აქსანა გუჩუა
დოქტორანტი
კავკასიის საერთაშორისო უნივერსიტეტი
ელ-ფოსტა: guchua94@gmail.com

ადგილობრივი თვითმმართველობა და პერსონალურ მონაცემთა დაცვა: რეგულირების სტანდარტები და ციფრული რისკები

აბსტრაქტი
თანამედროვე ციფრული ეპოქა ადგილობრივი თვითმმართველობის ორგანოების წინაშე მნიშვნელოვან გამოწვევებს აყენებს, როდესაც მოქალაქეებისთვის ეფექტიანი სერვისების უზრუნველყოფასთან ერთად, პერსონალური მონაცემების დაცვა ცენტრალურ საკითხად ყალიბდება. ადგილობრივი ხელისუფლების მიერ საინფორმაციო სისტემების, ელექტრონული სერვისებისა და „ჭკვიანი ქალაქის“ ტექნოლოგიების დანერგვა ზრდის როგორც დამუშავებული მონაცემების მოცულობას, ასევე კიბერუსაფრთხოების რისკების დონეს. ამდენად, პერსონალური მონაცემების დაცვა აღარ წარმოადგენს მხოლოდ სამართლებრივ ვალდებულებას და იძენს პოლიტიკურ, ტექნოლოგიურ და ეთიკურ განზომილებებს.

სტატიის მიზანია ადგილობრივ თვითმმართველობასა და პერსონალური მონაცემების დაცვის სტანდარტებს შორის ურთიერთკავშირის შესწავლა, ციფრული რისკების იდენტიფიცირება და მოქმედი სამართლებრივი ჩარჩოების ანალიზი. განსაკუთრებული ყურადღება ეთმობა 2024 წელს განხორციელებულ საკანონმდებლო ცვლილებებს, რომლებმაც არსებითად განაახლა როგორც საქართველოს კანონმდებლობა, ასევე ევროკავშირის მონაცემთა დაცვის პრაქტიკა. კვლევა აანალიზებს აღნიშნული ცვლილებების გავლენას ადგილობრივ მმართველობაზე, მათ შესაბამისობას GDPR-ის პრინციპებთან და იმ გამოწვევებს, რომლებიც დაკავშირებულია ტექნოლოგიურ რესურსებთან, ინსტიტუციურ კოორდინაციასა და მოქალაქეთა ნდობასთან.

სტატიაში დასაბუთებულია, რომ მონაცემთა დაცვის პოლიტიკის გაუმჯობესება მოითხოვს არა მხოლოდ საკანონმდებლო ჰარმონიზაციას, არამედ ადგილობრივი ხელისუფლების ინსტიტუციური შესაძლებლობების გაძლიერებას, კვალიფიციური კადრების მომზადებასა და ინფორმაციული უსაფრთხოების კულტურის განვითარებას. დასკვნით ნაწილში წარმოდგენილია კონკრეტული რეკომენდაციები, მათ შორის ადგილობრივი პერსონალური მონაცემების დაცვის სტრატეგიების შემუშავება, ციფრული რისკების პრევენციის მექანიზმების დანერგვა და მოქალაქეთა ჩართულობის ხელშეწყობა. აღნიშნული მიდგომით სტატია სთავაზობს როგორც თეორიულ ხედვებს, ისე პრაქტიკულ ინსტრუმენტებს, რომლებიც ხელს უწყობს მოქალაქეთა უფლებების დაცვას და ციფრულ გარემოში დემოკრატიული მმართველობის გაძლიერებას.

საკვანძო სიტყვები: ადგილობრივი თვითმმართველობა, პერსონალური მონაცემების დაცვა, ციფრული რისკები, მარეგულირებელი სტანდარტები.

შესავალი

თანამედროვე საზოგადოებაში პერსონალური მონაცემები იქცა ერთ-ერთ ყველაზე ღირებულ რესურსად, რომელიც არა მხოლოდ ინდივიდის პირად იდენტობას გამოხატავს, არამედ ციფრული ეკონომიკისა და დემოკრატიული მმართველობის ფუნდამენტურ საფუძველსაც წარმოადგენს. ადგილობრივი თვითმმართველობები, როგორც მოქალაქეებთან უშუალო კავშირის მქონე ინსტიტუციები, ყოველდღიურად ამუშავებენ და ინახავენ მრავალფეროვან პერსონალურ მონაცემს დაწყებული მოსახლეობის რეგისტრაციითა და სოციალური მომსახურებით, დამთავრებული მუნიციპალური სერვისების ციფრულ პლატფორმებზე გადატანით. სწორედ ამ კონტექსტში, პერსონალური მონაცემთა დაცვა იქცა კრიტიკულ საკითხად, რადგან თითოეული დარღვევა უშუალოდ აზიანებს მოქალაქეთა უფლებებსა და ნდობას ადგილობრივი მმართველობის მიმართ.

კვლევის მიზანია გაანალიზდეს, თუ რამდენად შეესაბამება საქართველოს ადგილობრივი თვითმმართველობების პრაქტიკა პერსონალური მონაცემთა დაცვის საერთაშორისო სტანდარტებს, განსაკუთრებით GDPR-ის პრინციპებს, და რა ტიპის ციფრული რისკები იჩენს თავს მმართველობის პროცესში. ამასთან, სტატიაში განიხილება 2024 წელს განხორციელებული საკანონმდებლო ცვლილებების გავლენა მონაცემთა დაცვის ხარისხზე და ადგილობრივი თვითმმართველობების ინსტიტუციურ შესაძლებლობებზე.

საკვლევი კითხვები ფორმულირდება შემდეგნაირად:

1. რამდენად ეფექტიანად ახორციელებენ საქართველოს მუნიციპალიტეტები პერსონალური მონაცემების დაცვის სამართლებრივ ვალდებულებებს?

2. რა ტიპის ციფრული და კიბერუსაფრთხოების რისკები არსებობს ადგილობრივ თვითმმართველობებში?

3. როგორ აისახება მონაცემთა დაცვის პოლიტიკა მოქალაქეთა ნდობასა და დემოკრატიული მმართველობის ხარისხზე?

კვლევა ეფუძნება ორ ძირეულ მიდგომას: პირველი — Institutional Trust Theory, რომლის მიხედვით მოქალაქეთა ნდობა სახელმწიფო ინსტიტუტებისადმი დამოკიდებულია ამ ინსტიტუტების გამჭვირვალობაზე, პასუხისმგებლობასა და სამართლიანობაზე. მონაცემთა დაცვა სწორედ ამ ნდობის ცენტრალური მექანიზმია: როცა მოქალაქეს ეძლევა გარანტია, რომ მისი ინფორმაცია უსაფრთხოდ მუშავდება,

იგი უფრო მეტად იდენტიფიცირდება სახელმწიფოსთან და ზრდის პოლიტიკური მონაწილეობის დონეს.
მეორე — **Digital Era Governance Theory**, რომელიც ხსნის, რომ თანამედროვე მმართველობა ეფუძნება ტექნოლოგიურ გადაწყვეტილებებს, რომლებიც ავითარებენ მომსახურების სიჩქარესა და გამჭვირვალობას, მაგრამ ამავდროულად აჩენენ ახალ საფრთხეებს მონაცემთა გაჟონვის, ტექნიკური ხარვეზებისა და ეთიკური პასუხისმგებლობის erosion-ის ფორმით.

