პამ დიქსონი[*]

ჯგუფის პირადი ცხოვრების ხელშეუხებლობა, მონაცემები და ხელოვნური ინტელექტი: პირადი ცხოვრების ხელშეუხებლობის კოლექტიური ფორმები და მისი კავშირი ტექნოლოგიასა და საკანონმდებლო ჩარჩოებთან

კოლექტიური პირადი ცხოვრების ხელშეუხებლობა ადამიანთა ჯგუფის პირადი ცხოვრების ხელშეუხებლობას გულისხმობს. რამდენადაც ხელოვნური ინტელექტის მეშვეობით პროგნოზირებადი ქცევის საფუძველზე ინფორმაციის ანალიზი და დაჯგუფება სულ უფრო მარტივი ხდება, კოლექტიური პირადი ცხოვრების ხელშეუხებლობის საკითხის აქტუალურობაც მზარდია. მიუხედავად აღნიშნულისა, სახეზეა საკითხის სამართლებრივ მოწესრიგებასთან დაკავშირებული ხარვეზი: მკვიდრი მოსახლეობის, მაგალითად, მაორის ტომელთა მმართველობის ჩარჩო აღიარებს კოლექტიური პირადი ცხოვრების ხელშეუხებლობას, თუმცა, პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონმდებლობათა უმეტესი ნაწილი პირადი ცხოვრების ხელშეუხებლობას ინდივიდის და არა კოლექტიურ დონეზე განიხილავს. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“, რომელიც სხვადასხვა ფორმით, მრავალ რეგიონში მონაცემთა დაცვის სფეროს სტანდარტად არის აღიარებული, ინდივიდის პირადი ცხოვრების ხელშეუხებლობის დაცვაზე ორიენტირებული სამართლებრივი მოწესრიგების მაგალითს წარმოადგენს. წინამდებარე სტატია ჯგუფის პირადი ცხოვრების ხელშეუხებლობის ცნებას განმარტავს და ცალკეულ რთულ სოციალურ და ტექნოლოგიურ ასპექტებს აანალიზებს , რომლებიც კოლექტიური პირადი ცხოვრების ხელშეუხებლობასთან

[*] მსოფლიოს პირადი ცხოვრების ხელშეუხებლობის ფორუმის დამფუძნებელი და აღმასრულებელი დირექტორი.

დაკავშირებულ საკანონმდებლო ხარვეზებს წარმოშვებს. ნაშრომი მიმოიხილავს მნიშვნელოვან შემთხვევებს, რომლებიც ჯგუფის პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებულ რიგ საკითხს შეეხება, მაგალითად: მაორის ალგორითმის ქარტია ახალი ზელანდიის მთავრობასთან, ა.შ.შ-ის გენეტიკური მონაცემების ბიო ბანკის პოლიტიკა, და ადამიანის უფლებათა ევროპული სასამართლოს საქმე „ლევიტი ავსტრიის წინააღმდეგ“.

საკვანძო სიტყვები: *კოლექტიური პირადი ცხოვრების ხელშეუხებლობა, ჯგუფის პირადი ცხოვრების ხელშეუხებლობა, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“, ხელოვნური ინტელექტი, გენეტიკური კონფიდენციალურობა, მკვიდრი მოსახლეობის მმართველობა, მაორის ალგორითმის ქარტია, „ლევიტი ავსტრიის წინააღმდეგ“.*

1. შესავალი

წინამდებარე სტატია პირადი ცხოვრების ხელშეუხებლობას ჯგუფების კონტექსტში განიხილავს, აგრეთვე, განმარტავს ტერმინებს კოლექტიური პირადი ცხოვრების ხელშეუხებლობა და ჯგუფების პირადი ცხოვრების ხელშეუხებლობა, როგორც: პირადი ცხოვრების ხელშეუხებლობის ინტერესები, რომელიც ეხება ან მიემართება ადამიანთა განსაზღვრულ ჯგუფს. პირადი ცხოვრების ხელშეუხებლობა, მრავალი მიზეზით, აქტუალურ პრობლემას წარმოადგენს, პრობლემატურია აგრეთვე ტექნოლოგიური განვითარების პარალელურად ჯგუფის პირადი ცხოვრების ხელშეუხებლობის ინტერესთა დაცვის თვალსაზრისით წარმოქმნილი ხარვეზები. კონკრეტულად, დომინანტური გლობალური პირადი ცხოვრების ხელშეუხებლობის ნორმები ყურადღებას ამახვილებს ინდივიდის პირადი ცხოვრების ხელშეუხებლობის უფლებებზე, თუმცა დღესდღეობით დიდი მონაცემების (“Big Data”) , ხელოვნური ინტელექტისა და მანქანური სწავლების (“Machine Learning”) პირობებში ტექნოლოგიური პროგრესი გავლენას ახდენს არა მხოლოდ ინდივიდის, არამედ ჯგუფს უფლებებზეც, კანონმდებლობა კი ხშირად, ინდივიდის და არა ჯგუფების პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვაზე ორიენტირდება.[1]

[1] ჯგუფის კონცეფცია შესწავლილია მრავალი დისციპლინის ფარგლებში, მათ შორის მათემატიკის, ფიზიკის და სოციალური მეცნიერებების. წინამდებარე ნაშრომი ეფუძნება კემპბელის ჯგუფურობის დასაბუთებას (1958), რომელიც მოგვიანებით დაიხვეწა ლიკელის და სხვების მიერ (2001), როგორც

ინდივიდის პირადი ცხოვრების ხელშეუხებლობის უფლება, როგორც თეორიული და დოქტრინული საკითხი, ღრმად არის შესწავლილი.[2] თუმცა, კოლექტიური პირადი ცხოვრების ხელშეუხებლობა სამეცნიერო ლიტერატურის ფარგლებში ნაკლებად განიხილება, როგორც პირადი ცხოვრების ხელშეუხებლობის, ასევე კოლექტიურობის ნაწილში.[3]

დღესდღეობით ხელმისაწვდომია კოლექტიური ან ჯგუფური პირადი ცხოვრების ხელშეუხებლობის შესახებ კრიტიკულად მნიშვნელოვანი როგორც სამეცნიერო და იურიდიული, ისევე სხვა შინაარსის ნაშრომები. კოლექტიური პირადი ცხოვრების ხელშეუხებლობის ყველაზე მკაფიო მაგალითად შეიძლება დასახელდეს ნაშრომები მკვიდრი მოსახლეობის ჯგუფების შესახებ, ეროვნულ და ტომობრივ ჩარჩოებში, სხვადასხვა იურისდიქციის ფარგლებში. მნიშვნელოვან მაგალითებს შორისაა ამერიკის მკვიდრი მოსახლეობის მონაცემთა სუვერენიტეტის ქსელი[4] და მაორის მონაცემთა მმართველობის

ჯგუფის ერთიანობის ხარისხის განსაზღვრის პირველადი თეორიული საფუძველი. კემპბელმა აღმოაჩინა, რომ ჯგუფის ჩამოყალიბების პროცესში შესაძლოა რაოდენობრივად განსაზღვრადი მახასიათებლების ფართო სპექტრის იდენტიფიცირება, რომლებიც განსაზღვრავს ჯგუფის ერთიანობის, ანუ „ჯგუფურობის“ მიახლოებით დონეს. ჯგუფურობა და მისი მიმართება კოლექტიური პირადი ცხოვრების ხელშეუხებლობის ამ ანალიზში უფრო დეტალურად არის განხილული წინამდებარე ნაშრომში. იხილეთ ტექსტი და სქოლიო 11-15.

[2] არსებობს პრაქტიკული და რელევანტური ლიტერატურა პირადი ცხოვრების ხელშეუხებლობის თემაზე. იხილეთ: *DeCew J.,* Privacy, Stanford Encyclopedia of Philosophy, 2018; *Gellman R.,* Fair Information Practices: A Basic History, 2025, <http://dx.doi.org/10.2139/ssrn.5348107> [12.11.2025]; *Bamburger K. A., Mulligan D.,* Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, Cambridge: MIT Press, 2016; *Solove D.,* Understanding Privacy, Cambridge: Harvard University Press, 2008; *Solove D.,* Against Privacy Essentialism, GWU Law School Public Law Research Paper, 2025-19; *Allen A. L.,* Presidential Address, The Philosophy of Privacy and Digital Life, 93 Proceedings of the American Philosophical Association, 2019, 21-38.

[3] კოლექტიურობა ვრცელი თემაა და მრავალი საკვლევი სფერო აქვს. აღნიშნულის ერთერთი მაგალითია კოლექტიური სასარჩელო წარმოება, რომელიც ფართოდ იქნა შესწავლილი რუანდის გაკაკას სასამართლოების მიერ, რომლებმაც 2001-დან 2012 წლამდე გენოციდთან დაკავშირებული თითქმის ორი მილიონი საქმე განიხილეს. See: *Megwalu A., Loizides N.,* Dilemmas of Justice and Reconciliation: Rwandans and the Gacaca Courts, African Journal of International and Comparative Law, 2010, <https://ssrn.com/abstract=1406863> [12.11.2025]. კოლექტიური მოლაპარაკებები გამოძიების კიდევ ერთი დიდი დარგია; იხილეთ: *Court de le A.,* Stabilising Collective Agreements in Continental Europe: How Contract Law Principles Reinforce the Right to Collective Bargaining, Oñati Socio-Legal Series, Vol. 9, No. 1, 2019. მიუხედავად იმისა, რომ კოლექტიურობის შესახებ ლიტერატურის უმეტესობა არ განიხილავს კოლექტიურ პირადი ცხოვრების ხელშეუხებლობას, როგორც ეს განსაზღვრულია ამ ნაშრომში, ის მაინც გვთავაზობს სასარგებლო ხედვებს იმის შესახებ, თუ როგორ ყალიბდება და გამოიხატება კოლექტიურობა.

[4] ადგილობრივი მონაცემთა სუვერენიტეტი, ანუ IDSov, მნიშვნელოვანი მოძრაობაა მრავალ იურისდიქციასა და რეგიონში. ადგილობრივი მონაცემთა სუვერენიტეტის განმარტება შეიძლება განსხვავდებოდეს სხვადასხვა რეგიონში და კულტურაში. ამ ნაშრომის მთავარი ორიენტირია მონაცემთა სუვერენიტეტი, რომელიც კოლექტიურ კონფიდენციალურობასთან არის კავშირში, თუმცა, მონაცემთა სუვერენიტეტის შესახებ იდეები მოიცავს გაცილებით ფართო საკითხებს, რომლებიც ამ ნაშრომის ფარგლებს სცილდება See: The Global Indigenous Data Alliance, <https://www.gida-global.org> [12.11.2025] .

მოდელი, სახელწოდებით: „ტე კაჰუი რარაუნგას, ქარტია“, „ტე მანა რარაუნგას ქარტია“ და სხვა. [5; 6; 7; 8]

კერძოდ, მაორთა ლიტერატურა და ნაშრომები კოლექტიური პირადი ცხოვრების ხელშეუხებლობის შესახებ კრიტიკული მნიშვნელობისაა, რამდენადაც იდეები კოლექტიური პირადი ცხოვრების ხელშეუხებლობის შესახებ, ისევე როგორც მონაცემთა კოლექტიური ხარისხი პირდაპირ არის მოხსენიებული.

ავტორი კაკუტაის განმარტებით, მაორის მოდელის თანახმად ცალკეულ შემთხვევებში შესაძლოა კოლექტიური უფლებები ინდივიდის უფლებებზე უპირატესი იქნეს. იგი ასევე აღნიშნავს, რომ ცალკეული ტიპის მონაცემები ხასიათდება მკაფიო კოლექტიური განზომილებით — მათ შორის, დნმ და გენეტიკურ მონაცემთა კატეგორიები.[9]

აღსანიშნავია, რომ მაორთა მონაცემთა მართვის ჩარჩო სახელწოდებით “Te Kāhui Raraunga”, რომელიც ახალი ზელანდიის მთავრობასთან დადებულ ფორმალურ ხელშეკრულებას წარმოადგენს, კოლექტიურ პირადი ცხოვრების ხელშეუხებლობას კონკრეტულად ხელოვნური ინტელექტის კონტექსტში მოიაზრებს, და მის ფარგლებში წარმოდგენილია ღრმა ანალიზი მაორთა კონტექსტში ალგორითმებისა და ხელოვნური ინტელექტის სხვა ასპექტების გამოყენების შესახებ.

---

[5] Te Kāhui Raraunga, <https://www.kahuiraraunga.io/maoridatagovernance> [12.11.2025]. See also Te Mana Raraunga Charter, <https://www.temanararaunga.maori.nz/tutohinga> [12.11.2025].

[6] მაგალითად, მაორის ტომელებს გააჩნიათ კარგად განვითარებული კოლექტიური პირადი ცხოვრების ხელშეუხებლობის კონცეფცია, რაც მათი კულტურისა და კანონების ნაწლია. მაორთა ტომი პირადი ცხოვრების ხელშეუხებლობას ჯგუფურ უფლებად მიიჩნევს. წინამდებარე სტატია განმარტავს ტერმინს კოლექტიური პირადი ცხოვრების ხელშეუხებლობა და ადარებს მას პირადი ცხოვრების ხელშეუხებლობის ინდივიდუალურ კონცეფციას. მკვიდრი მოსახლეობის კოლექტიური პირადი ცხოვრების ხელშეუხებლობის განმარტებისათვის იხ. მაგალითად: *Quince K., Houghton J.,* Privacy and Māori Concepts” in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136.

[7] აღნიშნული სტატია განიხილავს მკვიდრი მოსახლეობის ნაშრომებს და ლიტერატურას კოლექტიური პირადი ცხოვრების ხელშეუხებლობის შესახებ, წინამდებარე ნაშრომში განხილული საქმეების შესწავლის ფარგლებში.

[8] მაორთა რწმენის თანახმად კონფიდენციალურობა კოლექტიური უფლებაა. აღნიშნულის თაობაზე ხელმისაწვდომია მაორთა ტომის პირადი ცხოვრების ხელშეუხებლობის შესახებ დეტალური ლიტერატურა. კოლექტიური პირადი ცხოვრების არსის გასაგებად, მნიშვნელოვანია პირველ რიგში განხილული იქნეს მკვიდრი მოსახლეობის ფილოსოფია კოლექტიური პირადი ცხოვრების ხელშეუხებლობის შესახებ. See, e.g., *Quince K., Houghton J.,* “Privacy and Māori Concepts” in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136, <https://researchspace.auckland.ac.nz/handle/2292/67023> [12.11.2025].

[9] *Kukutai T.,* Indigenous Data Sovereignty – a New Take on an Old Theme, Science, Vol. 382, No. 6674, 2023. არტიკლის თანახმად, ავტორი კაკუტაი კოლექტიურობას ჯგუფების კონტექსტში განმარტავს: ყველა (CARE) პრინციპი (კოლექტიური ბენეფიტი, კონტროლის უფლებამოსილება, პასუხისმგებლობა და ეთიკა) პირდაპირ მიემართება კოლექტიურ უფლებებსა და ვალდებულებებს. მაორთა მონაცემთა დაცვის შესახებ პრინციპები ერთი ნაბიჯით წინ არის. წინამდებარე კონტექსტში აღნიშნულია რომ კოლექტიურად, ჯგუფის უფლებები ინდივიდის უფლებებზე უპირატესია” ავტორი კაკუტაის მიერ აღწერილი პრინციპები (The CARE) შედგენილი იქნა GIDA-ს მიერ (GIDA - Global Indigenous Alliance). იხ: Care Principles, GIDA, <https://www.gida-global.org/care> [12.11.2025].

2. რა არის ჯგუფი?

კოლექტიურ კონფიდენციალურობასთან დაკავშირებით ერთ-ერთი გამოწვევა მისი განმარტებაა — ჯგუფის პირადი ცხოვრების ხელშეუხებლობის ირგვლივ არსებული იდეები ბევრ კითხვას წარმოშვებს, მაგალითად: ჯგუფის არსის შესახებ, ჯგუფების მიერ კოლექტიური პირადი ცხოვრების ხელშეუხებლობის დაცვის უფლებით სარგებლობის საკითხის, წინამდებარე კითხვებზე პასუხის დადგენის მეთოდების და პასუხის გაცემაზე უფლებამოსილი პირების თაობაზე. ჯგუფის განმარტება ერთ-ერთი უმთავრესი საკითხია, კოლექტიური პირადი ცხოვრების ხელშეუხებლობის კონცეფციის განხილვისას. აღნიშნულის მისაღწევად, წინამდებარე კვლევაში განხილულია ჯგუფების შესახებ ლიტერატურა.

