Magn P., Lam S., COVID-19: 20 Countries' Higher Education Intra-Period Digital Pedagogy Responses, Journal of Applied Learning & Teaching, Vol. 3, No.1, 2020, 9-19.

დოს ონლაინ შეხვედრაზე არაავტორიზებული პირების დასწრება, ასევე ნებართვის გარეშე რომელიმე ახალი მონაწილეების დამატების შესაძლებლობა. გარდა აღნიშნულისა, მან უნდა უზრუნველყოს, რომ ელექტრონული პლატფორმის მეშვეობით აღირიცხებოდეს პერსონალურ მონაცემებთან დაკავშირებული ნებისმიერი ქმედება.

მნიშვნელოვანია საგანმანათლებლო დაწესებულებებში გამჭვირვალობის პრინციპის დანერგვა და დისტანციური სწავლებისას დამუშავებული პერსონალური მონაცემების თაობაზე სტუდენტის ინფორმირება. ამ მიზნით, უნდა შემუშავდეს წერილობითი დოკუმენტი, რომელიც სტუდენტს დაეგზავნება ორგანიზაციული ელექტრონული ფოსტის ან უნივერსიტეტის საგანმანათლებლო პლატფორმის მეშვეობით. იმისათვის, რომ დაწესებულებაც დარწმუნებული იყოს სტუდენტის ინფორმირებაში, მნიშვნელოვანია უკუკავშირისთვის მათგან დადასტურების მიღების გარკვეული მექანიზმის შემუშავება. სასურველია, სტუდენტთა თანხმობის გამომხატველი წერილობითი დოკუმენტის განცალკევებით შემუშავებაც, რომელსაც საგანმანათლებლო დაწესებულება საჭიროებისამებრ გამოიყენებს. კერძოდ, მაშინ, როდესაც პერსონალურ მონაცემთა დამუშავების მთავარი საფუძველი მონაცემთა სუბიექტისგან თანხმობის მიღებაა. მაგალითად, დისტანციური სწავლებისას ჩატარებული ონლაინ შეხვედრების აუდიო-ვიდეო ჩანაწერების განხორციელებისას.

ასევე, აუცილებელია, დაწესებულებამ შეიმუშაოს უსაფრთხოების პოლიტიკა და დანერგოს შესაბამისი ორგანიზაციულ ტექნიკური ზომები, რომელშიც ჩაერთვებიან მონაცემთა დამუშავების კანონიერებაზე მონიტორინგის განმახორციელებელი პირი/პირები და IT სპეციალისტები, რომლებიც დანერგავენ სისტემურ ღონისძიებებს მონაცემთა დაცვისათვის. მათ შორის, მნიშვნელოვანია მონაცემთა კრიპტოგრაფიული დაშიფვრა და კიბერთავდასხმისგან დამცავი მექანიზმის შემუშავება. ასევე, ინფორმაციული უსაფრთხოების სამსახურმა უნდა უზრუნველყოს დისტანციური სწავლებისას გამოყენებული ტექნიკური სისუსტეების გამოვლენა და შეუსაბამობების პრევენციული ღონისძიებების დანერგვაც. აუცილებელია განისაზღვროს ინციდენტებზე რეაგირების გზებიც. ამასთანავე, მნიშვნელოვანია, პერიოდულად გადაიხედოს მონაცემთა უსაფრთხოების უზრუნველყოფისთვის მიღებული ტექნიკური და ორგანიზაციული ზომები და შემოწმდეს მათი ეფექტურობა. დარღვევების ან არაეფექტურობის გამოვლენის შემთხვევაში კი ისინი უნდა შეიცვალოს და დაიხვეწოს. სასურველია, საგანმანათლებლო დაწესებულებამ, უსაფრთხოების წესების დანერგვასთან ერთად, გააცნოს იგი ადმინისტრაციულ პერსონალს, ლექტორებს და სტუდენტებს. ასევე, შეიმუშაონ რეკომენდაციები ან

შიდა ინსტრუქციები მათ მიერ ელექტრონული პლატფორმების უსაფრთხო გამოყენებასთან დაკავშირებით.