სწორედ ამ ორ თეორიულ ჩარჩოს შორისაა გაბმული სტატიის ანალიტიკური ხაზიც: მონაცემთა დაცვა წარმოდგენილია როგორც დემოკრატიული ნდობის შენარჩუნების ინსტრუმენტი და როგორც ტექნოლოგიური მმართველობის მდგრადობის გარანტი.

ციფრული ეპოქის რეალობაში ადგილობრივი თვითმმართველობები იქცნენ იმ ბირთვად, სადაც იკვეთება ტექნოლოგიური ინოვაცია და სამართლებრივი პასუხისმგებლობა. მუნიციპალიტეტები ყოველდღიურად ამუშავებენ დიდ მოცულობის მონაცემებს რეგისტრაციიდან დაწყებული სოციალური მომსახურებითა და მუნიციპალური სერვისების მართვით დამთავრებული. ამ მონაცემთა დიდი ნაწილი შეიცავს მოქალაქეთა პირად ინფორმაციას, რაც ზრდის როგორც მათი დაცვითი მექანიზმების მნიშვნელობას, ისე დარღვევის შემთხვევაში პოლიტიკური და სოციალური ზიანის საფრთხეს.

2024 წელს მიღებულმა საკანონმდებლო ცვლილებებმა როგორც საქართველოს, ასევე ევროკავშირის სივრცეში ახალი დინამიკა შესძინა მონაცემთა დაცვის სფეროს. საქართველოს კანონში „პერსონალურ მონაცემთა დაცვის შესახებ“ განხორციელებული ცვლილებები უფრო მკაფიოდ განსაზღვრავს ადგილობრივი თვითმმართველობების ვალდებულებებს, განსაკუთრებით კი მონაცემთა უსაფრთხოების უზრუნველყოფისა და მონაცემთა სუბიექტის უფლებების დაცვის მიმართულებით.

საკანონმდებლო ჩარჩოს გაძლიერება თავისთავად საკმარისი არ არის. პრობლემის არსი მდგომარეობს იმაში, რომ ადგილობრივ თვითმმართველობებს სჭირდებათ არა მხოლოდ ნორმატიული მოთხოვნების შესრულება, არამედ მონაცემთა დაცვის კულტურის ჩამოყალიბება. ეს გულისხმობს ინსტიტუციურ პასუხისმგებლობას, სპეციალისტების გადამზადებას, ტექნოლოგიური გადაწყვეტილებების დანერგვას და მოქალაქეთა ინფორმირებულობის ამაღლებას. მოქალაქეებისთვის მნიშვნელოვანია იცოდნენ, რომ მათი მონაცემები დაცულია, ხოლო თვითმმართველობებისთვის აუცილებელია აღიარონ,

რომ მონაცემთა დაცვა არა მხოლოდ იურიდიული მოვალეობაა, არამედ ნდობის შენარჩუნების უმთავრესი საფუძველი.

პერსონალური მონაცემთა დაცვა ადგილობრივი თვითმმართველობებისთვის არის არა მხოლოდ სამართლებრივი მოთხოვნა, არამედ ერთ-ერთი უმთავრესი გამოწვევა, რომელიც განსაზღვრავს როგორც ინსტიტუციური გამჭვირვალობის ხარისხს, ასევე დემოკრატიული მმართველობის ხარისხს.

ადგილობრივი თვითმმართველობა და პერსონალური მონაცემთა დაცვის სამართლებრივი ჩარჩო

პერსონალური მონაცემები თანამედროვე საზოგადოებაში წარმოადგენს ერთ-ერთ ყველაზე მნიშვნელოვან რესურსს, რომელიც განსაზღვრავს ინდივიდის პირად იდენტობას, საჯარო სერვისების ეფექტიანობასა და დემოკრატიული მმართველობის ხარისხს (Westin, 2015). ადგილობრივი თვითმმართველობები, რომლებიც ყოველდღიურ ურთიერთობაში არიან მოქალაქეებთან და აწარმოებენ მრავალფეროვან სერვისებს, განსაკუთრებულად მაღალი ინტენსივობით ამუშავებენ პირად ინფორმაციას, დაწყებული სოციალური პროგრამების ბენეფიციართა მონაცემებიდან, დამთავრებული საჯარო რეგისტრებისა და ციფრული მომსახურებების დიდი მოცულობის ჩანაწერებით (ჩიქვაიძე & წერეთელი, 2022). სწორედ ამიტომ მონაცემთა დაცვისა და უსაფრთხოების უზრუნველყოფა ადგილობრივ მმართველობაში არა მხოლოდ ტექნიკური მოვალეობა, არამედ დემოკრატიული მმართველობის, ინსტიტუციური ნდობისა და სახელმწიფო პოლიტიკის მდგრადობის ფუნდამენტური განმსაზღვრელი ხდება.

კვლევის ძირითადი მიზანი ამ კონტექსტში მდგომარეობს იმაში, რომ შეფასდეს საქართველოს ადგილობრივი თვითმმართველობების კანონმდებლობით განსაზღვრული ვალდებულებებისა და რეალური პრაქტიკის შესაბამისობა საერთაშორისო სტანდარტებთან, განსაკუთრებით ევროკავშირის ზოგადი მონაცემთა დაცვის რეგულაციასთან (GDPR), რომელიც გლობალური პლატფორმაა მონაცემთა დაცვის პრინციპების თანამედროვე ინტერპრეტაციისთვის (Dunleavy, 2006). საკვლევი პრობლემა კი სწორედ იმ კრიტიკულ აცდენაზეა ფოკუსირებული, რომელიც აღინიშნება ფორმალურ სამართლებრივ ჩარჩოსა და მისი პრაქტიკული აღსრულების ხარისხს შორის, მიუხედავად იმისა, რომ კანონმდებლობის ტექსტი ბოლო წლებში მნიშვნელოვნად ჰარმონიზებულია ევროპულ სტანდარტებთან (ჩიქვაიძე, 2019), ადგილობრივი თვითმმართველობები ხშირად ვერ ახერხებენ ამ სტანდარტების იმპლემენტაციას რესურსების სიმწირის,

ტექნოლოგიური ინფრასტრუქტურის ასაკის, ადამიანური კაპიტალის ნაკლებობისა და მონაცემთა დაცვის ორგანიზაციული კულტურის დაუმკვიდრებლობის გამო.