სამეცნიერო ლიტერატურაში არსებობს მრავალი ნაშრომი იმის შესახებ, თუ რას წარმოადგენს ჯგუფი. ეს ლიტერატურა აერთიანებს ჯგუფების შესახებ მათემატიკურ წარმოდგენებსა და კონცეფციებს, რომლებიც 1700-იანი წლებით თარიღდება. აბსტრაქტული ალგებრის განმარტებით „ჯგუფების თეორია“ ჯგუფების შესწავლას გულისხმობს, რომლებიც მათემატიკის კონტექსტში რთული ალგებრული სტრუქტურებია.[10] ალგებრულმა ჯგუფთა თეორიამ გავლენა მოახდინა ფიზიკის სფეროზეც, ისევე როგორც სიმრავლეთა თეორიაზე, რომლებიც საინტერესო იდეებს შეიცავენ ჯგუფების, ჯგუფური დინამიკის და სხვა ჯგუფური სტრუქტურების შესწავლის თაობაზე. ფიზიკა აერთიანებს ჯგუფური თეორიის სტრუქტურებს, განსაკუთრებით სიმეტრიის ან უცვლელობის კონტექსტში.[11] ჯგუფური თეორია ზოგიერთი თეორეტიკოსი ფიზიკოსის მიერ თანამედროვე ფიზიკის დომინანტურ მომწესრიგებელ პრინციპად ითვლება.[12]

სოციალურ მეცნიერებაში ჯგუფების თვალსაზრისით ერთ-ერთი მთავარი ცნებაა „ჯგუფურობა“ (“Enitativity”), „ჯგუფის ერთიანობის ხარისხი“, სოციოლოგმა დონალდ კემპბელმა ეს ტერმინი 1958 წელს შეიმუშავა, გარკვეული საერთო მახასიათებლების მქონე ჯგუფების აღსაწერად. რაც უფრო მაღალია ჯგუფის „ენიტატიურობის“ ხარისხი, იგი მით უფრო შეკრული და ერთმანეთთან დაკავშირებულია. ლიკელმა და სხვებმა განმარტეს აღნიშნული ტერმინი, მისი ამჟამინდელი მნიშვნელობით, ანუ „ენიტატიურობა“ არის „პირთა ერთიანობის, და ერთმანთთან დაკავშირებულობის ხარისხი“. [13]

ტერმინი „ჯგუფის“ სოციალურ მეცნიერებათა ფარგლებში ანალიზის მიზნით კემპბელმა რამდენიმე კრიტერიუმი განსაზღვრა: წევრთა

[10] *Dummitt D. S., Foote R. M.,* Abstract Algebra, 3rd ed., 2003. იხ. პირველი ნაწილი: ჯგუფის თეორია, თავები 1-6, ჯგუფის თეორია.

[11] *D'Hoker E.,* Mathematical Methods in Physics - 231B - Group Theory, *Mani L.* Bhaumik Institute for Theoretical Physics, Department of Physics and Astronomy, Course Notes, 2019, <https://www.pa.ucla.edu/faculty-websites/dhoker-lecture-notes/graduate-courses/group-theory.pdf> [12.11.2025].

[12] Ibid.

[13] *Lickel B., Hamilton D.L., Wieczorkowska G., Lewis A., Sherman S.J., Uhles A.N.,* Varieties of Groups and the Perception of Group Entitativity, Journal of Personality and Social Psychology, 78(2), 2000, 223–246. განმარტებისთვის იხ. გვერდი 224.

ერთმანეთთან ურთიერთობის სიხშირე, მათი მსგავსება, საერთო მიზნების არსებობა, და მკაფიო საზღვრების არსებობა.[14] კვლევები აჩვენებს, რომ გაერთიანებას, როგორც წესი, სამი ძირითადი ელემენტი აყალიბებს: არსი (წევრთა მსგავსება), წარმომადგენლობა (საერთო მიზნები და ჯგუფის წევრთა შორის ურთიერთქმედება) და ერთიანობა (ჯგუფის თვით-აღქმა და მნიშვნელობა).[15] ჯგუფების თვალსაზრისით, რომლებიც ხასიათდებიან ერთიანობის ანუ „ენიტატიურობის“ ნიშნებით შესაძლოა ოთხ სხვადასხვა კატეგორიად კლასიფიცირდეს: ჯგუფი, რომელსაც ქმნის ადამიანთა შიდა წრე (ოჯახი და მეგობრები), გარკვეული სამუშაოს შესასრულებლად შექმნილი ჯგუფი, სოციალური კატეგორგიები (გენდერი, რასა) და ჯგუფები რომელთაც გარკვეული საერთო ინტერესები აერთიანებთ (მაგალითად, ადამიანთა ჯგუფი რომელთაც მოსწონთ ერთი ჟანრის მუსიკა).[16]

კოლექტიური პირადი ცხოვრების ხელშეუხებლობის კონტექსტში აღნიშნული სტატია განიხილავს და აანალიზებს სამ შემთხვევას, რომლებიც ასახავს ჯგუფურობის მაღალ ხარისხს — ავტორების: ლიკელ ეტ ალის და აგადულინა ეტ. ალის თანახმად.

პირველი შემთხვევის ანალიზი ფოკუსირებულია მკვიდრი მოსახლეობის (აბორიგენთა) კოლექტიური პირადი ცხოვრების ხელშეუხებლობის ჩარჩოზე მათ შორის მაორთა ალგორითმულ ქარტიაზე, რაც კოლექტიური პირადი ცხოვრების ხელშეუხებლობის შესახებ ლიტერატურის მნიშვნელოვანი ნაწილია.

მეორე შემთხვევის ანალიზი შეეხება ამერიკის ნაციონალური ინსტიტუტების ჯანმრთელობის ბიო ბანკის (“THE ALL OF US PROGRAM”) პროგრამას, რომელიც მიზნად ისახავს კვლევის მიზნებით მილიონი გენეტიკური მონაცემის შეგროვებას. 2021 წელს დეტალურად შემოწმდა წინამდებარე პროგრამის ფარგლებში ტომთა წევრების დნმ მონაცემების დამუშავების მიზნით მონაცემთა თანხმობის მოპოვების პრაქტიკა.

ჯანმრთელობის ინსტიტუტის მიერ (გენეტიკური მონაცემების დონაციის პროგრამის ფარგლებში) განხორციელებული შესწავლის შედეგად გამოვლინდა მრავლობითი და კომპლექსური დარღვევები, კერძოდ, ზოგადი ფორმით მოპოვებული თანხმობის ნაწილში, რაც არ იყო საკმარისი მონაცემთა დაცვის თვალსაზრისით არსებული კანონმდებლობის მოთხოვნების თანახმად. ანგარიშის თანახმად, კონფიდენციალურობის დაცვის მიზნით გატარებული რიგი ზომებისა და მონაცემთა დეპერსონალიზაციის მიუხედავად, კვლევის ინდივიდუალური მონაწილის მათ ტომობრივ ჯგუფთან დაკავშირება კვლავ შესაძლებელი იყო.

[14] *Campbell D. T.,* Common Fate, Similarity and other Indices of the Status of Aggregates of Persons as Social Entities, Behavioral Science, 1958, <https://doi.org/10.1002%2Fbs.3830030103> [12.11.2025].

[15] As quoted in: *Agadullina E. R., Lovakov A. V.,* Understanding Entitativity: Are There Real Differences between Approaches? Journal of the Higher School of Economics, 2017.

[16] *Agadullina E. R., Lovakov A. V.,* Understanding Entitativity: Are There Real Differences between Approaches? Journal of the Higher School of Economics, 2017.

მესამე შემთხვევის ანალიზი ჰოლოკოსტის დროს გადარჩენილ პირთა კოლექტიურ ჯგუფს ეხება, რომლებიც მაუთაუზენის საკონტრენტაციო ბანაკიდან 1945 წელს გათავისუფლდნენ, და რომლებიც ჯერ კიდევ ცოცხლობდნენ 2016 წელს. ერთერთმა ავსტრიულმა პუბლიკაციამ მასმედიაში კონკრეტული ადამიანთა ჯგუფის მისამართით დეფამაციური (სახელის ან რეპუტაციის ინფორმაციების გავრცელების გზით შელახვა) ცნობები გაავრცელა, რის საპასუხოდაც ჯგუფმა კოლექტიურად შეიტანა სარჩელი სასამართლოში ცილისწამებისათვის. სასამართლომ აღნიშნული სარჩელი წარმოებაში არ მიიღო იმ მიზეზით მოსარჩელეები მხოლოდ ჯგუფად აღიარა და არა ინდივიდებად, რომელთაც ინდივიდუალურად გააჩნდათ კონფიდენციალურობის უფლებები.

წინამდებარე გადაწყვეტილების ფარგლებში სასამართლომ იმსჯელა კოლექტიური პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით ჯგუფების დაცვის ხარისხობრივ პრობლემებზე, იმ ქვეყნებშიც კი, სადაც პერსონალურ მონაცემთა დაცვის მაღალი საკანონმდებლო სტანდარტია.

წინამდებარე შემთხვევათა დეტალურ შესწავლამდე მნიშვნელოვანია კოლექტიური პირადი ცხოვრების ხელშეუხებლობის გაანალიზება ტექნიკური, სოციალური და იურიდიული კონტექსტის გათვალისწინებით.

3. კოლექტიური პირადი ცხოვრების ხელშეუხებლობა, ხელოვნური ინტელექტის და მანქანური სისტემის ეკოსისტემათა ზეგავლენა მონაცემებზე და პირადი ცხოვრების ხელშეუხებლობაზე

ხელოვნური ინტელექტის ინოვაციური ფორმებისა და ღრმა სწავლების სისტემების[17] განვითარება მონაცემთა გამოყენების პოლიტიკის, განსაკუთრებით აგრეგირებული ან დეპერსონალიზებული მონაცემების გამოყენების შემთხვევაში სირთულეებს წარმოშობს. უკვე არსებობს რიგი კვლევები ხელოვნური ინტელექტისა და ჯგუფების ურთიერთქმედების შესახებ. „ენიტატიურობა“ — იდეა იმის შესახებ, თუ რამდენად „მოქმედებს ჯგუფი ერთიან ერთეულად“ — სოციალურ მეცნიერებათა კვლევების ფარგლებში ფართოდ გამოიყენება,[18] ისევე როგორც ხელოვნურ ინტელექტთან დაკავშირებულ ახალ კვლევით სფეროებში.

მაგალითისთვის, შესაძლოა ხელოვნური ინტელექტისა და ღრმა სწავლების ტექნოლოგიის მიერ გამოყენებული იქნეს ტოპოლოგიური

[17] *Vaswani A., Shazeer N., Parmar N., Uszkoreit J., James L., Gomez A. N., Kaiser L., Polosukhin I.*, Attention is All You Need, arXiv:1706.03762v7 [cs.CL], <https://doi.org/10.48550/arXiv.1706.03762> [12.11.2025]. ნაშრომი პირველად წარდგენილი იყო ნეირონული ინფორმაციის დამუშავების სისტემების 31-ე კონფერენციაზე (NIPS 22017), კალიფორნია, აშშ. ეს არის გავლენიანი ისტორიული ნაშრომი ხელოვნური ინტელექტის ისტორიაში. ასევე, იხ.: *Murgia M.,* Generative AI Exists Because of the Transformer, This is How it: Writes, Works, Learns, Thinks and Hallucinates, Financial Times, 2023.

[18] *Bernado F., Palma-Oliveira J. M.,* Tell me Where you Live…How the Perceived Entitativity of Neighborhoods Determines the Formation of Impressions About their residents, Frontiers in Psychology, 2022.

მონაცემთა ანალიზის მეთოდი ჯგუფის წევრთა ერთმანეთთან კავშირის სიმტკიცის დასადგენად, ასევე მათი ქცევის ანალიზის მიზნით.[19] ზოგიერთი კვლევა აერთიანებს „ენიტატიურობასა“ და ხელოვნურ ინტელექტს ერთმანეთთან მჭიდროდ დაკავშირებული ჯგუფებისათვის დამახასიათებელი ქცევების მოდელების იდენტიფიცირებისათვის, ასევე იმის დადგენისათვის, თუ როგორ იმოქმედებს აღიშნული ქცევა სხვა პირებზე, ვინც არ არის აღნიშნული ჯგუფის წევრი.[20]

დიდი მოცულობის საჯარო მონაცემთა ბაზები (მაგალითად, SALSA)[21] — როდესაც ისინი კომბინიებულია „ენიტატიურობის“ (ჯგუფურობის) ანალიზის შედეგებთან და აერთიანებს ინფორმაციას ჯგუფების შესახებ, წარმოშვებს ეთიკურ და კონფიდენციალურობასთან დაკავშირებულ რისკებს.

ენობრივი მოდელების განვითარების პარალელურად გაადვილდა იმგვარი კოდის გენერირება, რომლის მეშვეობითაც შესაძლებელია ჯგუფის მახასიათებლების ანალიზი, რომლებიც თავმოყრილია დიდი ზომის მონაცემთა ბაზებში. აღნიშნული მიზეზით პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებული რისკები იზრდება და საჭიროა რისკის სისტემატიური შეფასება.[22]

დღესდღეობით არსებობს საერთო კონსესუსის საფუძველზე შექმნილი ნაშრომები, რომლებიც განიხილავენ პირადი ცხოვრების ხელშეუხებლობასა და მანქანური სწავლების[23] და ხელოვნური ინტელექტის თანაკვეთას. აღნიშნული ნამუშევრები ახდენენ რისკების იდენტიფიცირებას და აანალიზებენ ზოგად პრინციპებს. აღნიშნულის მნიშვნელოვანი მაგალითია იუნესკოს რეკომენდაცია ეთიკისა და ხელონური ინტელექტის შესახებ, რომელიც ხელშემკვრელ 194 წევრ სახელმწიფოზე ვრცელდება.[24]

მნიშვნელოვანია აღინიშნოს ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის პრინციპები ხელოვნური ინტელექტის შესახებ. წინამდებარე პრინციპები შემუშავდა ხელშემკვრელ მთავრობათა, შეთანხმებულ ორგანოთა და მათი ოფიციალური საკონსულტაციო ერთეულების მიერ, რომლებიც მოიცავს სამოქალაქო საზოგადოებას, ბიზნესს,

---

[19] *Liang C., Chen V., Shah J., Andrist S.,* Converting Spatial to Social: Using Persistent Homology to Understand Social Groups, ACM International Conference on Multimodal Interaction (ICMI), Canberra, Australia, 2025.

[20] *Bera A.,* Data Driven Modeling of Group Entitativity in Virtual Environments, VRST 2019, Tokyo Japan <https://arxiv.org/pdf/1810.00028> [12.11.2025].

[21] *Alameda-Pineda X.,* SALSA: A Novel Dataset for Multimodal Group Behavior Analysis, IEEE Trans Pattern Anal Mach Intell, 2016.

[22] ერთ-ერთ მაგალითში, ჯგუფის ვიზუალური სურათების გამოყენებით, ადამიანთა ჯგუფების ჯგუფური შეკავშირების ქულის პროგნოზირებისთვის გამოყენებული იქნა მრავალამოცანიანი კონვოლუციური ნეირონული ქსელი. *Gosh S.,* Predicting Group Cohesiveness in Images, 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2019, 1-8.

[23] Large Language Models or LLMs are architected utilizing transformer models. LLMs are often characterized by the exceptionally large datasets used to train the models. See Wikipedia entry “Large Language Model,” <https://en.wikipedia.org/wiki/Large_language_model> [12.11.2025].

[24] Recommendation on the Ethics of Artificial Intelligence, UNESCO, 2022, <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence> [12.11.2025].

სტანდარტების შემმუშავებელ ორგანიზაციებს და სხვა დაინტერესებულ მხარეებს. 2018 წელს ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ შეკრიბა ხელოვნური ინტელექტის ექსპერტთა ჯგუფი, ამ პროცესში ტექნიკური სიზუსტისა და მისი სიღრმისეული შესწავლის უზრუნველსაყოფად. პრინციპები რატიფიცირებული იქნა 2019 წელს და განახლდა 2024 წელს.[25] მიუხედავად მისი ღირებულებისა და მნიშვნელობისა, აღნიშნული ნაშრომები არ შეიცავს სიღრმისეულ ანალიზს იმ გავლენის შესახებ, რასაც ხელოვნური ინტელექტი ახდენს ჯგუფებზე, კონფიდენციალურობის თვალსაზრისით.