დიდმა საგანმანათლებლო დაწესებულებებმა, რომლებიც საკმაოდ დიდი მოცულობის პერსონალურ მონაცემებს ამუშავებენ, უმჯობესია დანერგონ მონაცემთა დაცვის ოფიცირის პოზიცია ეს კი უზრუნველყოფს ამ საკითხებზე პასუხისმგებელი პირის გამოყოფას და მონაცემთა კანონიერ დამუშავებაზე მუდმივი მონიტორინგის შესაძლებლობას. მნიშვნელოვანია, რომ დაწესებულების მიერ შერჩეულ პიროვნებას ჰქონდეს პერსონალურ მონაცემთა დაცვის საკითხებზე კარგი ცოდნა, რათა შეძლოს და შეაფასოს მონაცემთა დამუშავებასთან დაკავშირებული რისკები, მონაწილეობა მიიღოს შესაბამისი პოლიტიკის დახვეწაში და შეძლოს მოახდინოს ადეკვატური რეაგირება აღმოჩენილი უზუსტობების გამოსასწორებლად.

მნიშვნელოვანია საგანმანათლებლო დაწესებულებამ იზრუნოს დასაქმებული პირების ცნობიერების ამაღლებაზე. მაგალითად, ტრენინგების ჩატარებით, ინფორმაციის მიწოდებით ან სხვების მიერ ორგანიზებული სემინარებისა და ტრენინგებში მონაწილეობის უზრუნველყოფით. აღნიშნული რეკომენდაცია ხშირად გამოიყენება დანიის პერსონალურ მონაცემთა დაცვის სამსახურის მიერ²⁹⁰ დისტანციური სწავლებისას შემონმებული საგანმანათლებლო დაწესებულებებისათვის. ასევე, საგანმანათლებლო დაწესებულებებმა პერსონალისთვის, ლექტორებისა და სტუდენტებისათვის უნდა შეიმუშაონ რეკომენდაციები ტექნოლოგიების და ელექტრონული პლატფორმების უსაფრთხოდ გამოყენებასთან დაკავშირებით.

საბოლოოდ, იმისათვის, რომ საგანმანათლებლო დაწესებულებებმა პერსონალურ მონაცემების დამუშავებასთან დაკავშირებული რიგი პროცესების გაანალიზება და შემდგომში პრაქტიკაში ეფექტური დანერგვა მოახერხონ, სასურველი იქნება, შეიმუშაონ თვითშეფასების კითხვარიც. ეს მისცემთ შესაძლებლობას, თვითონვე აღმოაჩინონ პრობლემები და იზრუნონ მათ სამომავლო გამოსწორებაზე. გარდა ამისა, უმჯობესი იქნება, თუ მონაცემთა დამუშავებაზე პასუხისმგებელი პირები გაეცნობიან შესაბამისი ორგანოს მიერ მიღებულ გადაწყვეტილებებს, რეკომენდაციებს და ითანამშრომლებენ პერსონალური მონაცემების დაცვის სამსახურთან საჭირო საკითხებზე კონსულტაციების მიღების გზით.

გარდა ზემოაღნიშნული რეკომენდაციებისა, ასევე მნიშვნელოვანია, რომ პერსონალურ მონაცემთა დაცვის სამსახურმა გააძლიეროს საგანმანათლებლო დაწესებულებების კონტროლი, მათ მიერ დისტანციური სწავლების პროცესში პერსონალური მონაცემების დამუშავების კანონიერებაზე ზედამხედველობის

²⁹⁰ <<https://bit.ly/3yE1LdJ>> [30.06.2022].

მიმართულებით. დღევანდელი მდგომარეობით, მათ მიერ შემოწმებული უნივერსიტეტების რიცხვი საერთო ჯამში საკმაოდ მცირეა და ამასთან, აღნიშნული გადანყვეტილებები არ არის საჯაროდ ხელმისაწვდომი მათსავე საიტზე, რათა სხვა უნივერსიტეტებმაც შეძლონ კონკრეტული მაგალითების საფუძველზე თავიანთ ორგანიზაციებში პერსონალურ მონაცემთა დაცვის პრაქტიკის გაუმჯობესება. თუმცა, ამ გადანყვეტილებების საჯაროდ გამოქვეყნება ვერ იქნება ისეთი შედეგის მომტანი, როგორც კონკრეტული დანესებულების ინსპექტირება. ამგვარი გადანყვეტილებების გამოქვეყნება შეგვიძლია განვიხილოთ დამატებით და არა ძირითად ღონისძიებად.