თეორიული ჩარჩო, რომელზეც ეს ანალიზი დგას, ეფუძნება როგორც ინსტიტუციური ნდობის თეორიას (Mayer, 1995), ასევე ციფრული ეპოქის მმართველობის თეორიას (Dunleavy, 2006). ორივე მიმართულება ხაზს უსვამს იმას, რომ თანამედროვე საჯარო სისტემა მოქალაქის თვალში სანდო ხდება მხოლოდ მაშინ, როდესაც ინფორმაცია მოძრაობს გამჭვირვალედ, უსაფრთხოდ და ინტეგრირებულად; ხოლო ნებისმიერი მონაცემთა დარღვევა ან სისტემური სისუსტე პირდაპირ აზიანებს მოქალაქეთა ნდობას და ამცირებს ინსტიტუციის ლეგიტიმაციას. სწორედ ეს თეორიული ხედვა განაპირობებს იმას, რომ ადგილობრივი თვითმმართველობების მონაცემთა დამუშავება არ შეიძლება მოიაზრებოდეს მხოლოდ ტექნიკურ პროცედურად ის წარმოადგენს დემოკრატიული მმართველობის იმ კომპონენტს, რომელიც მწვანე შუქს ან წითელ ხაზს უთამაშებს მოქალაქის სახელმწიფოსადმი დამოკიდებულებას.

საქართველოს სამართლებრივი ჩარჩო პერსონალური მონაცემების დაცვის მიმართულებით სათავეს იღებს 2011 წლის კანონით (საქართველოს კანონი, 2011), თუმცა მისი პრაქტიკული გამოყენება განსაკუთრებით რთული აღმოჩნდა თვითმმართველობებისთვის, რომელებსაც აკლდათ როგორც ტექნიკური უნარები, ისე ადამიანური რესურსი. 2024 წლის საკანონმდებლო ცვლილებები მნიშვნელოვანი ნაბიჯია ამ პრობლემების ნაწილის აღმოფხვრისკენ: ისინი ამკაცრებენ ადგილობრივი თვითმმართველობების ანგარიშვალდებულებას, ამწესებენ მონაცემთა დამუშავების რეგისტრების ვალდებულებას, უზრუნველყოფენ მონაცემთა დაცვის ოფიცრების ინსტიტუციურ დაფუძნებას და ავალდებულებენ უსაფრთხოების პოლიტიკის ფორმალურ არსებობას. მიუხედავად ამისა, საერთაშორისო სტანდარტებთან შედარება ცხადყოფს, რომ ხშირად ეს ნაბიჯები უფრო ფორმალურია, ვიდრე რეალისტურად შესრულებადი (საქართველოს კანონი, 2024). GDPR-ის პრინციპები — მინიმიზაცია, გამჭვირვალობა, პროპორციულობა, ანგარიშვალდებულება — ადგილობრივი თვითმმართველობების პრაქტიკაში დიდწილად ბუნდოვნად არის მიჩენილი (European Union, 2016). მაგალითად, მონაცემთა მინიმიზაციის პრინციპი იშვიათადაა სრულად დაცული, რადგან პერსონალური მონაცემების მოპოვებისას მუნიციპალიტეტები ხშირად ითხოვენ იმაზე მეტ ინფორმაციას, ვიდრე მიზნიდან გამომდინარეა აუცილებელია (UN Department of Economic and Social Affairs, 2022). ანგარიშვალდებულების პრინციპის შესრულება ასევე პრობლემურია: მონაცემთა დაცვის

ოფიცრები ბევრ მუნიციპალიტეტში ნომინალური ფუნქციით არსებობენ და მათი ინსტიტუციური დამოუკიდებლობა შეზღუდულია.

პრაქტიკული დასკვნები მკაფიოდ ჩანს საერთაშორისო შედარებითაც. EGDI–ს (UN E-Government Development Index) 2022 წლის მონაცემებით, საქართველო მაღალი კატეგორიის ქვეყანაა, თუმცა ადგილობრივი სერვისების ხარისხის მაჩვენებელში (Local Online Services Index) წვდომის, უსაფრთხოებისა და ინტეგრირებულობის კუთხით კვლავაც შეიმჩნევა მნიშვნელოვანი პრობლემები (OECD, 2020). OECD-ის კვლევები მიუთითებს, რომ ადგილობრივი დონე საქართველოში ინფორმაციული უსაფრთხოების სფეროში კვლავ ფრაგმენტირებულია (European Data Protection Board, 2023), ხოლო ევროკავშირის მონაცემთა დაცვის საბჭოს (EDPB) 2023 წლის აუდიტის სახელმძღვანელო ცხადყოფს, რომ თვითმმართველობები განსაკუთრებით მოწყვლადნი არიან სოციალური ინჟინერიის, არასაკმარისი დაშიფვრისა და არასაკმარისი თანამშრომლობის მომზადების კუთხით. ეს მაჩვენებლები ნათლად აჩვენებს, რომ საკანონმდებლო ჰარმონიზაცია თავისთავად ვერ უზრუნველყოფს მაღალი სტანდარტის პრაქტიკას, თუ მას არ გაყვება სერიოზული ორგანიზაციული და ტექნოლოგიური გაძლიერება.

საერთაშორისო გამოცდილებაც ადასტურებს, რომ ეფექტური მონაცემთა დაცვის სისტემა ადგილობრივ დონეზე მაშინ მუშაობს, როდესაც სამართლებრივი ჩარჩო გამყარებულია ტექნოლოგიურ ინფრასტრუქტურასა და ადამიანური კაპიტალის გამყარებაზე. ესტონეთში ერთიანი პლატფორმის X-road-ის საშუალებით ყველა მუნიციპალური სერვისი დაცული და სტანდარტიზებულია, ფინეთში ადგილობრივი ბიუჯეტის მნიშვნელოვან ნაწილს მონაცემთა უსაფრთხოება და კიბერუსაფრთხოება შეადგენს, ნიდერლანდებში DPO-ს ინსტიტუციური დამოუკიდებლობა გარანტირებულია (OECD, 2020). ამ გამოცდილებების შედარება ცხადყოფს, რომ საქართველოს მუნიციპალიტეტებს ჯერ კიდევ აკლიათ სტრუქტურული მდგრადობა, რაც ხელს უშლის კანონმდებლობის ეფექტურ შესრულებას.