ევროპის საბჭოს (CoE) კომიტეტის (CAHAI) კვლევის ფარგლებში შესწავლილი იქნა ხელოვნური ინტელექტის სამართლებრივი ჩარჩოს (პოტენციური) ელემენტები. წინამდებარე კვლევის ფარგლებში ევროპის საბჭომ განიხილა ხელოვნური ინტელექტის გავლენა ჯგუფებზე და აღნიშნა, რომ ხელოვნური ინტელექტის მიერ განხორციელებულმა ანალიზმა შესაძლოა წარმოშვას ჯგუფების დისკრიმინაციის საფრთხე. კვლევაში „ჯგუფების“ სხვადასხვა ტიპის შესახებ ინფორმაცია არ იყო მოცემული, ასევე არ იყო განხილული კონფიდენციალურობის საკითხი, თუმცა ხაზგასმული იყო არსებული პრობლემების (დისკრიმინაციის საკითხი) შესახებ. ჩარჩო კონვენციის საბოლოო ვერსიაში არ განიმარტა ჯგუფის ცნება, თუმცა, აღნიშნული კვლევა ჯგუფების კონფიდენციალურობის თემატიკაზე ღირებულ რესურსს წარმოადგენს.[26];[27]

წინამდებარე საკითხი განხილულია ევროპის საბჭოს მიერ გამოცემულ კიდევ ერთ მნიშვნელოვან რეკომენდაციაში „პროფაილინგის“ კონტექსტში პერსონალური მონაცემების ავტომატიზირებულ დამუშავებასთან დაკავშირებით ფიზიკური პირების დაცვის შესახებ. რეკომენდაციის ფარგლებში საბჭომ კონკრეტულ კონტექსტში მიმოიხილა ხელოვნური ინტელექტისა და ჯგუფების ცნებები. რეკომენდაციის თანახმად:

> **1 i-j:** „მაღალი რისკის შემცველი პროფაილინგი“ შეიძლება, მათ შორის, გულისხმობდეს: პროფაილინგს, რომელიც წარმოშვებს სამართლებრივ შედეგებს ან მნიშვნელოვან გავლენას ახდენს მონაცემთა სუბიექტზე ან აღნიშნული პროფაილინგით იდენტიფიცირებულ პირთა ჯგუფზე;“
>
> 2.6:“...პროფაილინგის შედეგად ინდივიდებისათვის, ჯგუფების ან თემებისათვის არ უნდა დადგეს საზიანო შედეგი. ”

[25] OECD AI Principles, 2019 (Ratified), 2024 (updated).

[26] Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, 17 December 2020, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> [12.11.2025]. მაგ. იხილეთ პარ. 20, 25, და შენიშვნა 15 დისკრიმინაციის შესახებ. CAHAI იყო CAI-ის წინამორბედი, რომელმაც დაასრულა ის, რაც შემდგომში გახდა ევროპის საბჭოს ჩარჩო კონვენცია ხელოვნური ინტელექტისა და ადამიანის უფლებების, დემოკრატიისა და კანონის უზენაესობის შესახებ. იხ. შენიშვნა 26.

[27] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, 5 September 2024.

B. 78: ".....ხელოვნური ინტელექტის აპლიკაციებმა მონაცემთა სუბიექტებსა და ჯგუფებს უნდა მისცენ საშუალება ეფექტურად აკონტროლონ აპლიკაციების ინდივიდებზე, ჯგუფებსა და საზოგადოებაზე ზეგავლენა."

8.5: „საზედამხედველო ორგანოების მოკვლევის სფერო უნდა გაფართოვდეს და მოიცვას კოლექტიური და საზოგადოებრივი რისკები. რეკომენდებულია მოსაზრებებში აღნიშნული იქნეს ამგვარი რისკები და ისინი გათვალისწინებული იქნეს გადაწყვეტილებების მიღების პროცესში." [28]

ევროპის საბჭომ განმარტა ხელოვნური ინტელექტის ცნების ფარგლები, თუმცა, კონკრეტულად არ განმარტებულა ჯგუფის პირადი ცხოვრების ხელშეუხებლობის ან კოლექტიური პირადი ცხოვრების ხელშეუხებლობის ცნებები. მიუხედავად იმისა, რომ აღნიშნული ნაშრომი მნიშვნელოვანია, იგი არ წარმოადგენს სრულ ლიტერატურულ მიმოხილვას აღნიშნულ თემაზე. ევროკავშირის ხელოვნური ინტელექტის აქტი განიხილავს ჯგუფების ცნებას — მეხუთე მუხლის ფარგლებში გაწერილია კონკრეტული აკრძალული საქმიანობა რაც დაკავშირებულია ჯგუფებსა და ინდივიდებთან. ხელოვნური ინტელექტის აქტის ფარგლებში კონკრეტული განმარტება ჯგუფებისა და პირადი ცხოვრების ხელშეუხებლობის შესახებ არ არსებობს. [29]

„კოლექტიური პირადი ცხოვრების ხელშეუხებლობის" სრულად ჩამოყალიბებული პოლიტიკურ-საკანონმდებლო განმარტება, რომელიც ამ ცნებას პირდაპირ განსაზღვრავს (მათ შორის, ხელოვნური ინტელექტის კონტექსტშიც), ძირითადად ადგილობრივ ხალხთან თანამშრომლობით ან მათ მიერ არის შემუშავებული და შეეხება ტომების მონაცემებსა და მათი დაცვის შესახებ კანონებს. ლიტერატურაში მოცემულია სამართლებრივი არგუმენტები, რომლის მიხედვით, ზოგიერთი ტომის ხელისუფლებას უფლებამოსილება ჰქონდა ტომის ფარგლებში მონაცემთა დაცვის შესახებ

[28] Council of Europe Recommendation of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 3 November at the 1416th meeting of the Ministers' Deputies).

[29] EU Artificial Intelligence Act, Regulation – EU – 2024/1689. ევროკავშირის ხელოვნური ინტელექტის შესახებ აქტი განსაზღვრავს, რომ ხელოვნურ ინტელექტთან დაკავშირებული კონფიდენციალურობის საკითხების უმეტესობა უნდა დარეგულირდეს არსებული კანონმდებლობის, განსაკუთრებით GDPR-ის, შესაბამისად. თუმცა, ხელოვნური ინტელექტის აქტსა და GDPR-ს შორის ურთიერთქმედება კომპლექსური საკითხია. ამ ნაშრომის მიზნებისათვის მნიშვნელოვანია აღინიშნოს, რომ ხელოვნური ინტელექტის შესახებ აქტი არ არეგულირებს ჯგუფურ ან კოლექტიურ პირადი ცხოვრების ხელშეუხებლობის საკითხებს, როგორც ეს GDPR-შია განმარტებულია. ვინაიდან თავად GDPR ძირითადად ინდივიდუალურ პირადი ცხოვრების ხელშეუხებლობის უფლებებზეა ფოკუსირებული, ჯგუფური პირადი ცხოვრების ხელშეუხებლობა ხელოვნური ინტელექტის შესახებ აქტის მოქმედების ფარგლებს გარეთ რჩება. ვინაიდან ხელოვნური ინტელექტის შესახებ აქტი არ მიმოიხილავს კოლექტიურ პირადი ცხოვრების ხელშეუხებლობა, აღნიშნული საკითხის დეტალური ანალიზი - აგრეთვე, მისი GDPR-თან ურთიერთქმედება განხილული იქნება ცალკე ნაშრომში.

კანონები შეემუშავებინა. აღნიშნული კანონები განსაზღვრავდნენ, თუ რა განიხილებოდა ტომის მონაცემად. როგორც ცოსი აღნიშნავს:

> „...ფედერალური დონის ტომის მთავრობებს მართლაც აქვთ უფლებამოსილება ტომის ფარგლებში მიიღონ კანონები. მიუხედავად იმისა, რომ შესაძლოა არსებობდეს იურისდიქციული შეზღუდვები, ტომის კანონმდებლობა შეიძლება გახდეს შესაბამისი ფედერალური და შტატის პოლიტიკის ფორმირების საფუძველი. მაგალითად, ტომის კანონებმა შეიძლება განსაზღვროს, რა ჩაითვლება „ტომის მონაცემად“ და მონაცემების შეგროვებაზე, გამოყენებაზე ან განკარგვაზე ტომის თანხმობის მიღების გზები.“[30]

აღნიშნული იდეები და მიდგომები გამოიხატება რამდენიმე მაგალითში, რომლებიც ასახავს, თუ რა არის კოლექტიური პირადი ცხოვრების ხელშეუხებლობა, მათ შორის, ხელოვნური ინტელექტის კონტექსტშიც. ერთ-ერთ მაგალითად, რომელსაც ეს ნაშრომი უკვე ეხებოდა, შეიძლება ჩაითვალოს მაორების მონაცემთა მმართველობის მოდელი — “Te Kāhui Raraunga” — და მისი ქარტია, “Te Mana Raraunga Charter”. კიდევ ერთი მაგალითი არის კანადაში[31] არსებული “First Nations Principles of OCAP“, რომელიც განსაზღვრავს, თუ როგორ უნდა შეგროვდეს, დაცულ იქნეს, ან გავრცელდეს პირველი ერების მონაცემები და ინფორმაცია. მიუხედავად ადგილობრივი ხალხის მკაფიოდ ჩამოყალიბებული პოლიტიკისა, ამ პრინციპების პრაქტიკული დანერგვა კვლავ მნიშვნელოვან სირთულეს წარმოადგენს როგორც მონაცემთა მმართველობის პოლიტიკის შემუშავებისა და განხორციელებისას, ისე “AI” ინსტრუმენტებისა და სისტემების დანერგვის პროცესში.

ადგილობრივი ხალხის ლიტერატურას, რომელიც ეხება ხელოვნურ ინტელექტსა და კოლექტიურ პირადი ცხოვრების ხელშეუხებლობის უფლებას, უდიდესი მნიშვნელობა აქვს. როგორც ადრე აღინიშნა ნაშრომში, თანამედროვე ხელოვნური ინტელექტის სისტემები შეიძლება ეწინააღმდეგებოდეს პირადი ცხოვრების ხელშეუხებლობის უფლებებს ზოგადად, მათ შორის, კოლექტიურ პირადი ცხოვრების ხელშეუხებლობის რისკების ახალ სფეროებს, რომლებიც ახალ ხელოვნურ ინტელექტსა და მანქანურ სწავლებაში ჩნდება. ადგილობრივი სოციალურ-ტექნიკური მიდგომები ხშირად ხაზს უსვამენ პირადი ცხოვრების ხელშეუხებლობის უფლებას, როგორც კოლექტიურ საკითხს და არა მხოლოდ ინდივიდუალურს; ეს პოლიტიკა დღეს კოლექტიური მიდგომების ძირითად არტიკულაციას წარმოადგენს, რადგან კოლექტიური პირადი ცხოვრების ხელშეუხებლობა ჯერ კიდევ არ არის წინა პლანზე განხილვის საგანი დომინანტურ კულტურაში.

---

[30] *Tsosie R.,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019).

[31] First Nations Information Governance Centre, *The First Nations Principles of OCAP*, <https://fnigc.ca/ocap-training/>.

ასევე, ფილოსოფოსებისა და ტექნოლოგების მიერ შექმნილი ნაშრომების რაოდენობა იზრდება მონაცემებზე, ხელოვნურ ინტელექტსა და კოლექტიურ კონფიდენციალობაზე. ეს ავტორები, როგორც წესი, არ ეხებიან ადგილობრივ იდეებს; ამის ნაცვლად, ისინი ყურადღებას ამახვილებენ იმაზე, თუ როგორ მოქმედებს ტექნოლოგიები კონფიდენციალობაზე. ფილოსოფოსმა ალესანდრო მანტელერომ დაწერა იმის შესახებ, თუ როგორ შეუძლია დიდ მონაცემებს და მოწინავე ანალიტიკას ხელი შეუწყოს მონაცემთა დაცვის გაფართოებას. ის წერს:

> „დიდი მონაცემების ანალიზის შედეგად შექმნილ ჯგუფებს უნიკალური ბუნება აქვთ, რომელიც მხოლოდ ინდივიდუალურ უფლებებზე ვერ იქნება დაფუძნებული. მონაცემების ახალი მასშტაბური შეგროვება გულისხმობს ახალი ფენის აღიარებას, რომელიც ჯგუფების კოლექტიური პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვას წარმოადგენს.“[32]

მენტელეროს მიერ აღნიშნული „ახალი ფენა“ მნიშვნელოვანი დაკვირვებაა, რომელიც დასტურდება ხელოვნური ინტელექტის ტექნიკური კვლევებით.[33] თუმცა, არსებული კანონმდებლობა, რომელიც ინდივიდუალურ უფლებების დაცვაზეა ფოკუსირებული, შექმნილია ისე, რომ კოლექტიური პირადი ცხოვრების ხელშეუხებლობა მრავალი თვალსაზრისით გაუფასურებულია. აღსანიშნავია, რომ დეპერსონალიზებულ მონაცემთა ნაკრები, როგორც წესი, პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონმდებლობის ძირითადი ნაწილის მიღმაა. ამან შეიძლება პრობლემები შექმნას დღეს, როდესაც დეპერსონალიზებული მონაცემები ანალიზდება და/ან ფასდება და შედეგები გავლენას ახდენს ფიზიკურ პირებზე. გარდა ამისა, ხელოვნური ინტელექტის თანამედროვე ფორმებს შეუძლიათ მონაცემთა მრავალმხრივი ანალიზის ჩატარება მონაცემების დეპერსონალიზაციის გარეშე და იდენტიფიცირებული მონაცემების ნახვის, გამოყენების ან გამჟღავნების უფლების გარეშე.[34] მიუხედავად იმისა, რომ ეს შეიძლება იყოს კონფიდენციალობის კუთხით სასარგებლო, ინდივიდებზე გავლენა შეიძლება იყოს როგორც დადებითი, ისე პრობლემური. ამ ტიპის პრაქტიკას მნიშვნელოვანი შედეგები აქვს სამყაროში, სადაც ხელოვნური ინტელექტის მოწინავე ფორმებს შეუძლიათ დეპერსონალიზებული და დაშიფრული მონაცემების ზუსტი ანალიზი, რომელთა გამოყენება შემდეგ შესაძლებელია

[32] *Mantellerò A.,* From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era, 2017. Group Privacy. Philosophical Studies Series, vol 126. Springer, Cham. <https://doi.org/10.1007/978-3-319-46608-8_8> [12.11.2025].

[33] მაღალი ენტიტატიურობის მქონე ჯგუფების კვლევა მოიცავს, მაგალითად, ენტიტატიურობის განმარტებას: *Lickel B., Hamilton D. L., Wieczorkowska G., Lewis A., Sherman S. J., Uhles A. N.,* Varieties of Groups and the Perception of Group Entitativity, Journal of Personality and Social Psychology, 78(2), 2000, 223–246. იხ.: 224 განმარტებისთვის. ხელოვნური ინტელექტის სპეციფიკური მაგალითი მოიცავს: *Liang C., Chen V., Shah J., Andrist S.,* Converting Spatial to Social: Using Persistent Homology to Understand Social Groups, ACM International Conference on Multimodal Interaction (ICMI), Canberra, Australia, 2025.

[34] *Nicholson W., Cohen G.,* Privacy in the Age of Medical Big Data, Nature Medicine 25, 2019, 37–43.

ჯგუფურ, საყოფაცხოვრებო ან თუნდაც ინდივიდუალური საქმიანობის ფარგლებში. დღეს მოქმედი დომინანტური პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონმდებლობა, როგორც წესი, უპირატესობას ანიჭებს ინდივიდუალურ პირადი ცხოვრების ხელშეუხებლობის უფლებებს კოლექტიურ კონფიდენციალობასთან შედარებით და, შესაბამისად, ხშირად გამორიცხავს დეპერსონალიზებული მონაცემების დაცვას.