VI. დასკვნა

საქართველოში პერსონალურ მონაცემთა დაცვის კანონმდებლობა დისტანციური სწავლების დანერგვამდეც არსებობდა. უმაღლესი საგანმანათლებლო დაწესებულებები ნებისმიერ შემთხვევაში ვალდებული არიან ამ კანონმდებლობის შესაბამისად დაამუშაონ სტუდენტთა პერსონალური მონაცემები. თუმცა, კვლევის შედეგად დადგინდა, რომ კანონში არსებული ჩანაწერების მიუხედავად, მათი სათანადო რეალიზაცია დისტანციური სწავლებისას სტუდენტთა პერსონალური მონაცემების დამუშავებისას ვერ ხორციელდება.

ნაშრომში განხილულია პერსონალური მონაცემების ის ძირითადი სახეები, რომლებსაც დისტანციური სწავლების მიმდინარეობისას საგანმანათლებლო დაწესებულებები ამუშავებენ. მათ შორისაა, სტუდენტის ვინაობის დამდგენი და მისი საკონტაქტო მონაცემები, ასევე ხმა და ვიზუალური გამოსახულება, შესრულებული დავალებები და საგამოცდო ნაშრომები. გარდა აუცილებლად დასამუშავებელი მონაცემებისა, ზოგიერთ შემთხვევაში, დისტანციური სწავლების მიმდინარეობისას, საქართველოში გამოკითხული უნივერსიტეტების ნაწილი ელექტრონული პლატფორმების მეშვეობით მოცულობით მონაცემებს არამიზნობრივად ამუშავებს და ამჟღავნებს მესამე პირებზე. ასეთი მონაცემია სტუდენტის ოჯახური მდგომარეობის შესახებ ინფორმაცია, მისი პირადობის დამადასტურებელი მოწმობის სარეგისტრაციო ნომერი, ზოგიერთ შემთხვევაში IP მისამართი და სხვა.

საგანმანათლებლო დაწესებულებებში ჩატარებული კვლევის მიხედვით დადგინდა, რომ კვლევაში მონაწილე დაწესებულებებს არ აქვთ ცალკე განსაზღვრული ის პერსონალური მონაცემები, რომლებსაც დისტანციური სწავლების მიმდინარეობისას ამუშავებენ. მათ შორის, ერთ-ერთი უნივერსიტეტი აღნიშნავს, რომ სტუდენტის ელექტრონული ფოსტის მისამართს არ ამუშავებს დისტანციუ-

რი სწავლების განმავლობაში, მაშინ, როდესაც ეს დაწესებულება იყენებს “google meet“-ის პლატფორმას. აღნიშნული პლატფორმის გამოყენებისას კი სტუდენტი ლექცია/სემინარზე მოიწვევა ელექტრონული ფოსტის მისამართის მეშვეობით და სწორედ ამ მისამართით ესწრება შეხვედრას. შესაბამისად, ამ პლატფორმის მეშვეობით დისტანციური სწავლებისას სტუდენტის ელექტრონული ფოსტის მისამართი ყველა შემთხვევაში მუშავდება. ასევე, კვლევაში მონაწილე საგანმანათლებლო დაწესებულების მითითებით, დისტანციური სწავლებისას, ისინი აუდიტორული სწავლებისას დამუშავებული პერსონალური მონაცემისაგან განსხვავებულ მონაცემებს არ ამუშავებდნენ. თუმცა, არცერთ უნივერსიტეტს არ აღუნიშნავს, რომ ისინი ამუშავებდნენ სტუდენტის ხმასა და ვიზუალურ გამოსახულებას, მათ მიერ ონლაინ შეხვედრაზე ვიდეოს/მიკროფონის ჩართვის შემთხვევაში. მაგრამ გამოვლინდა, რომ ასეთი მონაცემები მუშავდებოდა, ვინაიდან, რამდენიმე უნივერსიტეტი იწერდა კიდეც ლექციებს, მათი შემდგომში ხელმისაწვდომობის მიზნით. ამასთანავე, კვლევაში მონაწილე არცერთი საგანმანათლებლო დაწესებულების მიერ არ იყო აღნიშნული, რომ ისინი ამუშავებდნენ სტუდენტის დავალებებს და საგამოცდო ნაშრომებს, როგორც მათ პერსონალურ მონაცემებს. კვლევის შედეგად დადგინდა, რომ ზოგიერთ შემთხვევაში საგანმანათლებლო დაწესებულები ზუსტად ვერ განსაზღვრავენ სტუდენტების პერსონალური მონაცემის სახეებს, რომლებიც დისტანციური სწავლებისას შეიძლება დამუშავდეს. ეს ეჭვქვეშ აყენებს სტუდენტთა პერსონალური მონაცემების დამუშავების კანონიერებას, ვინაიდან, სწორედ მონაცემთა სახეების, დამუშავების საფუძვლებისა და ფარგლების განსაზღვრაა მთავარი საფუძველი მონაცემთა კანონიერი დამუშავებისა და მათი უსაფრთხოების უზრუნველსაყოფად მისაღები საჭირო ზომების განსასაზღვრად.