ამდენად, ადგილობრივი თვითმმართველობების მონაცემთა დამუშავების პროცესების ანალიზი აჩვენებს, რომ თუნდაც კარგად ჩამოყალიბებული სამართლებრივი ჩარჩო არ არის საკმარისი, როდესაც დამუშავების პროცესი მექანიკურად ხორციელდება, ხოლო მისი უსაფრთხოებისა და ანგარიშვალდებულების ელემენტები ფაქტობრივად არ არის უზრუნველყოფილი. სპეციფიკურად ადგილობრივი თვითმმართველობების შემთხვევაში პრობლემად რჩება კადრების კვალიფიკაცია, ტექნოლოგიური ინფრასტრუქტურის დისკრეციული დონე, ერთიანი სტანდარტების არქონა და მონაცემთა დაცვის

კულტურის არასაკმარისი განვითარება. ეს ყველაფერი კიდევ ერთხელ ცხადყოფს, რომ პერსონალური მონაცემების დაცვა თანამედროვე პირობებში მხოლოდ სამართლებრივი ვალდებულება კი არა, არამედ ინსტიტუციური და საზოგადოებრივი პასუხისმგებლობაა, რომლის ეფექტიანობაც საბოლოოდ განაპირობებს სახელმწიფო მმართველობისადმი ნდობის ხარისხს.

ციფრული რისკები და მონაცემთა უსაფრთხოება ადგილობრივ მმართველობაში

ციფრული ტრანსფორმაციის პირობებში ადგილობრივი თვითმმართველობა გადაიქცა სისტემად, რომლის საქმიანობაც მნიშვნელოვნად ეფუძნება დიდი მოცულობისა და მაღალსენსიტიური პერსონალური მონაცემების ყოველდღიურ დამუშავებას. ელექტრონული სერვისები, „ჭკვიანი ქალაქების“ ტექნოლოგიები და მონაცემთა ინტენსიური ინფრასტრუქტურა ზრდის მუნიციპალიტეტების მუშაობის ეფექტურობას, მაგრამ ერთდროულად აჩენს ახალ, რთულ გამოწვევებს პერსონალური მონაცემების დაცვის კუთხით (OECD, 2020).

საქართველოში ციფრული რისკების ერთ-ერთი ყველაზე თვალსაჩინო წყაროა მონაცემთა გაჟონვა, რომელიც შესაძლოა გამოწვეული იყოს როგორც ტექნიკური ხარვეზით, ისე ადამიანური შეცდომით. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის ანგარიშის მიხედვით, მუნიციპალიტეტებში დაფიქსირებული მონაცემთა დარღვევების 41% უკავშირდებოდა არასაკმარის დაშიფვრას და წვდომის კონტროლის არაეფექტიანობას (Personal Data Protection Service, 2023). ჰაკერული შეტევებიც მნიშვნელოვანი საფრთხეა: CERT-ის მონაცემებით, ადგილობრივი თვითმმართველობების მიმართ განხორციელებული კიბერშეტევების 38% იყო ransomware ტიპის თავდასხმა, რომელიც ცდილობდა სოციალური და ფინანსური მონაცემების დაბლოკვას (Digital Governance Agency, 2023). ამასთანავე, სოციალური ინჟინერია — ფიშინგ შეტევები, ცრუ შეტყობინებები და მოტყუებითი წვდომის მოთხოვნები — საქართველოს მუნიციპალიტეტებში განსაკუთრებით მაღალია, 2023 წლის ფიშინგ-სიმულაციამ აჩვენა, რომ თანამშრომელთა 61% შეცდომით გადასცემს სისტემაზე წვდომის ინფორმაციას, რაც მიუთითებს ტექნოლოგიური განათლებისა და ინფორმაციული კულტურის ნაკლებობაზე.

გაციფრულებამ შეცვალა რისკების მასშტაბიც და ხასიათიც: ინტეგრირებულმა პლატფორმებმა, API-ებზე დაფუძნებულმა მონაცემთა გაცვლამ და ერთიანი რეესტრების გამოყენებამ მნიშვნელოვნად გაზარდა

დაუცველობის წერტილები. როგორც კუნერი აღნიშნავს, მოწინავე ტექნოლოგიების გამოყენება ავტომატურად არ ნიშნავს მაღალ დონეზე დაცვას, პირიქით სისტემებს შორის ინტეგრაცია ქმნის ერთიანი ჩავარდნის რისკს, როცა ერთ სისტემაში ხარვეზი გავლენას ახდენს სხვებზეც (Kuner, 2020). სწორედ ეს რეალობა აჩვენებს, რომ ადგილობრივი თვითმმართველობებისთვის მხოლოდ ტექნოლოგიური განახლება საკმარისი არ არის, საჭიროა უსაფრთხოების პოლიტიკის, პასუხისმგებლობების და შიდა კონტროლის მექანიზმების სისტემური გამკაცრება.

საქართველოს მუნიციპალიტეტებში პრევენციული მექანიზმები არსებობს, თუმცა ისინი ხშირად ფორმალურადაა დანერგილი. 2024 წლის საკანონმდებლო ცვლილებებით მუნიციპალიტეტებს დაეკისრათ მონაცემთა დაცვის ოფიცრის დანიშვნის, მონაცემთა დამუშავების რეგისტრის წარმოებისა და უსაფრთხოების პოლიტიკის არსებობის ვალდებულება (საქართველოს კანონი, 2024). მიუხედავად ამისა, 2023 წლის მონიტორინგი აჩვენებს, რომ 64 მუნიციპალიტეტიდან მხოლოდ 27 ფლობდა სრულყოფილად დოკუმენტირებულ უსაფრთხოების პოლიტიკას, ხოლო ოფიცრების დიდი ნაწილი არ ატარებდა სამსახურებრივი დამოუკიდებლობისა და სისტემური აუდიტის პრაქტიკას. ეს მიუთითებს, რომ სამართლებრივი ვალდებულებები ხშირად ფორმალურად სრულდება, თუმცა რეალური დაცვის ხარისხი დაბალია, რაც ეწინააღმდეგება GDPR–ის პრინციპებს, განსაკუთრებით მინიმიზაციის, გამჭვირვალობისა და ანგარიშვალდებულების ნაწილში (European Union, 2016).

საერთაშორისო გამოცდილება ამ კონტექსტში განსაკუთრებით მნიშვნელოვანი შედარებითი რესურსია. ესტონეთში X-road სისტემა უზრუნველყოფს მონაცემთა გაცვლას end-to-end დაშიფვრით, ხოლო ყველა მუნიციპალიტეტი თავს იყრის ერთიან უსაფრთხოების სტანდარტთან; ფინეთში კი ადგილობრივი ბიუჯეტების 8–12% ხმარდება კიბერუსაფრთხოების მიმართულებას, რაც მნიშვნელოვნად ამცირებს თავდასხმების წარმატების მაჩვენებელს; პოლონეთში მოქმედი ერთიანი SOC (Security Operations Center) მუნიციპალიტეტებს 24/7 რეჟიმში უწევს მონიტორინგს და რეაგირებას (OECD, 2020). აღნიშნული მაგალითები აჩვენებს, რომ ეფექტურობა იქ იქმნება, სადაც ტექნოლოგიური, ინსტიტუციური და სამართლებრივი კომპონენტები ერთიან სისტემად მუშაობს.

