Covid-19 და პერსონალურ მონაცემთა დაცვა „Zoom-ის“ გამოყენებით დისტანციური სწავლებისას

შესავალი

ახალი კორონავირუსის სახელწოდებით ცნობილმა პანდემიამ (შემდგომში — Covid-19) დიდი გავლენა იქონია მსოფლიოზე. მოდიფიცირება განიცადა სამუშაო ადგილებმა, ცალკეულმა სფეროებმა და სტრატეგიებმა. მათ შორის პანდემია შეეხო განათლებასაც. საქართველოს მთავრობის 2020 წლის 23 მარტის №181 დადგენილების მე-3 მუხლის 1-ლი პუნქტით საქართველოს მასშტაბით შეჩერდა განათლების პროცესი. ამავე აქტის საფუძველზე, ასეთი წინაპირობის არსებობის შემთხვევაში, საგანმანათლებლო დაწესებულებებს დისტანციური სწავლების ფორმის გამოყენების შესაძლებლობა მიეცათ. შესაბამისად, ბევრმა (როგორც საჯარო, ისე კერძო) უნივერსიტეტმა გადაწყვიტა სწავლების ახლებურ ფორმაზე გადასულიყო.

დისტანციურმა სწავლებამ პრაქტიკაში წარმოშვა ახალი გამოწვევები, რომელთა შორის გამორჩეულ ადგილს იკავებს პერსონალურ მონაცემთა დაცვა. ზოგიერთი ლექტორისა თუ სტუდენტის მიერ სოციალურ ქსელში აბსოლუტურად პოზიტიური განწყობითა თუ მიზნით გავრცელდა ონლაინ-სწავლების ამსახველი მასალა (უმეტესად, „Screenshot-ის“ სახით). მასალა კი შეიცავდა დისტანციური სწავლების სუბიექტის პერსონალურ მონაცემებს.

წინამდებარე ნაშრომი შეეხება სწორედ ამ საკითხს, თუ რამდენად დაცულია პირთა პერსონალური მონაცემები მაშინ, როდესაც ისინი არ აცხადებენ თანხმობას ასეთი მასალის გასაჯაროებაზე. სახელმწიფო ინსპექტორის სამსახურმა აღნიშნულის თაობაზე გამოსცა რეკომენდაციები, რომელიც დისტანციურ სწავლებას და პერსონალრ მონაცემთა დაცვას შეეხო (იხ. www.personaldata.ge/ka/press/post/6349). განსახილველი თემატიკა თავის სამართლებრივად აქტუალური იქნება Covid-19-ის პანდემიის დასრულების შემდეგაც, როდესაც ცალკეულ შემთხვევაში წარიმართება დისტანციური სწავლება.

1. დისტანციური სწავლების სახეები

უმაღლესმა სასწავლებლებმა შეიმუშავეს დისტანციური სწავლების რამდენიმე სახე. ერთი ასეთი შემთხვევაა ვიდეომასალის გავრცელება, როდესაც ლექტორი ლექციას ინდივიდუალურად წერს ვიდეოს სახით და აწვდის სტუდენტებს. მეორე მაგალითია სტუდენტებისთვის სალექციო აუდიომასალის მიწოდება. ეს შეიძლება მოხდეს როგორც პრეზენტაციასთან (მაგალითად, „Power Point“) ერთად, ისე მხოლოდ აუდიოჩანაწერის მომზადების გზით. მესამე და პრაქტიკაში საკმაოდ გავრცელებული მაგალითია „Zoom-ის“ გამოყენება, როდესაც სტუდენტებთან ერთად, ლექტორი ონლაინაა ჩართული და ამ გზით ახერხებს ლექციის წაკითხვას (მათ შორის, სტუდენტებს შეუძლიათ ჩართვა და შეკითხვების დასმა). შესაბამისი ტექნიკური მახასიათებლის გათვალისწინებით, წინამდებარე ნაშრომში განსაკუთრებით სწორედ „Zoom-ის“ შემთხვევაზე გამახვილდება ყურადღება.