ნაშრომში, ასევე, განხილულია ის ძირითადი წესები, რომლებიც საგანმანათლებლო დაწესებულებებმა უნდა დაიცვან სტუდენტთა პერსონალური მონაცემების კანონიერი დამუშავებისა და უსაფრთხო შენახვისთვის. მათ შორის, განსაზღვრული უნდა იყოს მონაცემთა დამუშავების მიზანი და საფუძვლები. ამასთანავე, წინასწარ უნდა დადგინდეს დასამუშავებელ მონაცემთა მოცულობა და მისი დამუშავების ფარგლები, რის შესახებაც წინასწარ უნდა ეცნობოს სტუდენტს და საჭიროების შემთხვევაში უნდა არსებობდეს მათგან მიღებული ინფორმირებული თანხმობა. ჩატარებული კვლევის შედეგად დადგინდა, რომ ერთ-ერთ მთავარ გამოწვევას უნივერსიტეტების მიერ მონაცემთა დამუშავების მიზნების განუსაზღვრელობა და დამუშავებული პერსონალური მონაცემების უვადოდ შენახვა წარმოადგენს. გარდა იმისა, რომ მონაცემთა უვადოდ შენახვა დაუშვებელია, ასევე მიუღებელია ყველა ტიპის პერსონალური მონაცემისთვის ერთნაირი შენახვის ვადის დადგენა. თითოეულ შემთხვევაში, აუცილებელია შე-

ფასდეს დამუშავებული მონაცემის მიზანი და ამ მიზნის მიღწევის შემდეგ ისინი უნდა წაიშალოს/განადგურდეს ან იმგვარად იქნეს შენახული, რომ შეუძლებელი იყოს პირის იდენტიფიცირება. მიუხედავად, კანონმდებლობით დადგენილი მიდგომისა, კვლევაში მონაწილე უმრავლესი საგანმანათლებლო დაწესებულების მიერ ეს პრინციპი არ არის დაცული. აღნიშნული კი, გარდა იმისა, რომ საკანონმდებლო ნორმების უხეში დარღვევაა, ასევე, უნდა მივიჩნიოთ გაუმართლებელ ჩარევად სტუდენტის პირადი და ოჯახური ცხოვრების უფლებაშიც.

მიჩნეულია, რომ პერსონალურ მონაცემთა დაცვის კანონიერების უზრუნველსაყოფად აუცილებელია არსებობდეს შიდაორგანიზაციული აქტი, სადაც დეტალურად გაიწერება მონაცემთა დამუშავების წესი და პროცედურა, მათი დამუშავების მიზნები და საფუძვლები, შენახვის ვადები და განადგურებისა და დაარქივების წესი. ამასთანავე, განსაზღვრული უნდა იყოს დამუშავებულ მონაცემებზე წვდომის წესი და ის პირები, ვინც ასეთი უფლებამოსილებით იქნებიან აღჭურვილნი. ამავე დოკუმენტის მეშვეობით შეიძლება მონაცემთა დამუშავებაზე პასუხისმგებელი პირის უფლებამოსილებების, მონიტორინგის ჩატარების წესისა და რისკების შეფასების შესახებ ვალდებულებების განსაზღვრაც. დადებითად უნდა მივიჩნიოთ ის ფაქტი, რომ კვლევაში მონაწილე ზოგიერთ უნივერსიტეტს მსგავსი დოკუმენტი შემუშავებული აქვს. თუმცა, ამ დოკუმენტებში ზოგადი დებულებებია მოცემული, რომელიც კანონმდებლობაში ასახული ჩანაწერების იდენტურია. საქართველოში, კვლევაში მონაწილე უნივერსიტეტებიდან მხოლოდ ერთ შემთხვევაში იყო დადგენილი ამ მნიშვნელოვანი საკითხების ზოგიერთი ნაწილი. ასევე, მხოლოდ ამ დაწესებულების მიერ იყო დეტალურად განსაზღვრული მონაცემთა შენახვის ვადებიც, თითოეულ მონაცემთან მიმართებით. რა თქმა უნდა, დადებითად უნდა შეფასდეს, რომ მონაცემთა დამუშავების პოლიტიკის შესახებ დოკუმენტები ყველა საგანმანათლებლო დაწესებულებას აქვს შემუშავებული. თუმცა, კვლევაში მონაწილე უნივერსიტეტების მიერ დისტანციური სწავლების პროცესში მონაცემთა დამუშავებასთან დაკავშირებულ საკითხების, მათ შორის, მონაცემთა წვდომის უფლების მქონე პირების განსაზღვრა, ქცევის წესების, დარღვევებზე რეაგირების წესების არქონა და სხვა დეტალური საკითხების განუსაზღვრელობა მონაცემთა დამუშავების პროცესს კითხვის ნიშნის ქვეშ აყენებს. იგი სტუდენტებისა და სხვა პირებისთვის მონაცემთა დამუშავების პროცესს ბუნდოვანს ხდის და მის კანონიერად განხორციელებას მხოლოდ საგანმანათლებლო დაწესებულებების მიერ მონაცემთა დამუშავებისას კეთილსინდისიერი ქმედებების განხორციელებაზე დამოკიდებულს ტოვებს.