საქართველოს რეალობა კი განსხვავებულია: EGDI–ს (UN E-Government Development Index) 2022 წლის მიხედვით, ქვეყანა მაღალი კატეგორიის ქვეყნებს შორისაა, თუმცა ადგილობრივი სერვისების ხარისხის

მაჩვენებელი (Local Online Services Index) კვლავაც მიუთითებს უსაფრთხოების, მონაცემთა ინტეგრირებულობისა და მომსახურებების სტანდარტიზაციის პრობლემებზე. OECD–ის შეფასებაც მიუთითებს, რომ ადგილობრივ დონეზე ინფორმაციული უსაფრთხოება ფრაგმენტირებულია და არ მოიცავს უწყვეტ მონიტორინგს (OECD, 2020). ეს ცხადყოფს, რომ მხოლოდ საკანონმდებლო ჰარმონიზაცია ვერ ქმნის რეალურ დაცვას, თუ მას არ ერთვის ტექნოლოგიური და ადამიანური რესურსების ზრდა.

ციფრული რისკების მართვის პროცესში მოქალაქეთა ნდობა ერთ-ერთი ყველაზე მნიშვნელოვანი ფაქტორია. ინსტიტუციური ნდობის თეორია მიუთითებს, რომ საჯარო ინსტიტუტებისადმი ნდობა იზრდება მაშინ, როდესაც მოქალაქეები დარწმუნებული არიან, რომ მათი მონაცემები უსაფრთხოდაა დაცული (Mayer, Davis, & Schoorman, 1995). საკუთარი მონაცემების გაუცნობიერებელი დაკარგვა ან არასწორი გამოყენება კი იწვევს არა მხოლოდ ტექნიკურ ზიანს, არამედ დემოკრატიული ლეგიტიმაციის შემცირებასაც (Personal Data Protection Service, 2023). ეს საქართველოს პრაქტიკაშიც ჩანს: მონაცემთა გაჟონვის შემდეგ მუნიციპალიტეტებში ელექტრონული სერვისების გამოყენება შეამცირა, ხოლო მოქალაქეთა მონაწილეობა ონლაინ პლატფორმებში მკვეთრად დაეცა.

ციფრული რისკები ადგილობრივ მმართველობაში არ არის მხოლოდ ტექნოლოგიური გამოწვევა, ეს არის სამართლებრივი, ინსტიტუციური და სოციალური საკითხების ერთობლიობა, რომელიც მოითხოვს სისტემურ, მრავალსაფეხურიან მიდგომას. საქართველოს მუნიციპალიტეტებისთვის კრიტიკულია ტექნოლოგიური ინფრასტრუქტურის განახლება, თანამშრომელთა გადამზადება, უსაფრთხოების პოლიტიკის სრულყოფილი იმპლემენტაცია და მოქალაქეთა ინფორმირების სისტემური გაძლიერება. მხოლოდ ამ პირობებში შეძლებს სამართლებრივი ჩარჩო, მათ შორის 2024 წლის ცვლილებები რეალურად უზრუნველყოს მონაცემთა უსაფრთხოება და ხელი შეუწყოს ნდობის ზრდას, რაც დემოკრატიული მმართველობის ფუნქციონირებისთვის ფუნდამენტურია.

მონაცემთა დაცვის სტანდარტების გაძლიერების გზები და რეკომენდაციები

ადგილობრივ თვითმმართველობებში პერსონალური მონაცემების დაცვის სისტემა 2024 წელს პერსონალურ მონაცემთა შესახებ ორგანულ

კანონში განხორციელებული ცვლილებების შემდეგ გარდაიქმნა ერთ-ერთ ყველაზე პრიორიტეტულ მიმართულებად, რადგან სწორედ მუნიციპალიტეტები იქცნენ მონაცემების ინტენსიური დამუშავების ცენტრებად. ახალი რედაქცია მნიშვნელოვნად ამკაცრებს მოთხოვნებს უსაფრთხოების პოლიტიკის, მონაცემთა დამუშავების გამჭვირვალობისა და ანგარიშვალდებულების მიმართულებით (Mayer, Davis და Schoorman 1995). თეორიული ჩარჩო ეფუძნება ინსტიტუციური ნდობის თეორიას, რომლის მიხედვით მოქალაქეთა ნდობა საჯარო ინსტიტუტებისადმი მათი ქმედებების პროგნოზირებადობასა და უსაფრთხოების ხარისხზეა დამოკიდებული და Digital Era Governance Theory-ს, რომელიც აჩვენებს, რომ მონაცემებზე დაფუძნებული მმართველობა მოითხოვს ტექნოლოგიური და ინსტიტუციური სტანდარტების მდგრად ინტეგრაციას. ადგილობრივი თვითმმართველობებისთვის ეს თეორიული ჩარჩო განსაკუთრებით აქტუალურია, რადგან მონაცემთა დამუშავება და მოქალაქეებთან ყოველდღიური კომუნიკაცია ქმნის მაღალ რისკებს, რომლებიც მხოლოდ სამართლებრივი ან ტექნიკური მიდგომებით ვერ გადაწყდება.

საერთაშორისო ინდექსების მიერ ფიქსირებული ტენდენციები ცხადყოფს, რომ მონაცემთა უსაფრთხოება ადგილობრივი თვითმმართველობების ერთ-ერთ ყველაზე სუსტი რგოლია: EGDI-სა და EPI-ის შეფასებებით, ადგილობრივი სერვისების დონეზე დაცულობა დაბალია, ხოლო პროცესების სტანდარტიზაცია — არათანაბარი. აღნიშნულმა გარემოებებმა აუცილებელი გახადა მონაცემთა დაცვის სტანდარტების ადეკვატური გაძლიერება, რათა მუნიციპალიტეტებმა შეძლონ ციფრული რისკების მართვა გრძელვადიანი სტრატეგიული მიდგომით. კვლევის თეორიული ჩარჩო ეყრდნობა ინსტიტუციური ნდობის თეორიას, რომლის მიხედვით საჯარო ინსტიტუტებისადმი ნდობა უზრუნველყოფილი დაცვის ხარისხზეა დამოკიდებულ (Mayer, Davis და Schoorman 1995) და Digital Era Governance-ის თეორიას, რომელიც ხაზს უსვამს, რომ მონაცემებზე დაფუძნებული მმართველობა მოითხოვს მაღალი ხარისხის ტექნოლოგიურ და ორგანიზაციულ სტანდარტებს (Dunleavy, 2006). შესაბამისად, რეკომენდაციების წარმოდგენა ეფუძნება როგორც თეორიულ მიდგომებს, ისე არსებული მონაცემების რაოდენობრივი და ხარისხობრივი ანალიზს.