მიულჰოფისა და რუშემაიერის აზრით, აღნიშნული პრობლემა პირადი ცხოვრების ხელშეუხებლობის საკითხში პროგნოზირებადი ანალიტიკისა და კოლექტიური კონფიდენციალობის დაცვის ნაკლებობის შედეგია. მათ თეორიას „პროგნოზირებად კონფიდენციალობას“ უწოდებენ. ეს საინტერესო ფორმულირებაა:

> „...ჩვენ ვამტკიცებთ, რომ ძირითადი უფლებების ინდივიდუალიზებული კონცეფცია ვერ ახერხებს პროგნოზირებადი ანალიტიკის შედეგების ადეკვატურად ასახვას. ჩვენ ვაჩვენებთ, რომ პროგნოზირებადი ანალიტიკა კოლექტიური კონფიდენციალობისა და არაფორმალური ძალაუფლების ასიმეტრიის პრობლემაა და პროგნოზირებად ანალიტიკაში მონაცემთა ძალაუფლების ფორმას „პროგნოზირების ძალად“ ვგულისხმობთ. გარკვეული აქტორების არარეგულირებადი პროგნოზირების ძალა სოციალურ რისკებს ქმნის, განსაკუთრებით თუ ინფორმაციის ძალაუფლების ასიმეტრიის ეს ფორმა ნორმატიულად არ არის წარმოდგენილი.“[35]

მიიჩნევა, რომ დეპერსონალიზებული მონაცემები დაცვას არ საჭიროებს. ამის მიზეზი ისაა, რომ კოლექტიური პირადი ცხოვრების ხელშეუხებლობა ხშირად ინდივიდუალურ პირადი ცხოვრების ხელშეუხებლობის უფლებას ნაკლებად მნიშვნელოვნად მიიჩნევს. ამას აქვს გარკვეული საფუძველი. მაგალითად, აშშ-ში “HIPAA”-ის კანონის მიხედვით, შესაძლებელია ჯანმრთელობასთან დაკავშირებული ინფორმაცია გაიგზავნოს ან გაიყიდოს, თუ დაცულია დეპერსონალიზაციის წესები. “HIPAA”-ის წესები შექმნილია 1990-იან წლებში და თანამედროვე AI-სა და ანალიზის პირობებში შესაძლოა მოძველებული იყოს, თუმცა იქიდან გამომდინარე, რომ საკმაოდ დამკვიდრებულია,[36] შეცვლა რთულია. ასევე, აშშ-ში „სამართლიანი საკრედიტო ანგარიშგების შესახებ“ კანონი მხოლოდ ფიზიკურ პირებზე ვრცელდება. შესაბამისად, იმ შემთხვევაში თუ ოჯახის რისკის ქულა იყენებს ფართო დემოგრაფიულ ინფორმაციას და გაერთიანებულ ფინანსურ მონაცემებს რეგულირებადი ელემენტების (როგორიცაა საკრედიტო ბიუროს მონაცემები), გამოყენების გარეშე, „სამართლიანი საკრედიტო ანგარიშგების

[35] *Muhlhoff R., Ruschemeier H.,* Predictive Analytics and the Collective Dimensions of Data Protection, 16.1 Law, Innovation and Technology, 2023.

[36] მაგალითად, HIPAA, ფედერალური კანონი ჯანდაცვის კონფიდენციალურობის შესახებ, უშვებს დეიდენტიფიცირებული მონაცემების გამოყენებას, როდესაც ისინი აკმაყოფილებენ გარკვეულ კრიტერიუმებს. ნაშრომი, რომელიც ასახავს, თუ როგორ აღიქმებოდა ტექნოლოგია იმ დროს, არის: S*weeney L.,* Weaving Technology and Policy Together to Maintain Confidentiality. Journal of Law, Medicine & Ethics, 25, nos. 2&3, 1997, 98-110.

შესახებ“ კანონით გათვალისწინებული უფლებები არ გამოიყენება.[37] ევროკავშირის მართლმსაჯულების სასამართლომ ცოტა ხნის წინ განმარტა ფსევდონიმით გაცემული მონაცემების დაცვის გარკვეული ასპექტები,[38] თუმცა, მონაცემების პირდაპირი ან ირიბი იდენტიფიცირებადობა კვლავ მთავარი კრიტერიუმია იმის დასადგენად, თუ როდის შეიძლება მონაცემების კლასიფიცირება პერსონალურ მონაცემებად.[39]

გაერთიანებულ ან დეპერსონალიზებულ მონაცემთა ნაკრების ხელახალი იდენტიფიკაციის რისკი ანალიტიკის გაუმჯობესებასთან ერთად ცვალებადია.[40] დამატებით გამოწვევას წარმოადგენს მონაცემების დეპერსონალიზებული სახით დამუშავება, რადგან, როგორც წესი, პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონმდებლობის ფარგლებში არ ექცევა, რომელიც ფოკუსირებულია ინდივიდუალურ უფლებებზე. მაგალითად, დიდი რაოდენობის მონაცემების ანალიზი და შემდეგი შეფასება შესაძლებელია მანქანური სწავლებისა და ხელოვნური ინტელექტის სხვადასხვა ტექნიკის გამოყენებით. ქულები — მიუხედავად იმისა, რომ ისინი არ შეიცავს იდენტიფიცირებად პირად მონაცემებს — შემდეგ შეიძლება გამოყენებულ იქნას სამეზობლოებზე, აღწერის ბლოკებზე ან ოჯახებზე[41]. ამ მაგალითის გაგრძელებით, მაღალი რისკის მქონე სამეზობლოებში მცხოვრებ პირებზე შეიძლება გავლენა იქონიოს; ეს შეიძლება მოხდეს მაშინაც კი, როდესაც სამეზობლო ქულა არის გაერთიანებული საზომი, რომელიც არ იყენებდა ან არ ავლენდა პირადად იდენტიფიცირებად ინფორმაციას.[42] მიუხედავად იმისა, რომ ამ პროცესის რეგიონული ვარიაციები შეიძლება არსებობდეს, რისკის ქულა, როდესაც გამოიყენება ადამიანთა ჯგუფზე, განსაკუთრებით თუ ინდივიდუალური მონაცემები ინახება დაჯგუფებული სახით, შეიძლება არ ვრცელდებოდეს რომელიმე კონკრეტული კანონით. ამასობაში, გაერთიანებული მონაცემები, კვლავ შეიძლება გამოყენებულ იქნეს

[37] Federal Trade Commission, Section 319 of the Fair and Accurate Credit Transactions Act of 2003: Fifth Interim Federal Trade Commission Report to Congress Concerning the Accuracy of Information in Credit Reports.

[38] ECLU:EU:C:2025:645, Case C-413/23 P, September 2025.

[39] Article 3 (6) of Regulation 2018/1725: „ფსევდონიმიზაცია“ ნიშნავს პერსონალური მონაცემების დამუშავებას ისე, რომ პერსონალური მონაცემები აღარ შეიძლება მიკუთვნდეს კონკრეტულ მონაცემთა სუბიექტს დამატებითი ინფორმაციის გამოყენების გარეშე, იმ პირობით, რომ ასეთი დამატებითი ინფორმაცია ინახება ცალკე და ექვემდებარება ტექნიკურ და ორგანიზაციულ ზომებს იმის უზრუნველსაყოფად, რომ პერსონალური მონაცემები არ მიკუთვნდეს იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.“ იხილეთ აგრეთვე მუხლი 3(1).

[40] *Sweeney L.,* You J. S., De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data*,* Harvard Journal of Technology Science, 2015, <https://techscience.org/a/2015092901/> [12.11.2025].

[41] *Dixon P.,* Gellman R., The Scoring of America, World Privacy Forum, 2014, <https://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf> [12.11.2025].

[42] Testimony of Pam Dixon regarding Data brokers and the impact on financial data privacy, credit, insurance, employment, and housing, before the United States Senate Committee on Banking, Housing, and Urban Affairs, 2019, <https://www.banking.senate.gov/hearings/data-brokers-and-the-impact-on-financial-data-privacy-credit-insurance-employment-and-housing> [12.11.2025].

ადამიანების კატეგორიზაციისთვის, ქცევის პროგნოზირებისთვის და მრავალფეროვანი ზემოქმედებისთვის.

წმინდა ტექნიკური თვალსაზრისით, დეპერსონალიზებული ან გაერთიანებული მონაცემების (მათ შორის, სამედიცინო მონაცემების) ხელოვნური ინტელექტით ანალიზი და შეფასება ადამიანთა ჯგუფების შესახებ დასკვნების გამოტანას უწყობს ხელს. თუმცა, როგორც ჩანს, ინდივიდუალური კონფიდენციალობის უფლებების მინიჭება, რომელიც ამჟამად კონფიდენციალობის შესახებ კანონმდებლობის უმეტეს ნაწილშია ხელმისაწვდომი, მნიშვნელოვნად არ უწყობს ხელს კოლექტიური კონფიდენციალობის ინტერესების დაცვას. ეს მოსაზრება ნათლად არის გამოკვეთილი ორი მაორი ავტორის მიერ, რომლებიც აღწერენ, თუ როგორ განსხვავდება არაადგილობრივი მოსახლეობის პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებული მიდგომები მათი მიდგომებისგან:

> „არსებობს შესამჩნევი განსხვავებები მაორებისა და არამაორების პირად ცხოვრებასთან დაკავშირებულ საკითხებს შორის. ეს განსხვავება აისახა რეფორმებთან დაკავშირებით ჩვენს განსხვავებულ მისწრაფებებში... ჩვენ ვამტკიცებთ, რომ მიუხედავად იმისა, რომ ახალი კანონი მხარს უჭერს პირადი ცხოვრების ინდივიდუალისტურ დასავლურ კონცეფციებს და ნაკლებად ითვალისწინებს პირადი ცხოვრების კოლექტიურ კონცეფციებს, მაორებისთვის მაინც შეიძლება პირადი ცხოვრების შესახებ კანონი სასარგებლოდ ჩაითვალოს გარკვეული მიზნების მისაღწევად...“[43]

კოლექტიური ინტერესები დასავლურ სამართალში თვალსაჩინოდ არ ჩანს. სადავოა არსებული დომინანტური კონფიდენციალობის შესახებ კანონების ეფექტიანობა ჯგუფური კონფიდენციალობის ასპექტების განხორციელებაში, გარკვეული სცენარების განხილვისას, მათ შორის, ხელოვნური ინტელექტის სისტემებთან დაკავშირებული სცენარების[44]. დომინანტური კანონები და ნორმები საკმარისად არ ითვალისწინებს იმას, რაც ადგილობრივ თემებს და სხვებს სჭირდებათ იმის უზრუნველსაყოფად, რომ კონფიდენციალობის შესახებ აზროვნებისა და პოლიტიკის კოლექტიური ფორმები ტომობრივ და სხვა დონეზე იყოს ინტეგრირებული და განხილული. გარდა ამისა, კონფიდენციალობის შესახებ მოქმედი კანონები ასევე საკმარისად არ ითვალისწინებს ადილობრივი თემების მიღმა კოლექტიური კონფიდენციალობის ინტერესების საჭიროებას.

[43] *Houghton J., Quince K.,* Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136, <https://researchspace.auckland.ac.nz/handle/2292/67023> [12.11.2025].

[44] *Gucluturk O.,* How to Handle GDPR Data Access Requests in AI-driven Personal Data Processing, 2024, <https://oecd.ai/en/wonk/gdpr-data-access-requests> [12.11.2025]. იხ.: discussion of broad consent regarding human subject research in this paper.

4. პირადი ცხოვრების ინდივიდუალური უფლება და პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონმდებლობის ევოლუციის მოკლე მიმოხილვა

პირადი ცხოვრების დაცვის შესახებ არსებული კანონმდებლობისა და ნორმების სპეციფიკის შესახებ დამატებითი კონტექსტუალიზაცია სასარგებლოა კოლექტიური მაგალითების განხილვამდე, რადგან ეს ნაშრომი განიხილავს დომინანტური და არადომინანტური პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონმდებლობის კონკრეტულ ელემენტებს.

დომინანტურ კანონმდებლობაში მოიაზრება ევროპაში დაფუძნებული ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”)[45] ფართო კონცეფციები. “GDPR” არ წარმოშობილა პოლიტიკური ვაკუუმიდან — არამედ ის დროთა განმავლობაში განვითარების ხანგრძლივი პროცესის გამოხატულებაა.

1960-იანი წლების ბოლოს, მონაცემთა მმართველობის,[46] მონაცემთა დაცვისა და კონფიდენციალობისადმი ინტერესი გაიზარდა, ძირითადად იმიტომ, რომ ინფორმაციული ტექნოლოგიები სწრაფად ვითარდებოდა. თავიდან პროგრესი ნელი იყო, მსოფლიოს სხვადასხვა კუთხეში მცირე

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[46] მონაცემთა მართვა და კონფიდენციალობა დაკავშირებულია, თუმცა მათი მნიშვნელობა განსხვავებულია. მიუხედავად იმისა, რომ ეს ტერმინები შეიძლება გამოყენებულ იქნას ტანდემში, ისინი ურთიერთშემცვლელი არ არის. მონაცემთა მართვა არის ორგანიზაციის ან ერთეულის მონაცემების მთლიანობისადმი ყოვლისმომცველი მიდგომა, რომელიც უზრუნველყოფს ინფორმაციის მართვას მონაცემთა სრული სასიცოცხლო ციკლის განმავლობაში. ეს შეიძლება მოიცავდეს მონაცემთა შეგროვების პრაქტიკას, მონაცემთა უსაფრთხოებას, ხარისხს, დოკუმენტაციას, კლასიფიკაციას, წარმომავლობას, კატალოგიზაციას, აუდიტს, გაზიარებას და სხვა ასპექტებს. მონაცემთა კონფიდენციალობა მონაცემთა მმართველობის ქვესიმრავლეა და საუკეთესოდ განისაზღვრება კონტექსტში, როგორც პერსონალური მონაცემების ან ადამიანთა ჯგუფის პერსონალური მონაცემების დაცვის ფორმები. იხ.: OECD’s *Recommendation on Privacy* (the Fair Information Practice Principles) or in Directive 95/46/EC, 1995 O.J. (L 281) 31 and the General Data Protection Regulation. როგორც ამ ნაშრომშია განხილული, მიუხედავად იმისა, რომ კონფიდენციალობის შესახებ ევროპული ყოვლისმომცველი კონცეფცია კანონმდებლობის თვალსაზრისით დომინანტურია, სხვა კულტურებში კონფიდენციალობის სხვა კონცეფციებიც არსებობს. მაგალითად, საზოგადოებაზე დაფუძნებული კონფიდენციალობის ნორმები, რომლებიც სხვა კულტურებთან ერთად მაორის მიდგომაშია ჩამოყალიბებული. ამ შემთხვევებში, როგორც ამ ნაშრომშია განხილული, კონფიდენციალობა განიხილება, როგორც საზოგადოების მახასიათებელი, რომელიც ადამიანთა ჯგუფს ეკუთვნის. იხ.: First Nations Information Governance Centre, The First Nations Principles of OCAP, https://fnigc.ca/ocap-training/(establishes how First Nations’ data and information will be collected, protected, used, or shared); იხ.: Te Mana Raraunga, the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz . For a general discussion of privacy, იხ.: *Bamberger K. A., Mulligan D. K.,* Privacy on the Books and on the Ground, 63 Stanford Law Review 247 (2011) (UC Berkeley Public Law Research Paper No. 1568385), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385> [12.11.2025].

ნაბიჯები იდგმებოდა.[47] სამართლიანი საინფორმაციო პრაქტიკა ("FIPs")[48], მონაცემთა მმართველობისა და პირადი ცხოვრების ხელშეუხებლობის ადრეულმა ძირითადმა დებულებამ, რომელიც 1973 წელს შეერთებულ შტატებში აღმოცენდა, ხელახლა ჩამოაყალიბა ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ ("OECD") 1980 წელს[49] და გახდა მთელი მსოფლიოს მასშტაბით პირადი ცხოვრების ხელშეუხებლობის შესახებ მრავალი კანონისა და პოლიტიკის საფუძველი.

დროთა განმავლობაში "FIPs" უკანა პლანზე გადავიდა, არა იმიტომ, რომ მათი პოლიტიკა არასწორი იყო, არამედ იმიტომ, რომ მათი ზოგადი პოლიტიკა, რომელიც დიდი ხნის განმავლობაში ასე კარგად მუშაობდა, საკმარისად სპეციფიკური არ იყო ტექნოლოგიების, ინდუსტრიისა და მთავრობის მიმდინარე განვითარების საკითხების მოსაგვარებლად. მაგალითად, ისინი არ ითხოვდნენ პირადი ცხოვრების ხელშეუხებლობის ორგანოების არსებობას, თუმცა მალევე იქნა აღიარებული მათი მნიშვნელობა და ღირებულება, რომელიც მსოფლიოში სწრაფად გავრცელდა. მონაცემთა დაცვის ორგანოები ფუნქციონირებენ, როგორც მონაცემთა დაცვისა და მმართველობის კანონების აღმასრულებლები და ისინი ეხმარებიან მონაცემთა მმართველობის ეკოსისტემების ეფექტიან განხორციელებას.[50]

ქვეყნებმა პირადი ცხოვრების ხელშეუხებლობის შესახებ კანონები 1970-იანი და 1980-იანი წლებიდან მიიღეს. დიდი დრო არ გასულა, სანამ ეროვნულ კანონმდებლობაში არსებულმა განსხვავებებმა და შეზღუდვებმა საერთაშორისო მონაცემთა ნაკადებთან დაკავშირებული პრობლემები შექმნა. ევროპამ ამ პრობლემების მოგვარება დაიწყო და ევროკავშირმა,

[47] The state of Hesse, Germany passed a federal law that regulated automated data processing in the public sector on October 7, 1970. (Bundesdatenschutzgesetz, or BDSG). იმავე თვესა და წელს აშშ-მ მიიღო პირველი მნიშვნელოვანი კანონი კონფიდენციალობის შესახებ, „სამართლიანი საკრედიტო ანგარიშგების აქტი", რომელიც ასევე ერთ-ერთი პირველი კანონია, რომელიც არეგულირებს მანქანურ სწავლებას. სხვა კანონებიც იქნა მიღებული ევროკავშირსა და აშშ-ში. 1981 წელს ევროკავშირმა ხელმოსაწერად გახსნა თავისი 108-ე კონვენცია ევროკავშირის წევრებისა და სხვა ქვეყნებისთვის. 1990-იან წლებში ევროკავშირმა მიიღო მონაცემთა დაცვის შესახებ მნიშვნელოვანი დირექტივა EU 95/46. მსოფლიოს 160-ზე მეტ იურისდიქციას ამჟამად აქვს მონაცემთა მმართველობის/მონაცემთა დაცვის კანონმდებლობის გარკვეული ფორმა, ძირითადად ევროკავშირის 95/46-ის მეორე თაობის, ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის, ნიმუშის მიხედვით. GDPR-ის ათვისება მოიცავს მოწიფულ და თითქმის გლობალურ მარეგულირებელ კვალს, თუმცა პოლიტიკასა და განხორციელებაში მნიშვნელოვანი განსხვავებები კვლავ რჩება.