დადგენილია, რომ უმაღლესი საგანმანათლებლო დაწესებულება ვალდებულია სტუდენტთა პერსონალური მონაცემების დასაცავად განსაზღვროს შე-

საბამისი ტექნიკური ზომები. მათ შორისაა, მონაცემებზე წვდომის შეზღუდვა, დაცვის სისტემების შემუშავება ანდა გამოვლენილ დარღვევებზე რეაგირების წესების განსაზღვრა. აღსანიშნავია, რომ ასეთი დოკუმენტის არსებობა პერსონალურ მონაცემთა დამუშავების საკმაოდ მაღალი სტანდარტის დანერგვაზე მიუთითებს. თუმცა, თუ მათი პრაქტიკაში იმპლემენტირება არ განხორციელდა, განერილი წესები მხოლოდ ფურცელზე დანერილ სიტყვებად დარჩება და რეალურად სტუდენტთა პერსონალური მონაცემები დიდი საფრთხის ქვეშ იქნება. ჩატარებული კვლევის შედეგად გამოვლინდა, რომ უმაღლესი საგანმანათლებლო დაწესებულებებისთვის უდიდესი გამოწვევა სწორედ უსაფრთხოების ზომების გატარებაა. ამ პრინციპის უზრუნველსაყოფად, მნიშვნელოვანია ძლიერი IT სპეციალისტების ჩართვა მონაცემთა დაცვის უსაფრთხოების პოლიტიკის დოკუმენტის შემუშავებასა და ტექნიკური უსაფრთხოების მაღალი სტანდარტის დაგეგმვაში. ამასთანავე, აუცილებელია, რომ თითოეულ შემთხვევაში შეფასდეს მაქსიმალურად საჭირო, გამოსადეგი და პროპორციული დაცვის ღონისძიებები და არ მოხდეს მხოლოდ მონაცემთა წვდომის შეზღუდვა, კომპიუტერზე ანტივირუსული პროგრამის დაყენება ან სხვა დაბალი დონის უსაფრთხოების ზომების დანერგვა. უმეტესწილად უმაღლესი საგანმანათლებლო დაწესებულებებისთვის (არა მხოლოდ საქართველოში), მთავარი გამოწვევა სათანადო უსაფრთხოების ზომების შემუშავებაა. შესაბამისად, მისასალმებელია ის ფაქტი, რომ რამდენიმე უნივერსიტეტის შემთხვევაში უსაფრთხოების უზრუნველსაყოფად სისტემური ზომები იქნა მიღებული. მონაცემთა სათანადო დაცვისთვის, საუკეთესო პრაქტიკის გათვალისწინებით, მნიშვნელოვანია სწორედ კომპლექსური და მუდმივად განახლებადი დაცვის ღონისძიებების გატარება, მათ შორის, დაშიფვრის შესაძლებლობის გამოყენება, კიბერშეტევისგან თავდაცვითი ღონისძიებების დანერგვა და სხვა. გარდა ამისა, აუცილებელია დამუშავებული მონაცემების მიმართ განხორციელებული ნებისმიერი ქმედების სისტემატური აღრიცხვა. ამ მიზნით, საგანმანათლებლო დაწესებულებებმა, დისტანციური სწავლებისას შესაძლოა დაამუშაონ კონკრეტული IP მისამართები და შეზღუდონ პერსონალურ მონაცემებზე წვდომა ზოგიერთი საფრთხის შემცველი სერვერებისთვის.