ციფრული ტრანსფორმაციის პირობებში მონაცემთა დაცვის სტანდარტების გაძლიერება ადგილობრივ თვითმმართველობებში წარმოადგენს ერთ-ერთ ყველაზე მნიშვნელოვან გამოწვევას. ეფექტური მონაცემთა დაცვის პოლიტიკა მოითხოვს სამ სტრატეგიულ კომპონენტს: სამართლებრივი ჰარმონიზაცია, ინსტიტუციური ორგანიზაცია და ტექნოლოგიური უზრუნველყოფა. სამართლებრივი ჰარმონიზაციის

ნაწილი გულისხმობს ადგილობრივი ნორმატიული ჩარჩოს დახვეწას, რათა მონაცემთა დაცვის რეგულაციები იყოს ადაპტირებული არა მხოლოდ ეროვნული, არამედ საერთაშორისო სტანდარტებთან, განსაკუთრებით GDPR–თან (European Union, 2016). საქართველოს კანონპროექტის 2024 წლის ცვლილებები მნიშვნელოვანი წინგადადგმული ნაბიჯია ამ მიმართულებით, რადგან ისინი ადგენენ მონაცემთა დამუშავების უფრო მკაფიო წესებს, ადგილობრივითვითმმართველობებისთვის ვალდებულებებს უსაფრთხოების უზრუნველყოფასა და მოქალაქეთა უფლებების დაცვაზე (საქართველოს კანონპროექტი, 2024).

საერთაშორისო ინდექსების მიხედვით, საქართველო ციფრული მმართველობის სფეროში მნიშვნელოვან პროგრესს აჩვენებს, თუმცა ადგილობრივი თვითმმართველობების დონეზე სურათი კვლავ არასაკმარისად სტაბილურია. EGDI–ს 2022 წლის ანგარიშის მიხედვით, საქართველო მოხვდა „High E-Government Development Index“ კატეგორიაში (UN DESA, 2022), თუმცა „Local Online Services Index“-ის ქვეკატეგორიაში მონაცემთა უსაფრთხოებისა და ინტეგრირებულობის მაჩვენებლები მნიშვნელოვნად ჩამოუვარდება ცენტრალურ ინსტიტუტებს. EPI-ს (E-Participation Index) მიხედვით, მოქალაქეთა ჩართულობა იზრდება, თუმცა კვლავ დაბალია ადგილობრივი სერვისების მიმართ ნდობა, რაც ნაწილობრივ განპირობებულია უსაფრთხოების დარღვევებითა და ინციდენტებზე რეაგირების არასისტემურობით.

ციფრული მმართველობის სააგენტოს (DEG) მიერ 2023–2024 წლებში გამოქვეყნებული მონაცემები ცხადყოფს, რომ საქართველოს 64 მუნიციპალიტეტიდან 49-ს არ აქვს სრულყოფილი მონაცემთა დაცვის პოლიტიკა, ხოლო 37 მუნიციპალიტეტში მონაცემთა დაცვის ოფიცრის ფუნქცია ფორმალურადაა დაკისრებული, თუმცა არ არის გამყარებული ინსტიტუციური რესურსით. სააგენტოს აღწერით, ყველაზე ხშირი პრობლემებია: მოძველებული ინფრასტრუქტურა, სუსტი დაშიფვრა, ადმინის ანგარიშების დაუცველობა, და თანამშრომლების არასაკმარისი მომზადება (Digital Governance Agency, 2024). მსგავსი ტენდენციები დაფიქსირებულია სახელმწიფო აუდიტის სამსახურის 2023 წლის ანგარიშშიც (State Audit Office of Georgia, 2023), სადაც დგინდება, რომ ადგილობრივი თვითმმართველობების 60%-ში მონაცემთა დამუშავების პროცესები განხორციელებულია დაუკანონებელი შიდა წესებით.

ზემოაღნიშნული პრობლემების გათვალისწინებით, კვლევის მიზანი იყო დაედგინა, თუ რამდენად შეესაბამება ადგილობრივი თვითმმართველობების პრაქტიკა საერთაშორისო სტანდარტებს,

კერძოდ GDPR-ის პრინციპებს. ანალიზმა აჩვენა, რომ კრიტიკული გამოწვევებია: მინიმიზაციის პრინციპის დაუცველობა, არასაკმარისი ანგარიშვალდებულება, დაუბალანსებელი წვდომის უფლებები, სუსტი ტექნიკური უსაფრთხოება და ინციდენტებზე რეაგირების არასისტემურობა. მეთოდოლოგიურად, კვლევა ეფუძნებოდა მეორეული მონაცემების ანალიზს (EGDI, DEG-ის ანგარიშები, UNDESA ინდექსები, OECD-ის ანგარიშები) და მიღებული მონაცემები წარმოადგენს საფუძველს რეკომენდაციების ჩამოსაყალიბებლად. თუმცა კვლევის შეზღუდვა მდგომარეობს პირველადი, ადგილობრივი ემპირიული მონაცემების სიმწირეში, რაც მომავალში კვლევის გაფართოებას საჭიროებს.

ადგილობრივი თვითმმართველობების დონეზე მონაცემთა დაცვის გაძლიერების პირველი სტრატეგიული ნაბიჯია სამართლებრივი ჰარმონიზაცია. 2024 წლის საკანონმდებლო ცვლილებები, რომლებიც ადგენს უფრო მკაფიო წესებს მონაცემთა დამუშავებისას და ავალდებულებს უსაფრთხოების პოლიტიკის შემუშავებას, წარმოადგენს მნიშვნელოვან წინგადადგმულ ნაბიჯს, თუმცა მათი ეფექტიანობა დამოკიდებულია იმაზე, შეძლებენ თუ არა მუნიციპალიტეტები შესაბამისი პროცედურების პრაქტიკულ დანერგვას (UN DESA, 2022). ჰარმონიზაციის პროცესში მნიშვნელოვანია GDPR–ის პრინციპების ინტეგრირება, მათ შორის ანგარიშვალდებულების, გამჭვირვალობისა და პროპორციულობის უზრუნველყოფა, რაც ადგილობრივ დონეზე ჯერ კიდევ არასრულყოფილად ხორციელდება.

მეორე კრიტიკული მიმართულებაა მონაცემთა დაცვის ოფიცრის ინსტიტუციონალიზაცია. არსებული მონაცემებით, ბევრ მუნიციპალიტეტში ოფიცრის როლი მხოლოდ ფორმალური სახით არსებობს და მას არ აქვს საკმარისი დამოუკიდებლობა, რესურსი ან უფლებამოსილება (OECD, 2021). ეფექტური მოდელი მოითხოვს, რომ DPO იყოს შიდა კონტროლის მექანიზმის ნაწილი, ჰქონდეს წვდომა ყველა ინფორმაციულ სისტემასთან და რეგულარულად აწარმოებდეს მონიტორინგს, ინციდენტების აღრიცხვას და თანამშრომელთა განმზადებას. ესტონეთისა და ნიდერლანდების პრაქტიკა ადასტურებს, რომ DPO-ს ძლიერი ინსტიტუციური პოზიცია მნიშვნელოვნად ზრდის სერვისების უსაფრთხოებას და მოქალაქეთა ნდობას.