[48] *Gellman R.,* Fair Information Practices: A Basic History, Version 2.32 (July 2025), <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf> [12.11.2025].

[49] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Feb. 12, 2002), <https://doi.org/10.1787/9789264196391-en> [12.11.2025].

[50] იხ.: Generally Global Privacy Assembly, https://globalprivacyassembly.org, (the Assembly is comprised of the international data protection and privacy commissioners or authorities. They met the first time in 1979). იხ.: Irish Data Protection Commission, https://www.dataprotection.ie; Data Protection Office Mauritius, https://dataprotection.govmu.org/SitePages/Index.aspx; Personal Information Protection Commission Japan, https://www.ppc.go.jp/en/; Office of the Privacy Commissioner for New Zealand (Te Mana Matapono Matatapu), <https://www.privacy.org.nz/privacy-act-2020/privacy-principles> [12.11.2025] (examples of the work of data protection authorities).

მნიშვნელოვანი ძალისხმევის შემდეგ, 1990-იან წლებში მიიღო მონაცემთა დაცვის დირექტივა.[51] დირექტივის ნაკლოვანებებისა და მისი განხორციელების სირთულეების გამო, იგი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ ჩანაცვლდა, რომელიც 2018 წლიდან ამოქმედდა.[52] მსოფლიოს მრავალი სხვა ქვეყანა ამჟამად გარკვეულწილად ევროკავშირის მოდელს მიჰყვება.[53] ეჭვგარეშეა, რომ “GDPR” ნორმატიულია. “GDPR” დღეს მონაცემთა დაცვის თითქმის გლობალური კანონმდებლობის საფუძველს წარმოადგენს.[54]

როდესაც კონფიდენციალობის შესახებ კანონები და ინსტიტუტები გაფართოვდა განვითარებად ქვეყნებში, გაირკვა, რომ გადაწყვეტილებები, რომლებიც თეორიულად კარგად გამოიყურებოდა, პრაქტიკაში ყოველთვის კარგად არ მუშაობდა. იდეები, რომლებიც მუშაობდა ერთ ქვეყანაში ან სოციალურ გარემოში, ყოველთვის არ ერგება სხვას.[55] მაგალითად, “GDPR”-ის მსგავსი კანონმდებლობა, რომელიც ფოკუსირებულია ინდივიდუალურ უფლებებზე, ყოველთვის კარგად არ ერგება ადგილობრივ კონტექსტს, სადაც პირადი ცხოვრების ხელშეუხებლობა განიხილება, როგორც საზოგადოებრივი უფლებები.[56] “GDPR”-ის ტიპის კანონები, ასევე, რთული მოსარგებია

[51] Directive 95/46/EC, 1995 O.J. (L 281) 31.

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[53] *Dixon P.,* Research; *Emerson J.,* Data Visualization and Design, Global Table of Countries with Data Privacy Laws, Treaties, or Conventions, World Privacy Forum, June 2024, <https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/> [12.11.2025].

[54] More than 165 countries or jurisdictions have passed either GDPR, or very similar legislation, or have a draft bill. იხ.: *Dixon P., Emerson J.,* Global Table of Countries with Data Privacy Laws, Treaties, or Conventions, World Privacy Forum. For a detailed discussion of GDPR and its impact; იხ.: *Greenleaf G.,* Global Data Privacy Laws 2023: International Standards Stall, but UK Disrupts, Privacy Laws & Business International Report 8-15, UNSW Law Research Paper No. 23-50, (2023). იხ.: *Greenleaf G.,* Global Data Privacy Laws 2023: 162 National Laws and 20 Bills. Privacy Laws and Business International Report (PLBIR) 1, 2-4, UNSW Law Research Paper No. 23-48, February 2023.

[55] *Pisa M., Dixon P., Ndulu B., Nwankwo U.,* Governing Data for Development: Trends, Challenges, and Opportunities, Center for Global Development, November 12, 2020. https://www.cgdev.org/publication/governing-data-development-trends-challenges-and-opportunities.

[56] როგორც ამ ნაშრომშია განხილული, ადგილობრივი მოსახლეობის მონაცემთა დაცვის უფლებების მხრივ მნიშვნელოვანი წინსვლაა. ეს ვრცელდება ადგილობრივი მოსახლეობის უფლებებზე, შეიმუშაონ მონაცემთა მართვის საკუთარი მეთოდები, რომლებსაც, კონტექსტიდან გამომდინარე, შეუძლიათ საზოგადოების დონეზე მიანიჭონ უფლებები, რომლებიც მნიშვნელოვნად განსხვავდება GDPR-ში გათვალისწინებული ინდივიდუალური კონფიდენციალობის უფლებებისგან. ამ კონტექსტუალურ განსხვავებებს მნიშვნელოვანი გავლენა აქვს ხელოვნური ინტელექტის მართვის ინსტრუმენტებსა და მათ გამოყენებაზე. იხ.: First Nations Information Governance Centre, The First Nations Principles of OCAP, https://fnigc.ca/ocap-training/(establishes how First Nations' data and information will be collected, protected, used, or shared); იხ.: *Raraunga Te M.,* the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz; იხ.: United Nations, G.A. Res 61/295 art. 18 (Sept. 13, 2007) (უზრუნველყოფს მკვიდრი მოსახლეობის უფლებას, მონაწილეობა მიიღონ გადაწყვეტილებების მიღების პროცესში იმ საკითხებში, რომლებიც გავლენას მოახდენს მათ უფლებებზე, მათ მიერ არჩეული წარმომადგენლების მეშვეობით, საკუთარი პროცედურების შესაბამისად, ასევე შეინარჩუნონ და განავითარონ საკუთარი მკვიდრი მოსახლეობის მიერ გადაწყვეტილების მიღების ინსტიტუტები).

მცირეკუნძულოვანი ერებისთვის, რომლებსაც შეზღუდული მოსახლეობა და რესურსები აქვთ, რაც განსაკუთრებით ართულებს მონაცემთა დაცვის სრული სისტემის შექმნას.[57] საერთო ჯამში, კონფიდენციალობის მართვის სწავლა ხანგრძლივი პროცესია და მონაცემთა ეკოსისტემის თითოეული დაინტერესებული მხარე კვლავ სწავლას განაგრძობს.

მონაცემთა დაცვის სფეროში მნიშვნელოვანი გლობალური დისკუსია მიმდინარეობს "GDPR"-ისა და ხელოვნურ ინტელექტს შორის ურთიერთმიმართებასთან დაკავშირებით. საკითხავია, შეესაბამება თუ არა "GDPR"-ის მიზნებს ხელოვნურ ინტელექტთან დაკავშირებული კონფიდენციალობის გამოწვევები და უნდა არსებობდეს თუ არა ახალი რეგულაციები, რომლებიც მხოლოდ ხელოვნურ ინტელექტზე ან მის ქვეჯგუფზე, როგორიცაა ხელოვნური ინტელექტის გენერირებადი ფორმები, იქნება ფოკუსირებული.

ხელოვნური ინტელექტის მარეგულირებელი საქმიანობის ტემპი ეწინააღმდეგება მონაცემთა მმართველობისა და კონფიდენციალობის კანონებისა და ნორმების განვითარებას, რომელიც ხანგრძლივი პერიოდის განმავლობაში მიმდინარეობდა. თუმცა, ხელოვნური ინტელექტის გარკვეული მოწინავე ფორმები საკმაოდ სწრაფად მოექცა საზოგადოებისა და პოლიტიკის ყურადღების ცენტრში, კონფიდენციალობის მარეგულირებელი საქმიანობის ტემპთან შედარებით. მაგალითად, "ChatGPT"-იმ 2022 წლის ნოემბრიდან[58] მრავალი მარეგულირებლის ყურადღება მიიპყრო. გენერირებად ხელოვნურ ინტელექტთან დაკავშირებული მოდელების სხვადასხვა ხარისხის განხილვები, წინადადებები და წესები სწრაფად განვითარდა.[59]

დღესდღეობით, აქტივობების საწყისმა ტალღამ გამოიწვია მრავალი კანონის საკმაოდ სწრაფი მიღება სუბნაციონალურ დონეზე, მაგალითად, ბევრმა იურისდიქციამ მიიღო სპეციალური კანონმდებლობა გენერირებად ხელოვნურ ინტელექტთან დაკავშირებით.[60]

ევროკავშირის ხელოვნური ინტელექტის აქტი მნიშვნელოვანი, ყოვლისმომცველი დოკუმენტია.[61] მიუხედავად იმისა, რომ სახელმწიფოთა

[57] *Dixon P.,* Research; *Emerson J.,* Data Visualization and Design, Global Table of Countries with Data Privacy Laws, Treaties, or Conventions, World Privacy Forum, 2024, <https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/> [12.11.2025]. იხ.: Small Island Nations filter. The small island group of countries has notably low adoption of GDPR-like regulations.

[58] *Introducing ChatGPT*, OpenAI, 30 November 2022, <https://openai.com/index/chatgpt/> [12.11.2025].

[59] იხ.: Generally the OECD AI Observatory, particularly the *Global AI law and Policy Tracker,* AI Observatory, OECD, <https://oecd.ai/en/dashboards/policy-initiatives> [12.11.2025].

[60] In the U.S. as of 2025 all 50 states have introduced or enacted laws regarding AI. იხ.: National Conference of State Legislators, Artificial Intelligence Legislation Tracker. <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation> [12.11.2025].

[61] EU Artificial Intelligence Act, Regulation – EU – 2024/1689. ნაშრომი არ განიხილავს ევროკავშირის ხელოვნური ინტელექტის აქტის (EU AI Act) გავლენას კოლექტიურ პირადი ცხოვრების ხელშეუხებლობაზე; მიუხედავად იმისა, რომ აღნიშნული აქტი ზოგიერთ კონკრეტულ კონტექსტში ჯგუფებს ეხება — მაგალითად, ის კრძალავს დისკრიმინაციას საკრედიტო ქულების განსაზღვრისას. ევროკავშირის AI აქტი კონკრეტულად არ ეხება კონფიდენციალურობას, ამიტომაც ეს საკითხი აქ არ განიხილება.

უმეტესობამ არ გაიზიარა ევროპის მაგალითი, ხელოვნურ ინტელექტთან დაკავშირებული კანონმდებლობის მიმართ დიდი დისკუსიაა, ასევე, პირადი ცხოვრების ხელშეუხებლობის შესახებ.[62]

აღსანიშნავია, რომ მანქანური სწავლების სხვადასხვა მოდელი გამოიყენებოდა მრავალი ათწლეულის განმავლობაში. მაგალითად, საკრედიტო რეგულაციები, რომლებიც ეხება მონაცემთა დამუშავებას, ალგორითმებს, ამოცანებსა და მანქანური სწავლების სხვა ასპექტებს — მოქმედებს ცალკეულ სახელმწიფოებში 1970-იანი წლებიდან.[63] მანქანური სწავლების რეგულაციების ეს ადრეული ფორმები ხშირად მოიცავს კარგად გააზრებულ და ნაცნობ მექანიზმებს, როგორიცაა: დაშვებული შეცდომების გამოსწორება, დავის ფორმალური გადაწყვეტის პროცესი, ზედამხედველობა და მომხმარებელთა უფლებების დაცვა. საკრედიტო ქულის მართვის მეთოდები პრაქტიკაში კარგად არის გააზრებული. ამ ტიპის რეგულაციებში გამოყენებული პროცედურული და ადმინისტრაციული კონტროლი საერთაშორისო დონეზე რეგულირდება. თუმცა, დღეს პირადი ცხოვრების ხელშეუხებლობის გამოწვევებთან დაკავშირებული ნორმატიული გადაწყვეტილებები არც ისე ეფექტურია ხელოვნური ინტელექტის კონტექსტებში. ხელოვნური ინტელექტის ახალი ციფრული სივრცე ჩვენთვის უცნობია, განსაკუთრებით იმის გათვალისწინებით, თუ როგორ იცვლება თავად პირადი ცხოვრების ხელშეუხებლობა ხელოვნური ინტელექტის ეკოსისტემებში.[64]

ხელოვნური ინტელექტის სფეროში მიღწეული პროგრესით წამოჭრილი ერთ-ერთი შეკითხვაა — საკმარისი იქნება თუ არა ინდივიდუალურ უფლებებზე დაფუძნებულ, რეგულაციებსა და პოლიტიკის დოკუმენტებში ამჟამად გამოყენებული მეთოდები პირადი ცხოვრების ხელშეუხებლობის რისკების კოლექტიური ფორმების მოსაგვარებლად, რომლებიც, განსაკუთრებით ხელოვნურ ინტელექტსა და მანქანური სწავლების ეკოსისტემებში ჩნდება. ამ შეკითხვაზე ყველა პასუხი ბოლომდე შემუშავებული არ არის, მაგრამ სულ უფრო ცხადი ხდება, რომ კოლექტიური პირადი ცხოვრების ხელშეუხებლობა ახალი სფეროა, რომლის მოწესრიგება საჭირო იქნება. წინამდებარე ნაშრომში წარმოდგენილი შემთხვევების ანალიზი ნათელს ჰფენს იმას, თუ სად არის

[62] *OECD AI Policy Navigator*, AI Observatory, OECD, <https://oecd.ai/en/dashboards/national> [12.11.2025]. See also: IAPP Global AI Law and Policy Tracker, IAPP. <https://iapp.org/resources/article/global-ai-legislation-tracker/> [12.11.2025].

[63] The Fair Credit Reporting Act in the U.S. is an exemplar of such a regulation. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.

[64] ხელოვნური ინტელექტის მართვის ინსტრუმენტების გლობალურმა მიმოხილვამ და მათი ეფექტიანობისა და მიზანშეწონილობის ანალიზმა აჩვენა, რომ არსებული ნორმები ჯერ ვერ ფარავს იმ პრობლემების სრულ სპექტრს, რომლებიც დაკავშირებულია კონფიდენციალურობის ავტომატიზაციასთან — ფაქტობრივად, მასშტაბურ მანქანურ ზედამხედველობასთან — სხვა გამოწვევებთან ერთად. Kate Kaye and Pam Dixon, *Risky Analysis: Assessing and Improving AI Governance Tools - An International review of AI governance tools and suggestions for pathways forward*, World Privacy Forum, December 2023.

ძირითადი ხარვეზები ამჟამინდელ სისტემაში და ბადებს ძირითად კითხვებს იმის შესახებ, თუ როგორ დავიწყოთ ფიქრი რისკების გადასაჭრელად.

5. კოლექტიური პირადი ცხოვრების ხელშეუხებლობის პრაქტიკული შემთხვევები

ნაშრომში განხილულია კოლექტიური პირადი ცხოვრების ხელშეუხებლობის სამი განსხვავებული შემთხვევა. შემთხვევები შეირჩა იმ მიზეზით, რომ მასში მონაწილე ჯგუფები ავლენენ იმგვარ სოციალურ ხასიათს, რაც აუცილებელია სამართლებრივი ანალიზისთვის საკმარისად მკაფიო შემთხვევების შესასწავლად.