2. „Zoom-ის“ გამოყენება და პერსონალური მონაცემები

„Zoom-ის“ გამოყენებისას ტექნიკურად შესაძლებელია გამოჩნდეს მასში გაწევრიანებული (დამსწრე) პირის სახელი და გვარი, ასევე ვი-

ზუალი. უმეტეს შემთხვევაში, სტუდენტის (ასევე, ლექტორის) გადასაწყვეტია, ჩართავს თუ არა ვიდეოს და გამოაჩენს თუ არა საკუთარ ვიზუალს. თითოეულ შემთხვევაში, გადაწყვეტილების მიღებისას, დისტანციური ლექციის დამსწრე ხელმძღვანელობს სალექციო მიზნებით. მას არ აქვს გააზრებული, რომ მისი ვიზუალი შეიძლება გასაჯაროვდეს.

3. განსხვავება ონლაინ-ლექციასა და საუდიტორიო ლექციას შორის *(პერსონალურ მონაცემთა დაცვის ჭრილში)*

ონლაინ-ლექციის შემთხვევაში, „Zoom-ით“ მიიღება ინდივიდუალური უნიკალური კოდი. კერძოდ, ლექციის ორგანიზატორი (უმეტესად, ლექტორი) არეგისტრირებს დისტანციურ შეხვედრას. მას შესაბამის უნიკალურ კოდს ანიჭებს „Zoom-ის“ სისტემა, რაც ეგზავნება სტუდენტებს, რათა მათაც შეძლონ ვირტუალურ შეხვედრაში ჩართვა.

კოდი ეგზავნებათ მხოლოდ დაინტერესებულ / დარეგისტრირებულ პირებს. იგი არ წარმოადგენს საჯარო ინფორმაციას (თუ უშუალოდ ორგანიზატორის მიერ არ იქნა გასაჯაროებული პირთა განუსაზღვრელი წრის მიმართ). შესაბამისად, ნებისმიერ პირს არ აქვს შესაძლებლობა მოისმინოს ონლაინ-ლექცია.

აღნიშნული განსხვავდება საუდიტორიო ლექციისგან: უმაღლეს სასწავლებელთა უმეტეს შემთხვევაში, ნებისმიერ პირს აქვს უფლება, დაესწროს ლექციას, შევიდეს აუდიტორიაში და ყოველგვარი ავტორიზებისა და რეგისტრაციის გარეშე მოუსმინოს ლექტორს.

მიუხედავად არსებული განსხვავებისა, როგორც ონლაინ, ისე საუდიტორიო ლექციის დამსწრეთა პერსონალური მონაცემები მათი თანხმობის გარეშე არ უნდა დამუშავდეს/გასაჯაროვდეს. ეს ეხება როგორც სურათის გადაღებას (მით უმეტეს, გავრცელებას), ისე სახელისა და გვარის შესახებ მონაცემების პირთა განუსაზღვრელი წრისთვის მიწოდებას, „Screenshot-ის“ გაკეთებას და ა.შ. თანხმობისთვის კი საჭიროა, ერთი მხრივ, ლექტორის (ორგანიზატორის) მოწოდება (შეთავაზება) ან გარემოების შექმნა, ხოლო, მეორე მხრივ, დამსწრე პირის მხრიდან ნების გამოვლენა (მოწოდებაზე პოზიტიური ქმედება ან უმოქმედობა).

4. სოციალურ ქსელში გავრცელებული მონაცემები

დისტანციური სწავლების დაწყების შემდეგ საქართველოში დაფიქსირდა რამდენიმე შემთხვევა, როდესაც ლექტორმა ან სტუდენტმა სოციალურ ქსელში გაავრცელა „Zoom-ის“ სახით ჩატარებული ლექციის „Screenshot-ი“. უმეტეს შემთხვევაში (როგორც ეს ცნობილია ამ ეტაპზე), მათ დანარჩენ მონაწილეთაგან არ ჰქონდათ აღებული ნებართვა გამოსახულების გავრცელების თაობაზე. შესაბამისად, პერსონალურ მონაცემებზე წვდომის მოპოვება შეძლეს იმ პირებმა, რომლებიც საერთოდ არ იყვნენ კავშირში სალექციო კურსთან (ღონისძიებასთან).

5. ლექციის დამსწრეთა თანხმობა პერსონალურ მონაცემთა გავრცელებაზე

როგორც შესავალში აღინიშნა, სახელმწიფო ინსპექტორის სამსახურმა რეკომენდაცია გასცა, რომ სოციალურ ქსელში (ისევე, როგორც სხვა გზით) ონლაინ-ლექციის ამსახველი ვიდეო-ფოტო მასალის გავრცელებისას გათვალისწინებული უნდა იყოს პერსონალურ მონაცემთა სუბიექტის ინტერესი. ეს კი თავის თავში გულისხმობს ლექციის დამსწრეთა თანხმობის გაცემას. საკითხი სამართლებრივად ექცევა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 (ცალკეულ შემთხვევაში, მე-6) მუხლის ფარგლებში.