მესამე აუცილებელი კომპონენტია ტექნოლოგიური უზრუნველყოფა: დაშიფვრა, ქსელის სეგმენტაცია, მრავალფაქტორიანი აუთენტიფიკაცია, სისტემური აუდიტები და ხელოვნური ინტელექტის ეთიკური გამოყენება (Floridi & Taddeo, 2018). AI–ზე დაფუძნებული ანალიტიკური ინსტრუმენტები, როგორიცაა ავტომატური დაბრკოლებების

იდენტიფიკაცია ან ანონიმიზაციის ალგორითმები, უნდა გამოყენებულ იქნას დასაბუთებული და ეთიკური ჩარჩოების ფარგლებში, რათა თავიდან იქნეს აცილებული მონაცემთა შეუფერებელი ან დისკრიმინაციული დამუშავება.

მეოთხე მიმართულებაა თანამშრომელთა რეგულარული გადამზადება. არსებული კვლევები აჩვენებს, რომ კიბერშეტევების 70%-ზე მეტი დაკავშირებულია ადამიანის ფაქტორთან (ENISA-ს, 2023), რაც ადგილობრივი თვითმმართველობებისთვის განსაკუთრებით რისკიანია. ტრენინგების სისტემატურობა, პრაქტიკული სწავლება, უსაფრთხოების პროცედურების გაცნობა და თანამშრომელთა ცნობიერების ამაღლება წარმოადგენს კრიტიკულ ფაქტორს.

მეხუთე აუცილებელი მიმართულებაა მოქალაქეთა ინფორმირებულობა და ნდობის გაძლიერება. EPI-ის მონაცემებით, საქართველოში მოქალაქეთა მონაწილეობა ციფრულ სერვისებში იზრდება, თუმცა ნდობის დონე კვლავ სუსტია (UN DESA-ს, 2022). ნდობის გაძლიერება შესაძლებელია გამჭვირვალე კომუნიკაციის გზით, მონაცემთა დამუშავების პროცედურების საჯაროობით, მარტივად გასაგები კონფიდენციალურობის პოლიტიკების შემუშავებითა და მოქალაქეთა ინფორმირების აქტიური კამპანიებით.

ამრიგად, მონაცემთა დაცვის სტანდარტების გაძლიერება ადგილობრივ თვითმმართველობებში მოითხოვს სამართლებრივი, ტექნოლოგიური, ინსტიტუციური და სოციალური კომპონენტების ინტეგრირებულ, კომპლექსურ მიდგომას. მხოლოდ 2024 წლის საკანონმდებლო ცვლილებები საკმარისი არ არის. წარმატების მიღწევა დამოკიდებულია მრავალშრიან რეფორმაზე, რომელიც მოიცავს ევროპულ სტანდარტებთან შესაბამისობას, ტექნოლოგიურ მოდერნიზაციას, თანამშრომელთა უწყვეტ განათლებას და მოქალაქეთა ნდობის გამყარებას. ასეთ შემთხვევაში ადგილობრივი თვითმმართველობები შეძლებენ ციფრული ეპოქის გამოწვევებთან გამკლავებას და უზრუნველყონ მოქალაქეთა პერსონალური მონაცემების რეალური, არა მხოლოდ ფორმალური დაცვა.

დასკვნა

პერსონალური მონაცემების დაცვის სისტემის ანალიზმა ადგილობრივი თვითმმართველობების დონეზე მკაფიოდ აჩინა ის სტრუქტურული დისბალანსი, რომელიც არსებობს სამართლებრივ მოთხოვნებსა და მათი პრაქტიკული აღსრულების შესაძლებლობებს შორის. მიუხედავად იმისა, რომ 2024 წელს მიღებულმა საკანონმდებლო ცვლილებებმა

მნიშვნელოვნად განაახლა ნორმატიული ჩარჩო და დააწესა უფრო მკაფიო პასუხისმგებლობები, კვლევის პროცესმა ცხადყო, რომ მუნიციპალიტეტებში მონაცემთა დაცვის პრაქტიკა კვლავ ფრაგმენტირებულია, სტანდარტიზაციის გარეშე და სუსტი ინსტიტუციური რესურსებით. ემპირიული მონაცემების სიმწირე, როგორც ინციდენტებზე რეაგირების სტატისტიკის, ისე მოქალაქეთა ნდობის დინამიკის თვალსაზრისით, ხელს უშლის სისტემური პრობლემების სრულფასოვან შეფასებას და ასუსტებს მუნიციპალიტეტების შესაძლებლობას, ადეკვატურად მართონ ციფრული რისკები. ეს დეფიციტი განსაკუთრებით საყურადღებოა იმ პირობებში, როდესაც ადგილობრივი თვითმმართველობები ყოველდღიურად ახორციელებენ მაღალი სენსიტიურობის მონაცემთა დამუშავებას, თუმცა ტექნოლოგიური ინფრასტრუქტურა, უსაფრთხოების მექანიზმები და ადამიანური კაპიტალი ვერ უზრუნველყოფს მაღალი სტანდარტების დაცვას. სწორედ ამ წინააღმდეგობების გამოც მონაცემთა უსაფრთხოების გარემო საქართველოში რჩება არასაკმარისად სტაბილური და ვერ ქმნის იმ ინსტიტუციურ ნდობის საფუძველს, რომელიც თანამედროვე ციფრული მმართველობისთვის გადამწყვეტია.

წარმოდგენილი კვლევის ანალიზი ცხადყოფს, რომ პერსონალური მონაცემების დაცვა ადგილობრივი თვითმმართველობის დონეზე კვლავ რჩება ერთ-ერთ ყველაზე პრობლემურ და სისტემურად დაურეგულირებელ სფეროდ, მიუხედავად იმისა, რომ ბოლო წლებში სამართლებრივი ჩარჩო მნიშვნელოვნად გამკაცრდა. 2024 წლის ცვლილებებმა „პერსონალურ მონაცემთა დაცვის შესახებ“ ორგანულ კანონში უკვეთესი ფორმულირებები შესძინა მუნიციპალიტეტების ვალდებულებებს, თუმცა კვლევის შედეგები მიუთითებს, რომ სამართლებრივი მოთხოვნები ხშირად ფორმალურად სრულდება და რეალური, ტექნოლოგიურ-ინსტიტუციური დაცვა კვლავ არასაკმარისია.