პირველი შემთხვევის შესწავლა ფოკუსირებულია ადგილობრივი მოსახლეობის კოლექტიურ უფლებებზე, თავდაპირველად ფართოდ, შემდეგ კი ფოკუსირებულია სამთავრობო ხელშეკრულებაზე, რომელიც მაორებისთვის კოლექტიურ შეთანხმებას ადგენს. ეს არის მკაცრად განსაზღვრული ჯგუფი და ამ შემთხვევის შესწავლა საკანონმდებლო თვალსაზრისით განსაზღვრავს კოლექტიურ პირადი ცხოვრების ხელშეუხებლობას სპეციფიკურად. მეორე შემთხვევის შესწავლა ფოკუსირებულია კოლექტიურ პირადი ცხოვრების ხელშეუხებლობასა და გენეტიკური მონაცემების ბიოსამედიცინო ანალიზზე, რომელიც მოიცავს კიდევ ერთ ჯგუფს, ამერიკელი ინდიელების დნმ-ის შეფასებას აშშ-ს დიდი გენეტიკური ბიო ბანკის კონტექსტში. ამ შემთხვევის შესწავლაში განსაკუთრებულად საინტერესოა თანხმობის შესახებ კოლექტიური კონტექსტი და არსებული კანონმდებლობის მიერ გენეტიკური მონაცემების ხელახალი იდენტიფიკაციისგან დაცვის შეუძლებლობაზე. მესამე შემთხვევის შესწავლა ეხება ჰოლოკოსტის გადარჩენილს, რომელიც ცილისწამების მსხვერპლი გახდა, როგორც მაუტჰაუზენის საკონცენტრაციო ბანაკის გადარჩენილთა კოლექტიური ჯგუფის წევრი; მან სარჩელი შეიტანა იმ საფუძვლით, რომ მიუხედავად იმისა, რომ ცილისწამება კოლექტიური იყო, კანონით მინიჭებული პირადი ცხოვრების უფლებები მაინც უნდა მოქმედებდეს, რადგან ის კოლექტიური ჯგუფის იდენტიფიცირებადი წევრი იყო. ეს საქმე ევროპის მართლმსაჯულების სასამართლოში განიხილეს და მის სასარგებლოდ გადაწყდა.

5.1. შემთხვევის შესწავლა: ადგილობრივი კოლექტიური პირადი ცხოვრების ხელშეუხებლობა და მონაცემთა სუვერენიტეტი

მიუხედავად იმისა, რომ დღეს კანონმდებლობების უმეტესობა პირადი ცხოვრების ხელშეუხებლობას და მასთან დაკავშირებულ უფლებებს ძირითადად ინდივიდუალურ უფლებებად ასახელებს, იგი ასევე არსებობს,

როგორც კოლექტიური ან საზოგადოებაზე დაფუძნებული უფლება.[65] ჯგუფური პირადი ცხოვრების ხელშეუხებლობა შეიძლება მოიძებნოს მმართველობის მთელ სპექტრში, მრავალმხრივ ეროვნულ და ტომობრივ უფლებების დონეზე.

საერთაშორისო ჩვეულებითი სამართალი უზრუნველყოფს არსებით უფლებებს ადგილობრივი მოსახლეობისთვის.[66] ყველაზე მნიშვნელოვანი დოკუმენტია გაერთიანებული ერების ორგანიზაციის დეკლარაცია ადგილობრივ მოსახლეობათა უფლებების შესახებ ("UNDRIP"), რომელიც განსაზღვრავს ადგილობრივი მოსახლეობის თვითმმართველობის ძირითად უფლებებს.[67] რამდენიმე სახელმწიფო უკვე იყენებს იგივე პრინციპებს ხელოვნური ინტელექტის პრაქტიკულ გამოყენებასთან დაკავშირებით.

"UNDRIP"-ის რამდენიმე მუხლი ასახავს კოლექტიური უფლებების, ავტონომიის, თვითმმართველობისა და პირადი ცხოვრების ხელშეუხებლობის გარკვეული უფლებების ძირითად კონტურებს, სხვა საკითხებთან ერთად:

მუხლი 4

თვითგამორკვევის უფლების განხორციელებისას, ადგილობრივ მოსახლეობას აქვს ავტონომიის ან თვითმმართველობის უფლება მათ შიდა და ადგილობრივ საქმეებთან დაკავშირებულ საკითხებში, ასევე მათი ავტონომიური ფუნქციების დაფინანსების გზებისა და საშუალებების შესახებ.

მუხლი 7

1. ადგილობრივ მოსახლეობას აქვს სიცოცხლის, ფიზიკური და ფსიქიკური მთლიანობის, თავისუფლებისა და პირადი უსაფრთხოების უფლება.

[65] მაგალითად, მაორებს აქვთ კოლექტიური კონფიდენციალურობის გამოკვეთილი და კარგად განვითარებული კონცეფციები, რომლებიც გამყარებულია მათ კულტურასა და ტომობრივ კანონებში. მაორები კონფიდენციალურობას განიხილავენ როგორც კოლექტიურ უფლებას, რომელიც კოლექტიურად უნდა განხორციელდეს. არსებობს დეტალური ლიტერატურა მაორებისთვის კოლექტიური კონფიდენციალურობის კონცეფციის შესახებ. ეს ნაშრომი წარმოგიდგენთ ამ კონცეფციას და ავითარებს მას ინდივიდუალური კონფიდენციალურობის კონცეფციებთან შედარებით. See, e.g., Khylee Quince and Jayden Houghton, Privacy and Māori Concepts in Stephen Penk and Nikki Chamberlain (eds) _Privacy Law in New Zealand_ (3rd ed, Thomson Reuters, Wellington, 2023) 43–136.

[66] ჩვეულებრივ, საერთაშორისო სამართალში (Customary International Law) საუბარია საერთაშორისო ვალდებულებებზე, რომლებიც წარმოიქმნება დამკვიდრებული საერთაშორისო პრაქტიკიდან და არა ფორმალური წერილობითი კონვენციებისა და ხელშეკრულებების საფუძველზე. ადგილობრივი ხალხების უფლებებსა და კონფიდენციალურობასთან დაკავშირებულ სამართალში შედის გაერთიანებული ერების ორგანიზაციის ადგილობრივი ხალხების უფლებების დეკლარაცია (UNDRIP), რომელიც ადგენს ადგილობრივი ხალხების ძირითადი უფლებებს თვითმმართველობისთვის. ეროვნული კანონმდებლობის დონეზე ეს იდეები განმარტებულია, მაგალითად, აშშ-ს ფედერალურ კანონში, კანადის კანონმდებლობასა და ნიუ ზელანდიის კანონმდებლობაში.

[67] United Nations Declaration on the Rights of Indigenous Peoples, Resolution adopted by the General Assembly on 13 September 2007, 62/295.

2. ადგილობრივ მოსახლეობას აქვს კოლექტიური უფლება, იცხოვროს თავისუფლად, მშვიდობიანად და უსაფრთხოდ, როგორც განსხვავებულმა ხალხმა, და არ უნდა დაექვემდებაროს გენოციდის ან სხვა ძალადობის აქტს, მათ შორის ჯგუფის ბავშვების იძულებით გადაყვანას სხვა ჯგუფში.

მუხლი 12

1. ადგილობრივ მოსახლეობას აქვს უფლება გამოხატოს, შეასრულოს, განავითაროს და ასწავლოს თავისი სულიერი და რელიგიური ტრადიციები, წეს-ჩვეულებები და ცერემონიები; უფლება შეინარჩუნონ, დაიცვან და ჰქონდეთ წვდომა მათ რელიგიურ და კულტურულ ადგილებზე; უფლება გამოიყენონ და აკონტროლონ თავიანთი ცერემონიალური ნივთები; და უფლება დაიბრუნონ თავიანთი გარდაცვლილი წინაპრების ნეშტი.

მუხლი 18

ადგილობრივ მოსახლეობას უფლება აქვს მონაწილეობა მიიღოს გადაწყვეტილების მიღებაში იმ საკითხებში, რომლებიც გავლენას მოახდენს მათ უფლებებზე, მათ მიერ არჩეული წარმომადგენლების მეშვეობით, საკუთარი პროცედურების შესაბამისად, ასევე შეინარჩუნონ და განავითარონ საკუთარი გადაწყვეტილების მიმღები ინსტიტუტები.

მუხლი 19

სახელმწიფოები კეთილსინდისიერად ატარებენ კონსულტაციებს და თანამშრომლობენ ადგილობრივ მოსახლეობასთან საკუთარი წარმომადგენლობითი ინსტიტუტების მეშვეობით, რათა მიიღონ მათი თავისუფალი, წინასწარი და ინფორმირებული თანხმობა საკანონმდებლო ან ადმინისტრაციული ზომების მიღებამდე და განხორციელებამდე, რომლებმაც შეიძლება გავლენა მოახდინონ მათზე.

ეს იდეები ჩამოყალიბებულია აშშ-ის ინდიელთა კანონმდებლობაში, კანადის კანონმდებლობასა და ახალი ზელანდიის კანონმდებლობაში. გარდა ამისა, ადგილობრივი მოსახლეობის მნიშვნელოვანი პოლიტიკის დოკუმენტები ეხება ტომობრივ დონეზე შენახულ მონაცემებს. ამ ლიტერატურის ერთ-ერთი მთავარი კონტრიბუტორი — ცოსი, ამტკიცებს, რომ ტომობრივ მთავრობებს აქვთ უფლებამოსილება, მიიღონ მონაცემთა კონფიდენციალურობის შესახებ კანონები ტომობრივ დონეზე, რათა განსაზღვრონ, თუ რა წარმოადგენს „ტომობრივ მონაცემებს“.[68] ეს არის

[68] *Tsosie R.,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019)

ფუნდამენტური უაღრესად აქტუალური საკითხი ხელოვნური ინტელექტისა და კვლევისთვის, სხვა სფეროებთან ერთად. ამ საკითხებთან დაკავშირებულია კოლექტიური მონაცემთა საკუთრება, კოლექტიური პირადი ცხოვრების ხელშეუხებლობის უფლებები და ეთიკური პრინციპების კოლექტიური გამოყენება. ამ ტიპის მიდგომები შეიძლება ვნახოთ, მაგალითად, აშშ-ის მკვიდრი მოსახლეობის მონაცემთა სუვერენიტეტის ქსელსა და მაორის მონაცემთა მმართველობის მოდელში. კიდევ ერთი მმართველობის ჩარჩოა "OCAP"-ის პირველი ერების პრინციპები. "OCAP" (საკუთრება, კონტროლი, წვდომა და ფლობა) ნათლად განსაზღვრავს,[69] თუ როგორ შეგროვდება, დაცული იქნება, გამოიყენება ან გაიზრდება პირველი ერების მონაცემები და ინფორმაცია კანადაში. კანადაში ხელოვნური ინტელექტის სტანდარტების შემუშავების ნებისმიერი სამუშაო უნდა უზრუნველყოფდეს "OCAP"-ის პრინციპების დაცვას და კანადის პირველი ერების წარმომადგენლებს სტანდარტების შემუშავების პროცესებში მონაწილეობის მიღებას.

ხელოვნური ინტელექტის თვალსაზრისით, მაორებმა შექმნეს მნიშვნელოვანი და გავლენიანი პოლიტიკური ლიტერატურა, რომელშიც ავტორები — კუკუტაი და სხვები განმარტავენ, რომ პირადი ცხოვრების ხელშეუხებლობის ადგილობრივი კონცეფციები თანდაყოლილი და კოლექტიურია. ახალი ზელანდიის მთავრობა მაორებთან ერთად თანამშრომლობს ხელოვნური ინტელექტის პოლიტიკის ჩარჩოების შემუშავებაზე, რომლებიც გამოყენებული იქნება ყოველთვის, როდესაც საქმე ადგილობრივ მონაცემებს ან უფლებებს ეხება. ახალი ზელანდიის მიდგომა ხელოვნური ინტელექტის მიმართ მნიშვნელოვან პრეცედენტს ქმნის. ახალი ზელანდიის მიდგომის სტრუქტურა პოტენციურად მნიშვნელოვან გრძელვადიან გავლენას მოახდენს გლობალური სტანდარტიზაციის მოდელებსა და ძალისხმევაზე.

5.2. ახალი ზელანდიის მთავრობისა და მაორი მოსახლეობის მონაცემთა მმართველობის ერთობლივი დიზაინის შემუშავება

პირველ რიგში, ახალმა ზელანდიამ ხელოვნური ინტელექტის სფეროში მუშაობა ადრეულ ეტაპზევე დაიწყო. 2017 წელს მანდატის საფუძველზე შემოღებულ იქნა მონაცემთა სამთავრობო მენეჯერის როლი.[70] ახალ ზელანდიას უკვე აქვს მონაცემთა მართვის სფეროში მუშაობისა და პრაქტიკის გამოცდილება. მონაცემთა მთავარი მენეჯერის როლს ასრულებს ახალი

[69] The First Nations Principles of OCAP, First Nations Information Governance Centre, <https://fnigc.ca/ocap-training/> [12.11.2025].

[70] Government Chief Data Steward Mandate, Office of the Minister of Statistics New Zealand, <https://www.stats.govt.nz/assets/Uploads/Corporate/Cabinet-papers/Strengthening-data-leadership-across-government-to-enable-more-effective-public-services/strengthening-data-leadership-across-government-to-enable-more-effective-public-services-redacted.pdf> [12.11.2025].

ზელანდიის სტატისტიკის აღმასრულებელი დირექტორი (“Stats New Zealand”). ამ როლს რამდენიმე ფუნქცია აქვს: სავალდებულო სტანდარტების დადგენა; „მონაცემთა შეგროვების, მართვისა და გამოყენებისადმი საერთო მიდგომის უზრუნველყოფა“ და „მონაცემთა საერთო შესაძლებლობების დანერგვის ხელმძღვანელობა“.

მონაცემთა მთავარმა მენეჯერმა შეიმუშავა მონაცემთა სტრატეგია და გზამკვლევი,[71] ხელმძღვანელობდა ხელოვნური ინტელექტის გამჭვირვალობისა და ანგარიშვალდებულების განვითარებას,[72] შექმნა მონაცემთა მართვის ფართო ჩარჩო, იმუშავა ღია მონაცემებზე და შეიმუშავა თანამშრომლობის ჩარჩო მაორებთან თანამშრომლობით.[73] თავდაპირველად, ამ ძალისხმევის მიზანი იყო იმის უზრუნველყოფა, რომ Covid-19-თან დაკავშირებით შესრულებული სამუშაო შესაბამისობაში ყოფილიყო მაორების მიდგომებთან.

სტრუქტურულად, ახალი ზელანდიის მონაცემთა მართვის ჩარჩო ინკლუზიური და დამოკიდებულია მთავრობაზე. ახალი ზელანდია აღწერს მონაცემთა მართვის ჩარჩოს, როგორც ახალი ზელანდიის მონაცემთა სისტემაში მმართველობითი ფუნქციების მქონე როლების ფართო სპექტრს, მათ შორის, მონაწილეობს:

- მთავრობის მონაცემთა მთავარი მენეჯერი,
- მთავრობის მთავარი ინფორმაციული უსაფრთხოების ოფიცერი,
- მთავრობის მთავარი ციფრული ოფიცერი,
- მთავრობის მთავარი კონფიდენციალურობის ოფიცერი.

კონფიდენციალურობის კომისარს, ომბუდსმენს, გენერალურ აუდიტორს და მთავარ არქივს ასევე აქვთ როლები.

პირადი ცხოვრების ხელშეუხებლობის კომისრის უფლებამოსილება განსაზღვრულია 2020 წლის ახალი ზელანდიის პირადი ცხოვრების ხელშეუხებლობის აქტში, რომელიც მოიცავს ინფორმაციის კონფიდენციალურობის 13 პრინციპს და მოითხოვს, რომ სააგენტოებმა გარკვეული მონაცემთა დარღვევის შესახებ შეატყობინონ კომისარს. ახალი ზელანდიის პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობა ითვალისწინებს “GDPR”-ს და, შესაბამისად, ის კვალიფიცირდება, როგორც მონაცემთა დაცვის თანამედროვე კანონი, თუმცა აქტი არ არის “GDPR”-ის იდენტური და იყენებს განსხვავებულ ტერმინოლოგიას.

---

[71] The Government Data Strategy and Roadmap, Government Chief Data Steward, September 2021, <https://www.data.govt.nz/leadership/strategy-and-roadmap/> [12.11.2025].

[72] Algorithm Assessment Report, Stats NZ, 2018, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/> [12.11.2025].

[73] Māori Data Governance Co-design Review, Te Kāhui Raraunga, January 2021, <https://www.kahuiraraunga.io/_files/ugd/b8e45c_0b1a378da21c459eb4fb88dfbf6aea81.pdf> [12.11.2025]. See also: COVID-19 Lessons Learnt: recommendations for improving the resilience of New Zealand’s government data system. Stats NZ Tatauranga Aotearoa, March 2021, <https://data.govt.nz/docs/covid-19-recs-report/> [12.11.2025].