თანხმობის გაცემა არ ნიშნავს ხელის მოწერას, რაიმე თანხმობის სპეციალური ფორმით მიწოდებას და ა.შ. ეს შეიძლება მოხდეს რამდენიმე გზით: ა) „Zoom-ის“ ფორმატშივე მიმოწერაში („Chat“) ინდივიდუალური თანხმობის გაცხადებით; ბ) სიტყვიერი თანხმობის გაცხადებით; გ) კონკლუდენტური ქმედებით. ვთქვათ, როდესაც ლექტორი (ადმინისტრატორი/ორგანიზატორი, ასევე, ერთ-ერთი მონაწილე) განა-

ცხადებს, რომ მას სურს ფოტოს („Screenshot-ი“) სახით მასალის გავრცელება და დანარჩენი მონაწილეები (დამსწრეები) დაეთანხმებიან მას (ვთქვათ, თავის დაკვრით და ა.შ.); დ) კონკლუდენტური ქმედების, რაც უმოქმედობაში გამოიხატება — ბოლო მაგალითის მსგავსად, როდესაც მონაწილეები (დამსწრეები) არ გამოთქვამენ საპირისპირო აზრს. შეიძლება, ზოგიერთმა მათგანმა საერთოდ გათიშოს ვიდეოს ჩაწერის სისტემა, მაგრამ არ დატოვოს ღონისძიება და ა.შ.; ე) როდესაც ყველა სხვა დამსწრე (მონაწილე) წინასწარვე გაფრთხილებულია ლექტორის (ან მონაწილის) მიერ, რომ იგი აპირებს ფოტოს ან ვიდეოს გადაღებას და შემდეგ მის გავრცელებას და თუ ამის მიუხედავად, სტუდენტი ჩაერთვება შეხვედრაში, არ გააპროტესტებს მას და გონივრული მოლოდინი ექნება, რომ მისი პერსონალური მონაცემები გასაჯაროვდება.

ანალოგიურ ვითარებასთან გვექნება საქმე ონლაინ-ლექციის ჩაწერის შემთხვევაშიც: ვინაიდან პრაქტიკულად რთულია წინასწარვე რაიმე დარღვევის (შეუსაბამო გამოყენების) აღმოფხვრა, პრევენციული მიზანი უნდა ჰქონდეს ნებართვის აღებას და თანხმობის გაცხადების შემთხვევაში, გონივრულ მოლოდინს. თუმცა, აქაც დასაშვებია გარკვეული პირობების დაწესება: ვიდეოს გამოყენების ფარგლები, შეზღუდვის წინაპირობები და გავრცელების არეალი, რომლის დარღვევამაც შეიძლება გამოიწვიოს პასუხისმგებლობა.

შეჯამება

ნებისმიერი ახალი ტექნოლოგიის გამოყენებას თან ახლავს საკითხი, რომელიც ეხება პერსონალური მონაცემების დაცვას. „Zoom-ის“ გამოყენებით ლექციის ჩატარება არ ნიშნავს, რომ ის პერსონალური მონაცემების დაცვისგან თავისუფალ სივრცეს წარმოადგენს: ასეთ დროს იგივენაირად უნდა იქნეს ნებისმიერი პირის უფლებები დაცული, როგორც ვთქვათ, „Skype-ის“, „Viber-ისა“ და სხვა შემთხვევაში იქნებოდა შესაძლებელი.

ამდენად, წინასწარი თანხმობის (ნების გამოვლენის) არსებობის გარეშე ონლაინ-ლექციის ვიდეო თუ ფოტო მასალის განთავსება წარმოადგენს პერსონალურ მონაცემთა დარღვევას და პირს ამისთვის დაეკისრება პასუხისმგებლობა საქართველოს კანონმდებლობიდან გამომდინარე. ყურადსაღებია, რომ ასეთ დროს არ აქვს მნიშვნელობა, პერსონალური მონაცემის გამავრცელებლის ქმედება პოზიტიურ მიზანს ემსახურებოდა თუ ნეგატიურს. ორივე შემთხვევაში პერსონალურ მონაცემთა დაცვის საკითხია გასათვალისწინებელი.

სერგი ჯორბენაძე