EGDI და EPI ინდექსებში საქართველოს პოზიცია აჩვენებს, რომ ქვეყანა მაღალი ციფრული განვითარების კატეგორიაში რჩება, თუმცა ადგილობრივი თვითმმართველობების დონეზე მონაცემთა უსაფრთხოების, ინტეგრირებულობისა და მომსახურების სტანდარტიზაციის პრობლემები კვლავ მწვავეა. ციფრული მმართველობის სააგენტოს 2023–2024 წლების მონაცემები მიუთითებს, რომ მუნიციპალიტეტების უმეტეს ნაწილს არა მხოლოდ არ გააჩნია სრულყოფილი უსაფრთხოების პოლიტიკა, არამედ მონაცემთა დაცვის ოფიცრის ფუნქციაც ხშირ შემთხვევაში ნომინალურია. ეს ვითარება კიდევ უფრო ამძაფრებს ინსტიტუციურ რისკებს და მიუთითებს, რომ

კანონით გაწერილი რეგულაციების პრაქტიკული იმპლემენტაცია კვლავ გამოწვევად რჩება.

თეორიული ჩარჩოს — Institutional Trust Theory და Digital Era Governance Theory — გათვალისწინებით, ცხადი ხდება, რომ მონაცემთა დაცვის პრობლემები მხოლოდ ტექნოლოგიურ ხარვეზებზე არ არის შეზღუდული. ინსტიტუციური ნდობის თეორია გვაჩვენებს, რომ მოქალაქეთა ნდობა ადგილობრივი თვითმმართველობის მიმართ დამოკიდებულია იმაზე, რამდენად უსაფრთხოა მათი მონაცემების დამუშავება და რამდენად გამჭვირვალეა ამ პროცესის მართვა. Digital Era Governance კი ხაზს უსვამს, რომ ტექნოლოგიური მმართველობა ეფექტიანია მხოლოდ მაშინ, როცა მას თან ახლავს ორგანიზაციული მდგრადობა, სტანდარტიზებული უსაფრთხოება და კომპეტენტური ადამიანური რესურსი.

კვლევის პროცესში იდენტიფიცირებული ძირითადი პრობლემები — არასაკმარისი ტექნიკური ინფრასტრუქტურა, სუსტი დაშიფვრა, დაუბალანსებელი წვდომის კონტროლი, ანგარიშვალდებულების ნაკლებობა, თანამშრომელთა დაბალი კვალიფიკაცია და უსაფრთხოების პოლიტიკის ფრაგმენტულობა — მიუთითებს, რომ მუნიციპალიტეტებში მონაცემთა დაცვის კულტურა კვლავ დაუმკვიდრებელია. მუნიციპალიტეტების მნიშვნელოვანი ნაწილი ვერ ახერხებს GDPR-ის ძირითადი პრინციპების მინიმიზაციის, პროპორციულობის, გამჭვირვალობისა და უსაფრთხოების დაცვას, რაც არა მხოლოდ სამართლებრივ, არამედ დემოკრატიულ რისკებს ქმნის.

ამრიგად, კვლევის დასკვნა ხაზს უსვამს, რომ მონაცემთა დაცვის გაძლიერება შეუძლებელია მხოლოდ ნორმატიული ცვლილებებით. ის მოითხოვს ტექნოლოგიურ მოდერნიზაციას, მონაცემთა დაცვის ოფიცრების რეალურ ინსტიტუციურ გაძლიერებას, სტანდარტიზებულ უსაფრთხოების მექანიზმებს, თანამშრომელთა სისტემურ გადამზადებას და მოქალაქეთა ჩართულობის ზრდას. მხოლოდ ამ კომპლექსური მიდგომით იქნება შესაძლებელი ადგილობრივი თვითმმართველობების მზადყოფნა ციფრული ეპოქის გამოწვევებისთვის და მოქალაქეთა პერსონალური მონაცემების რეალური, არა დეკლარაციული დაცვა, რაც თავის მხრივ დემოკრატიული მმართველობის ხარისხის ერთ-ერთი უმთავრესი წინაპირობაა.

Aksana Guchua

PhD Student

Caucasus International University

Local Self-Government and Personal Data Protection: Regulatory Standards and Digital Risks

Abstract

The contemporary digital era poses significant challenges for local self-governments, where, alongside ensuring the efficient delivery of services to citizens, the protection of personal data has become a central concern. The implementation of information systems, electronic services, and "smart city" technologies by local authorities increases both the volume of data processed and the exposure to cybersecurity risks. Consequently, personal data protection is not merely a legal obligation but also a political, technological, and ethical issue.

This article aims to examine the relationship between local self-governance and personal data protection standards, identify digital risks, and explore the legal frameworks in place. Special emphasis is placed on the legislative amendments introduced in 2024, which have significantly updated both Georgian legislation and EU data protection practices. The study analyzes how these changes impact local governance, their alignment with GDPR principles, and the challenges arising from technological resources, institutional coordination, and citizen trust.

The article demonstrates that enhancing data protection policies requires not only legislative harmonization but also the strengthening of local authorities' capacities, the training of specialists, and the development of an information security culture. The conclusion offers concrete recommendations, including the formulation of local personal data protection strategies, the implementation of digital risk prevention mechanisms, and the promotion of citizen engagement. In doing so, the article provides both theoretical insights and practical approaches that support the protection of citizens' rights and strengthen democratic governance in a digital environment.

Keywords: local self-government, personal data protection, digital risks, regulatory standards.

ბიბლიოგრაფია

საქართველოს კანონი. (2011). პერსონალური მონაცემთა დაცვის შესახებ. თბილისი: საქართველოს პარლამენტი.

საქართველოს კანონპროექტი. (2024). პერსონალური მონაცემთა დაცვის შესახებ – ცვლილებები. თბილისი: საქართველოს პარლამენტი.

Digital Governance Agency. (2023). Cybersecurity awareness and phishing simulation report. Tbilisi: DGA.

Digital Governance Agency. (2024). Annual report on local government digitalization. Tbilisi: DGA.

Dunleavy, P. (2006). Digital era governance: IT corporations, the state, and e-government. Oxford University Press.

ENISA. (2023). Threat landscape report 2023. European Union Agency for Cybersecurity.

European Data Protection Board. (2023). Guidelines on data protection impact assessments and local administration practices. Brussels: EDPB Publications.

European Union. (2016). General Data Protection Regulation (GDPR): Regulation (EU) 2016/679. Official Journal of the European Union, L119.

Floridi, L., & Taddeo, M. (2018). Ethics of AI in public administration. Government Information Quarterly.

Kuner, C. (2020). EU data protection law: GDPR and beyond. Oxford University Press.

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. Annual Review of Political Science.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review.

OECD. (2020). Digital government and local authorities: Best practices and challenges. Paris: OECD Publishing.

OECD. (2021). Digital Government Index. Paris: OECD Publishing.

Personal Data Protection Service. (2023). Annual report on data protection incidents in municipalities. Tbilisi: PDPS.

State Audit Office of Georgia. (2023). Performance audit report on information security in municipalities. Tbilisi: State Audit Office.

UN DESA. (2022). United Nations e-government survey 2022. New York: United Nations.