ახალი ზელანდიის მიდგომა ალგორითმების, ანუ ხელოვნური ინტელექტისა და მანქანური სწავლების მიმართ პროგრესული და ინკლუზიურია. 2018 წელს ახალმა ზელანდიამ გამოაქვეყნა ალგორითმების შეფასების ანგარიში, რომელიც მოიცავდა 14 სამთავრობო უწყების პრაქტიკას.[74] ეს არის მონაცემთა მმართველობის, მენეჯმენტის, სტანდარტების, მმართველობის, ღია მონაცემებისა და კონფიდენციალურობის შესახებ საფუძვლიანი განხილვის ერთ-ერთი პირველი მაგალითი ალგორითმების მთავრობის მიერ გამოყენების სფეროში. 2018 წლის ანგარიშმა გამოიწვია 2020 წლის ივლისში ახალი ზელანდიის ალგორითმების ქარტიის პირველი ვერსიის გამოქვეყნება სტატისტიკის მინისტრის მიერ.[75] ქარტია გამოირჩევა ხელოვნური ინტელექტის მიერ ინფორმირებული გადაწყვეტილებების გასაჩივრების საშუალებების უზრუნველყოფის მიდგომით. ახალმა ზელანდიამ ასევე გამოუშვა ალგორითმების საწყისი ნაკრები 2021 წელს ქარტიის განსახორციელებლად.[76]

2024 წლის მდგომარეობით, ახალი ზელანდიის მთავრობამ განაახლა და გააფართოვა ხელოვნურ ინტელექტთან დაკავშირებული მასალები თავისი წესდების ფარგლებში, ყოვლისმომცველი ინსტრუმენტების ნაკრების სახით, რომლის უახლესი განახლება 2023 წელს მოხდა.[77]

ადგილობრივ მოსახლეობაზე დაფუძნებული მიდგომებისთვის დამახასიათებელია ახალი ზელანდიის მთავრობის ალგორითმის გავლენის შეფასების მომხმარებლის სახელმძღვანელო.[78] სახელმძღვანელო გვთავაზობს ახალი ზელანდიის მაორებთან ურთიერთობის დეტალურ განხილვას. ის კონკრეტულად ასახავს მის ვალდებულებას, პატივი სცეს მონაცემებთან დაკავშირებულ მაორების მიდგომას და უზრუნველყოფს, რომ ალგორითმების გამოყენება შეესაბამებოდეს მისი წესდების მუხლებსა და დებულებებს.

სახელმძღვანელოში 29-ე გვერდზე აღნიშნულია:

„ზოგადი მითითებები ქარტიაში პარტნიორობის ვალდებულების შესასრულებლად, თქვენ უნდა:

[74] Algorithm Assessment Report, Stats NZ, 2018, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/> [12.11.2025].

[75] Algorithm Charter for Aotearoa New Zealand, Stats NZ. July 2020, <https://www.data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf> [12.11.2025].

[76] Government Algorithm Transparency and Accountability, Stats NZ. March 2021, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability> [12.11.2025].

[77] ახალი ზელანდიის აოტეაროას ალგორითმის ქარტია, რომელიც მოიცავს შემდეგ ფუნდამენტურ ნაშრომებს: მონაცემთა და ანალიტიკის უსაფრთხო და ეფექტური გამოყენების პრინციპები. სანდო ხელოვნური ინტელექტი აოტეაროაში - ხელოვნური ინტელექტის პრინციპები. ღია მმართველობის პარტნიორობა. მონაცემთა დაცვისა და გამოყენების პოლიტიკა და კონფიდენციალურობის, ადამიანის უფლებებისა და ეთიკის ჩარჩო.

[78] Algorithm impact assessment user guide, New Zealand Government, Te Kāwanatanga o Aotearoa, December 2023, <https://data.govt.nz/assets/data-ethics/algorithm/AIA-user-guide.pdf> [12.11.2025].

- ჩართოთ “te ao Mãori”-ს პერსპექტივები ალგორითმების დიზაინსა და გამოყენებაში
- უზრუნველყოთ ალგორითმის შემუშავება და გამოყენება “Te Tiriti o Waitangi”-სთან შესაბამისობაში
- გაითვალისწინოთ, თუ როგორ შენარჩუნდება მაორის მონაცემთა სუვერენიტეტი
- შეაფასოთ, თუ როგორ იმოქმედებს ალგორითმის გამოყენება “iwi”-სა და მაორის ცხოვრებაზე.

"Te ao Mäori“ აღიარებს ყველა ცოცხალი და არაცოცხალი არსების ურთიერთკავშირს სულიერი, კოგნიტური და ფიზიკური ლინზების მეშვეობით. ეს მიდგომა ცდილობს გაიგოს მთელი გარემო და არა მხოლოდ მისი ნაწილები. (ეს განმარტება მომდინარეობს ვაიტანგის ხელშეკრულებიდან/”Te Tiriti”-დან და მაორის ეთიკის სახელმძღვანელო პრინციპებიდან: ხელოვნური ინტელექტი, ალგორითმები, მონაცემები და ნივთების ინტერნეტი.

ალგორითმული შეფასების მომხმარებლის სახელმძღვანელოს შემდგომ ნაწილში, 32-ე გვერდზე, კითხვა 5.3-ში აღნიშნულია, რომ:

მაორის მონაცემები არ ეკუთვნის რომელიმე ერთ ინდივიდს, არამედ ეკუთვნის ერთ ან რამდენიმე ოჯახს. ინდივიდების უფლებები, მონაცემებთან დაკავშირებული რისკები და სარგებელი უნდა იყოს დაბალანსებული იმ ჯგუფების უფლებებთან, რომელთა ნაწილსაც ისინი წარმოადგენენ. მაორის მონაცემთა სუვერენიტეტი აღიარებს, რომ მაორის მონაცემები უნდა ექვემდებარებოდეს მაორის მმართველობას - მაორის უფლებას, ფლობდეს, აკონტროლოს, ჰქონდეს წვდომა და ფლობდეს მაორის მონაცემებს. მაორის მონაცემთა სუვერენიტეტი მხარს უჭერს ტომობრივ სუვერენიტეტს და მაორისა და ივი-ს მისწრაფებების რეალიზაციას.

ახალი ზელანდიის მთავრობის მიერ მონაცემებთან და ხელოვნურ ინტელექტთან დაკავშირებული ადგილობრივი მიდგომების აღიარება ხელოვნური ინტელექტის პოლიტიკაში სხვა მთავრობებისთვის კრიტიკულად მნიშვნელოვან მაგალითს წარმოადგენს. შესაძლებელია მონაცემებთან დაკავშირებით მრავალი თვალსაზრისის გათვალისწინება. მნიშვნელოვანი იქნება იმის უზრუნველყოფა, რომ გლობალური სტანდარტების შემუშავების ძალისხმევა ითვალისწინებდეს ადგილობრივი მიდგომების გამოყენებას, რომლებიც სხვა ქვეყნებში ფორმალურ ხელმძღვანელობას ან კანონს წარმოადგენს. შეიძლება ითქვას, რომ სტანდარტების შემუშავების პროცესში კარგი იქნება არაფორმალური ხელმძღვანელობის გათვალისწინებაც.

ხელოვნური ინტელექტის სტანდარტებისა და პოლიტიკისთვის ადგილობრივ კონტექსტში, რამდენიმე ეროვნულმა მთავრობამ “UNDRIP” მიიღო, როგორც ეროვნული კანონმდებლობა. მაგალითად, ახალი ზელანდია “UNDRIP”-ის ხელმომწერია და მას ოფიციალური შეთანხმებები აქვს. 2021 წელს კანადამ მიიღო აქტი, რომელიც ეხება გაეროს ადგილობრივი

მოსახლეობის უფლებების დეკლარაციას. ეს კანონპროექტი კანადის კანონმდებლობას UNDRIP-თან შესაბამისობაში მოჰყავს.[79]

5.3. შემთხვევის შესწავლა: ბიოსამედიცინო კვლევა და კოლექტიური კონფიდენციალურობა: გენეტიკური ბიო ბანკის მონაცემების კვლევისთვის გამოყენების „ფართო თანხმობა“ შესაძლოა არ იყოს გათვალისწინებული საერთო წესით ან ჯანმრთელობის ან კვლევის კონფიდენციალურობის შესახებ სხვა კანონმდებლობით

ბიოსამედიცინო კვლევის სუბიექტებს ხშირად შეიძლება ჰქონდეთ კოლექტიური კონფიდენციალურობის ინტერესები ბიო ბანკებში, რომლებიც ინახავს მათ ბიოლოგიურ ან გენეტიკურ ნიმუშებს და სხვა მონაცემებს, რომლებიც გამოიყენება სამედიცინო კვლევაში ანალიზისთვის. ამ სფეროში მნიშვნელოვანი შემთხვევის შესწავლა აშშ-ში ჩატარებული ბიოსამედიცინო კვლევის მასშტაბური ძალისხმევიდან მოდის. 2015 წელს, აშშ-ში ჯანმრთელობის ეროვნულმა ინსტიტუტებმა (“NIH”) წამოიწყეს ზუსტი მედიცინის ინიციატივა, რომლის მიზანიც კვლევისთვის 1 მილიონი ბიონიმუშის შეგროვება იყო.[80;81] “NIH”-მა კონსულტაციები ჩაატარა ტომის დაინტერესებულ მხარეებთან თავისი ბიო ბანკის პროექტისთვის და საჯაროდ აღიარა ტომის სუვერენიტეტი. “NIH”-მა ამ ჩართულობის შესახებ ანგარიში 2023 წელს დაწერა.[82] ანგარიში მრავალი თვალსაზრისით რევოლუციურია და შეიცავს ტომის შეშფოთების მნიშვნელოვან არტიკულაციას. ანგარიშის თანახმად, „კონსულტაციის პროცესის მეშვეობით, ტომის ლიდერებმა გამოთქვეს ღრმა შეშფოთება მონაცემების მეორადი (მომავლის) კვლევისთვის გამოყენების შესახებ...“.[83]

ასევე, ანგარიშში, “NIH”-მა კონკრეტულად აღწერა ჯგუფური ან კოლექტიური პირადი ცხოვრების ხელშეუხებლობის გავლენა, რაც ამ შემთხვევაში შეიძლება გამომდინარეობდეს ტომობრივი კვლევის მონაწილის იდენტიფიცირებადი ჯგუფის ნაწილად იდენტიფიცირების შესაძლებლობიდან.

“NIH”-ის პასუხი ამ საკითხზე მნიშვნელოვანია, რადგან ის შეიცავს „ფართო თანხმობის“ იდეის იშვიათ განხილვას და დეიდენტიფიკაციის კონტექსტში კონკრეტული ჯგუფისთვის კუთვნილების იდენტიფიცირებული მონაცემების მეორად გამოყენებას. დეიდენტიფიკაცია, აშშ-ს კონტექსტში,

[79] An Act respecting the United Nations Declaration on the Rights of Indigenous Peoples, Bill C-15, Parliament of Canada, <https://www.parl.ca/LegisInfo/en/bill/43-2/C-15> [12.11.2025].

[80] All of Us Research Program, National Institutes of Health, <https://allofus.nih.gov/about/faq> [12.11.2025].

[81] *Gellman R., Dixon P.,* Privacy, the Precision Medicine Initiative, & the All of Us Research Program: Will Any Legal Protections Apply? World Privacy Forum, March 16, 2017.

[82] All of Us Tribal Engagement, NIH, <https://allofus.nih.gov/about/diversity-and-inclusion/tribal-engagement> [12.11.2025].

[83] All of Us Research Program Tribal Consultation Final Report March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].

როგორც ეს ამ ნაშრომშია განხილული, როგორც წესი, ქმნის გამონაკლისებს კანონიდან, მაშინაც კი, როდესაც საქმე გენეტიკურ ან ბიოლოგიურ მონაცემებს ეხება, კონტექსტიდან გამომდინარე. ეს გამონაკლისი განსაკუთრებით რთულია, როდესაც ის ეხება კვლევას, რომელიც მოიცავს ბიოლოგიურ ნიმუშებს და გენეტიკური კავშირის პოტენციალს.

“NIH”-მ თავის ანგარიშში განაცხადა:

„ფართო თანხმობა და მეორადი კვლევა

კვლევითი პლატფორმის ფარგლებში მოწოდებული ყველა მონაცემი და ბიოლოგიური მასალა იქნება დეპერსონალიზებული საერთო სტანდარტების შესაბამისად. პროგრამა „ყველა ჩვენგანი“ (“All of Us”) არ გეგმავს რომელიმე პირდაპირ იდენტიფიცირებადი მონაცემის ან ბიოლოგიური მასალის გაზიარებას. ამ ეტაპზე პროგრამა არ ითხოვს ფართო (“broad”) თანხმობას მეორადი კვლევებისთვის იმ ფორმით, როგორც ეს განსაზღვრულია 2018 წლის საერთო სტანდარტების დოკუმენტში. ასეთი თანხმობა სავალდებულო გახდება მხოლოდ იმ შემთხვევაში, როდესაც მონაცემების მეორადი გამოყენება ეხება პირდაპირ იდენტიფიცირებად მონაცემებსა და ნიმუშებს. მონაცემთა ტიპები ჩაითვლება „იდენტიფიცირებადად“, თუ არსებობს მნიშვნელოვანი ალბათობა, რომ ამ მონაცემების საფუძველზე – ცალკე ან სხვა მონაცემებთან ერთად – შესაძლებელია კონკრეტული ფიზიკური პირის იდენტიფიცირება. სხვა სიტყვებით რომ ვთქვათ, იდენტიფიცირებადობა უფრო კონტექსტზეა დამოკიდებული, ვიდრე ცალკეულ მონაცემზე. თუმცა, გარკვეული მონაცემები, მაგალითად სახელი ან სოციალური უსაფრთხოების ნომერი, თავისთავად იძლევა ფიზიკური პირის პირდაპირი იდენტიფიცირების შესაძლებლობას. გარდა ამისა, ზოგიერთი სხვა ტიპის მონაცემი ან მისი ელემენტი — მათ შორის ელექტრონული ჯანმრთელობის ჩანაწერების ტექსტური (ნარატიული) ველები — ითვლება პოტენციურად იდენტიფიცირებადად, რადგან ასეთი ველებში იდენტიფიკატორები ხშირად გვხვდება. შესაბამისად, მათი დეპერსონალიზაცია აუცილებელია, რათა ამ მონაცემების გაზიარება მკვლევრებისთვის შესაძლებელი გახდეს.

საგულისხმოა, რომ მონაცემების საფუძველზე ფიზიკური პირების იდენტიფიცირების რისკის შეფასება არ მოიცავს ჯგუფის იდენტიფიცირებადობასთან დაკავშირებულ პრობლემებსაც. კვლევითი პროცესის მნიშვნელოვანი ნაწილი ხშირად არის მონაცემების ჯგუფებად დაყოფა და ქვეჯგუფების გამოყოფა, თუმცა გარკვეულ შემთხვევებში ასეთმა დაყოფამ შეიძლება კონკრეტული ჯგუფი სტიგმატიზაციის ან დისკრიმინაციის რისკის წინაშე დააყენოს. პროგრამა „ყველა ჩვენგანი“ მიზანმიმართულად ცდილობს თავიდან აიცილოს ისეთი კვლევების ჩატარება, რომლებმაც შესაძლოა გამოიწვიოს ჯგუფების სტიგმატიზაცია ან დისკრიმინაცია. ამასთან, პროგრამა ითვალისწინებს, რომ ზოგიერთ ჯგუფს, თემს ან ქვეჯგუფს — მიუხედავად არსებული რისკებისა — შესაძლოა თავად სურდეს მონაცემთა ბაზაში იდენტიფიცირება, რათა ხელი შეუწყოს კვლევებს, რომლებიც მიზნად ისახავს ჯანდაცვის სფეროში უთანასწორობის აღმოფხვრას ან სხვაგვარი

სისტემური პრობლემების გადაჭრას. თუმცა, განსაკუთრებით იმ შემთხვევებში, როდესაც ისტორიული კონტექსტი ზრდის სტიგმატიზაციისა და დისკრიმინაციის საფრთხეს, პროგრამის ფარგლებში უნდა ჩატარდეს შესაბამის ჯგუფებთან, თემებთან და ქვეჯგუფებთან (მათ შორის ტომებთან) შეხვედრები, რათა განისაზღვროს, როგორ უნდა განხორციელდეს ჯგუფის იდენტიფიცირებადობის მართვა და რა ზომებია საჭირო ზიანის შესამცირებლად.