ანალიზის შედეგად გამოვლინდა, რომ საგანმანათლებლო დაწესებულებების მიერ, უგულებელყოფილია ფაილური სისტემის კატალოგის წარმოების და მისი შესაბამისი სტრუქტურისთვის წარდგენის ვალდებულების წესიც. აღნიშნულის გამომწვევი მიზეზი კი ფაილური სისტემის კატალოგის არწარმოება ან კანონმდებლობით დადგენილი ნორმების უგულებელყოფაა. ასევე, საკმაოდ სუსტია პერსონალურ მონაცემთა დაცვის სამსახურის კონტროლი, დისტანციური სწავლების პროცესში უმაღლესი საგანმანათლებლო დაწესებულებების მიერ პერსონალური მონაცემების დამუშავების კანონიერებაზე.

ნაშრომში ყურადღება გამახვილებულია ევროპის კავშირსა და რიგ სახელმწიფოებში დანერგილი პრაქტიკული მიდგომების შესახებ და ანალიზის საფუძველზე შემოთავაზებულია ის რეკომენდაციები, რომელთა დანერგვითაც საგანმანათლებლო დაწესებულებები სტუდენტების პერსონალური მონაცემების დაცვის უფრო მაღალი სტანდარტის დამკვიდრებას უზრუნველყოფენ. მათ შორისაა, მონაცემთა გამჭვირვალედ დამუშავების პრინციპის დანერგვა, რათა სტუდენტებისთვის წინასწარ იყოს განჭვრეტადი მის შესახებ რა ტიპის პერსონალურ მონაცემებს და რა გზით დაამუშავებს უნივერსიტეტი. უნივერსიტეტების მიერ მონაცემთა დამუშავების რაოდენობისა და ინგლისისა და ევროკავშირის პრაქტიკის გათვალისწინებით, სასურველი იქნება პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუტის შემოღება საქართველოში აკრედიტებული უმაღლესი საგანმანათლებლო დაწესებულებებისთვის, რაც გააიოლებს ამ დაწესებულებებში პერსონალური მონაცემების დამუშავებაზე და დაცვაზე ზედამხედველობას და მონაცემთა დაცვა უბრალო ფორმალობად არ იქნება აღქმული. ამასთანავე, დისტანციური სწავლების პროცესში მონაცემებთან დაკავშირებული რისკების მართვის მიზნით, ასევე, რეკომენდებულია ზეგავლენის დოკუმენტებისა და თვითშეფასების კითხვარის შემუშავება და მუდმივი მონიტორინგის განხორციელება პერსონალური მონაცემების დამუშავებასა და უსაფრთხოების დაცვაზე. ამ მიზნით, აუცილებელია საგანმანათლებლო დაწესებულებებმა მუდმივად უზრუნველყონ თავიანთი თანამშრომლების დატრენინგება და პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით მათი ცნობიერების ამაღლება. მნიშვნელოვანია, საგანმანათლებლო დაწესებულებების პერსონალისთვის, ლექტორებისა და სტუდენტებისათვის შემუშავდეს რეკომენდაციები ტექნოლოგიების და ელექტრონული პლატფორმების უსაფრთხოდ გამოყენებასთან დაკავშირებით, რაც საბოლოოდ, ხელს შეუწყობს სტუდენტების მონაცემების კანონიერ დამუშავებას, მათთან დაკავშირებული რისკების იდენტიფიცირებას, უზუსტობებზე და ნაკლოვანებებზე დროულ რეაგირებასა და მუდმივად განახლებადი დაცვის სისტემების შემუშავებას.

კვლევის შედეგად საბოლოოდ დადგინდა, რომ უმაღლესი საგანმანათლებლო დაწესებულებების მიერ სტუდენტთა პერსონალური მონაცემების დამუშავების მაღალი სტანდარტის დასანერგად, საქართველოს კანონმდებლობით გათვალისწინებული ნორმების პარალელურად, აუცილებელია ევროპული საუკეთესო პრაქტიკის გათვალისწინება და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ეფექტიანი კონტროლის განხორციელება. შეიძლება ითქვას, რომ მხოლოდ ამ მექანიზმით მიიღწევა საგანმანათლებლო დაწესებულების მიერ სტუდენტების მონაცემების სამართლიანი და კანონიერი დამუშავების მიზანი.