პროგრამა აღნიშნავს, რომ ფართო თანხმობის ("broad consent") რეალური კონცეფცია უფრო ფართოა, ვიდრე მისი ფორმალური განსაზღვრება, რომელიც ჩამოყალიბებულია 2018 წლის საერთო სტანდარტების დოკუმენტში. შესაბამისად, პროგრამა ხაზს უსვამს, რომ მონაწილეებისგან ითხოვს ფართო თანხმობას კონცეფციის შინაარსობრივი გაგებით და არა იმ სპეციფიკური სამართლებრივი განმარტების შესაბამისად, რომელიც მოცემულია აღნიშნულ დოკუმენტში."[84]

კვლევებში — განსაკუთრებით დიდი ბიო ბანკების კონტექსტში — ერთ-ერთი მნიშვნელოვანი გამოწვევაა, რომ არსებული დაცვის მექანიზმები, რომლებიც დეპერსონალიზაციას იყენებს კონფიდენციალურობის უზრუნველსაყოფად, ყოველთვის ეფექტურად ვერ მოქმედებს. გარკვეულ შემთხვევებში შესაძლებელია ჯგუფების გენეტიკური იდენტიფიცირება დეპერსონალიზებულ მონაცემთა ბაზაშიც კი. "NIH"-ის კვლევაში თავად სააგენტო აღიარებს, რომ არსებობს ბიოლოგიური მასალების უფრო ფართო, იდენტიფიცირებად ჯგუფთან დაკავშირების რისკი, და ასევე მიუთითებს, რომ არსებული დაცვის მექანიზმები ამ რისკს ვერ ანეიტრალებს. ეს ხაზგასმულია განცხადებაში: „პროგრამა აღნიშნავს, რომ მონაწილეებს სთხოვს ფართო თანხმობას მისი კონცეპტუალური გაგებით და არა 2018 წლის საერთო სტანდარტების დოკუმენტში ჩამოყალიბებული სამართლებრივი განმარტების შესაბამისად."[85] ფართო თანხმობის მოდელი კვლავაც ერთ-ერთი ყველაზე რთული საკითხია. აუცილებელია განისაზღვროს, როგორ უნდა განხორციელდეს „ფართო თანხმობა" როგორც ტომობრივი ჯგუფების, ისე სხვა ჯგუფების შემთხვევაში, სადაც კოლექტიური უფლებები, ისტორიული გამოცდილება და სოციალური კონტექსტი განსხვავებულ მოთხოვნებს აწესებს.

ამ რისკთან ერთად, დამატებით სერიოზულ გამოწვევას წარმოადგენს კოლექტიური კონფიდენციალურობის უზრუნველყოფა იმ გარემოში, სადაც ბიო ბანკის მონაცემებს მასშტაბურად ამუშავებს ხელოვნური ინტელექტი. აღნიშნული ორი ტენდენცია კიდევ უფრო ართულებს როგორც ინდივიდუალური, ისე კოლექტიური კონფიდენციალურობის დაცვის მექანიზმების რეალიზებას გარკვეული ტიპის ბიო ბანკების შემთხვევაში.

[84] All of Us Research Program Tribal Consultation Final Report March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].
[85] All of Us Research Program Tribal Consultation Final Report March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].

“NIH”-ის მიერ გამოყენებული ტერმინი “identitativity”, რომელიც მიუთითებს ბიოლოგიური მასალის გარკვეულ ჯგუფთან იდენტიფიცირებადობის რისკზე, ამ კონტექსტში განსაკუთრებით მნიშვნელოვანია, რადგან ის ეხმიანება “entitativity”-ის შესახებ არსებულ კვლევებს. ეს საკითხი განსაკუთრებით თვალსაჩინოა სტრასბურგის სასამართლოს გადაწყვეტილების ანალიზში ლევიტის საქმე, რომელიც განხილულია შემდეგ თავში.

5.4. შემთხვევის ანალიზი: ლევიტი ავსტრიის წინააღმდეგ და ადამიანის უფლებათა ევროპული სასამართლოს მიდგომა კოლექტიური ჯგუფების ინდივიდუალური წევრების მიმართ

2016 წლის ივლისში ბატონმა აბა ლევიტმა შეიტანა ინდივიდუალური საჩივარი ადამიანის უფლებათა ევროპული სასამართლოს წინაშე.[86] მომჩივანი აცხადებდა, რომ მისი პირადი ცხოვრების ხელშეუხებლობის უფლება დაირღვა მემარჯვენე იდეოლოგიასთან დაკავშირებული გამოცემის მიერ გავრცელებული პუბლიკაციის შედეგად, რომელმაც კოლექტიურად ცილი დასწამა ჰოლოკოსტს გადარჩენილთა ჯგუფს. საგულისხმოა, რომ პუბლიკაციაში სახელობითად არ იყო მოხსენიებული უშუალოდ ბატონი ლევიტი ან სხვა რომელიმე პირი. პუბლიკაცია კოლექტიურად იხსენიებდა ჰოლოკოსტს გადარჩენილ მსხვერპლებს, რომლებიც 1945 წელს გათავისუფლდნენ მაუტჰაუზენის საკონცენტრაციო ბანაკიდან და აღწერდა მათ განსაკუთრებულად დამაკნინებელი ეპითეტებით, მათ შორის, ცილს სწამებდა კრიმინალურ მოქმედებებში თანამონაწილეობაში.

წინამდებარე ინციდენტზე, ეროვნულ დონეზე წარიმართა შემდეგი პროცესი. 2016 წლის ივნისში, მაუტჰაუზენის ბანაკის ყოფილმა ტყვეებმა (პატიმრებმა), ორ სხვა პირთან ერთად (მაუტჰაუზენის საკონცენტრაციო ბანაკის გარდაცვლილი პატიმრის ქალიშვილი და ტერეზიენშტადტის საკონცენტრაციო ბანაკის ყოფილი პატიმარი) გრაცის სასამართლოში, სამოქალაქო პალატაში, შეიტანეს სარჩელი ცილისწამებაზე. იმავე წლის აგვისტოში გრაცის სასამართლომ დააკმაყოფილა მოსარჩელეების შუამდგომლობა უზრუნველყოფის ღონისძიებაზე, რაც ძალაში დარჩა საქმის როგორც სააპელაციო, ასევე საკასაციო ეტაპზე განხილვისას. 2017 წლის თებერვალში საქმე მორიგებით დასრულდა. გამომცემლობას დაეკისრა ვალდებულება გამოექვეყნებინა განცხადება პუბლიკაციაში ნახსენები ფაქტების უარყოფის თაობაზე. ვინაიდან ლევიტი აღნიშნულ საქმეში არ იყო მოსარჩელე, მორიგების პირობები მასზე არ ვრცელდებოდა.

ზემოაღნიშნული პროცესისგან დამოუკიდებლად ეროვნულ დონეზე წარიმართა დავა ზიანის ანაზღაურებაზე, რომლის ფარგლებშიც მოსარჩელეები იყვნენ პირვანდელი საქმიდან 9 პირი და ლევიტი - ისინი

[86] *Lewit v. Austria*, Application No. 4782 / 18, Judgment 10 October 2019.

ითხოვდნენ ზიანის ანაზღაურება პუბლიკაციით მიყენებული ცილისწამების გამო. ადამიანის უფლებათა ევროპულმა სასამართლომ, მოგვიანებით წინამდებარე საქმეზე გამოტანილ გადაწყვეტილებაში მომჩივანთა არგუმენტები, რომლებიც ეხებოდა მათ „იდენტიფიცირებადობის“ — ანუ კონკრეტული ჯგუფის წევრად იდენტიფიცირების პოტენციალს — შემდეგნაირად გადმოსცა:

„მომჩივნები ამტკიცებდნენ, რომ ცილისწამების საქმეებში, როდესაც ცილისწამება ეხება ადამიანთა ჯგუფს, მომჩივნების მსხვერპლის სტატუსის (სტრასბურგის სასამართლოს მიზნებისთვის) განსაზღვრისთვის გადამწყვეტია, რომ ჯგუფის თითოეული წევრი იყოს იდენტიფიცირებადი, თუნდაც უშუალოდ სახელობით არ იყოს მითითებული. ისინი მიუთითებდნენ, რომ ყველა მათგანი ნაცისტური რეჟიმის მსხვერპლი იყო და დაპატიმრებულნი იყვნენ თავიანთი წარმოშობის, რწმენის ან რელიგიის გამო. დაკავებისა და/ან საკონცენტრაციო ბანაკში გაძევების დროს ზოგიერთი მსხვერპლი იყო ბავშვი, სხვები კი — პოლიტიკური პატიმრები. მათ არ ჩაუდენიათ რაიმე კრიმინალური ქმედება არც საკონცენტრაციო ბანაკებში დატყვევებამდე და არც ბანაკებიდან გათავისუფლების შემდეგ.“[87]

მიუხედავად აღნიშნული არგუმენტებისა, 2016 წლის სექტემბერში გრაცის სასამართლომ უარი თქვა მოსარჩელეების ზიანის ანაზღაურების მოთხოვნაზე. როგორც სტრასბურგის სასამართლო ამ ფაქტის შეფასებისას აღნიშნავს, „სასამართლოსთვის გადამწყვეტი იყო შეკითხვა — შეძლებდა თუ არა საშუალო მოქალაქე კონკრეტული პირების იდენტიფიცირებას და მათ მიმართ ცილისმწამებლური განცხადებების დაკავშირებას“ (პარაგრაფი 21). ეროვნული სასამართლოს პოზიცია ეფუძნებოდა გარემოებას, რომ 1945 წელს მაუტჰაუზენის ბანაკიდან დაახლოებით 20,000 პატიმარი გაათავისუფლეს, რაც, სასამართლოს შეფასებით, ზედმეტად დიდი ჯგუფი იყო ინდივიდთა იდენტიფიცირებისათვის. სხვა სიტყვებით რომ ვთქვათ, ავსტრიის პირველი ინსტანციის სასამართლომ, ფაქტობრივად, „რიცხვობრივი ბუნდოვანების“ არგუმენტი გამოიყენა და ამ საფუძვლით უარი თქვა მოსარჩელეთა ინდივიდუალურ პროცესუალურ სტატუსზე (“standing”) — დაადგინა, რომ ცილისწამების საქმეში კოლექტიური ჯგუფის წევრებს ვერ ექნებოდათ ინდივიდუალური „მსხვერპლის“ სტატუსი.

ლევიტმა აღნიშნული გადაწყვეტილება გაასაჩივრა. საჩივარში ის მიუთითებდა, რომ გადაწყვეტილებაში მსჯელობა კოლექტიურ ჯგუფს მიკუთვნებული პირების იდენტიფიცირებაზე მცდარი იყო, რადგან იგი ფაქტობრივად იდენტიფიცირებადი იყო ცილისმწამებლურ პუბლიკაციაში. კერძოდ, განცხადების გამოქვეყნების დროისთვის 96 წლის ბატონი ლევიტი იყო მაუტჰაუზენის საკონცენტრაციო ბანაკის ერთ-ერთ უკანასკნელი ცოცხალი გადარჩენილ ტყვე (პატიმარი). შესაბამისად, ადგილობრივ საზოგადოებაში იგი ცნობილი იყო როგორც მაუტჰაუზენის საკონცენტრაციო ბანაკის

[87] Id. პარაგრაფი 19.

გადარჩენილი მსხვერპლი, ხოლო ჯგუფის მიმართ გაცხადებული ცილისმწამებლური ბრალდებები მის რეპუტაციაზე უშუალოდ აისახებოდა. ადამიანის უფლებათა ევროპულმა სასამართლომ წინამდებარე საკითხთან დაკავშირებით აღნიშნა: „კომიტეტის აზრით, ჯგუფის შესახებ უარყოფითი სტერეოტიპების დამკვიდრებამ, თუ ის აღწევს გარკვეულ ზღვარს, შესაძლოა ზიანი მიაყენოს ჯგუფის და შესაბამისად მისი წევრების თვითღირებულებას, ღირსებისა და თავდაჯერებულობის განცდას. ამდენად, ეს სტერეოტიპები აისახება ჯგუფის ინდივიდუალური წევრების პირად ცხოვრებაზე“ (იხილეთ: *Aksu v. Turkey* [GC], საჩივრები № 4149/04 და 41029/04, § 58, ECHR 2012). სასამართლო მიიჩნევს, რომ აღნიშნული ზოგადი პრინციპები ვრცელდება წინამდებარე საქმეზეც, სადაც განხილვის საგანია მაუტჰაუზენის საკონცენტრაციო ბანაკის ყოფილი პატიმრების ცილისწამება. აღნიშნული პირები, როგორც ჰოლოკოსტის გადარჩენილები, შეიძლება ჩაითვალონ (ჰეტეროგენულ) სოციალურ ჯგუფად (პარაგრაფი 46).

ევროპულმა სასამართლომ ასევე აღნიშნა, რომ იმ საქმეებში, სადაც ჯგუფები ცილისწამებისთვის ზიანის ანაზღაურებას ითხოვდნენ, „თუ ჯგუფი რაოდენობრივად ძალიან დიდია, შიდა სასამართლოები, როგორც წესი, მიიჩნევენ, რომ ჯგუფის წევრები ინდივიდუალურად არ იქნებოდნენ დაზარალებულნი. თუმცა, გარკვეულ შემთხვევებში ავსტრიის უზენაესმა სასამართლომ დაადგინა, რომ დიდი ჯგუფების შემთხვევაშიც შესაძლებელია, ჯგუფზე განხორციელებულმა ქმედებებმა მის ინდივიდუალურ წევრებსაც მიაყენოს ზიანი“ (საილუსტრაციოდ იხილეთ 1978 წლის 11 იანვრის გადაწყვეტილება საჩივარზე № 10 OS 196/77 და 2011 წლის 29 ივნისის გადაწყვეტილება საჩივარზე № 15 OS 15q/10k.) (პარაგრაფი 36).

საბოლოოდ, სტრასბურგის სასამართლომ გაიზიარა მომჩივნის - ბატონო ლევიტის პოზიცია და დაადგინა, რომ ავსტრიამ დაარღვია ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლი („პირადი და ოჯახური ცხოვრების დაცულობის უფლება“). სასამართლომ დაადგინა, რომ ავსტრიის ეროვნულმა სასამართლოებმა დაუსაბუთებლად შეწყვიტეს სამართალწარმოება მაუტჰაუზენის საკონცენტრაციო ბანაკს გადარჩენილთა სარჩელებზე და შესაბამისი გადაწყვეტილებები არსებითად იყო ხარვეზიანი, როგორც ფაქტობრივი გარემოებების შეფასების, ისე სამართლებრივი დასაბუთების თვალსაზრისით. სტრასბურგის სასამართლოს დასკვნით, ეროვნულ სასამართლოებს ევალებოდათ სათანადოდ განესაზღვრათ, მაუტჰაუზენის საკონცენტრაციო ბანაკის რამდენი ყოფილი პატიმარი იყო ცოცხალი 2016 წელს და რამდენად იყო შესაძლებელი მათი ინდივიდუალური იდენტიფიცირება განსახილველი ცილისმწამებლური განცხადებების კონტექსტში.

სტრასბურგის სასამართლოს წინამდებარე გადაწყვეტილება დღეს აქტიურად გამოიყენება ავსტრიაში მოსამართლეების გადამზადების პროცესში, რათა გაიზარდოს სენსიტიურობა ქვეყნის ისტორიულ წარსულთან დაკავშირებული საკითხების მიმართ. აღსანიშნავია, რომ ბატონი ლევიტი,

რომელიც იყო ერთ-ერთი ყველაზე ხანგრძლივი სამართლებრივი ბრძოლის მონაწილე, 2020 წლის ნოემბერში, 97 წლის ასაკში გარდაიცვალა. მან მოასწრო საკუთარი საქმის წარმატებული დასრულება.

აღნიშნული შემთხვევის ანალიზი ხაზს უსვამს რამდენიმე მნიშვნელოვან საკითხს კოლექტიური კონფიდენციალურობის ჭრილში. საგულისხმოა, რომ კოლექტიურ ჯგუფს — ამ შემთხვევაში საკონცენტრაციო ბანაკს გადარჩენილ ტყვეებს — პირადი ხელშეუხებლობის უფლების რეალიზებისთვის დასჭირდათ დაემტკიცებინათ, რომ შესაძლებელი იყო მათი ინდივიდუალური იდენტიფიცირება ჯგუფში და რომ მათ ინდივიდუალურად მიადგათ ზიანი. ეს ხაზგასმული იყო საქმის მსვლელობის ყველა ეტაპზე: სწორედ ინდივიდუალური იდენტიფიცირების დამტკიცებამ მისცა ლევიტს შესაძლებლობა, წარმატებით ებრძოლა სახელმწიფოს წინააღმდეგ.

ლევიტის საქმე კიდევ უფრო ამძაფრებს კითხვას, რომელიც ამ ნაშრომში უკვე დასმულ იქნა ბიომედიცინის კონტექსტში შემთხვევის ანალიზის დროს: რა არის ინდივიდის ხელახალი იდენტიფიცირების რისკი კონკრეტულ ჯგუფთან კავშირში? როგორ იცვლება ეს რისკი ჯგუფის “entitativity”-ის ხარისხის მიხედვით ე.ი. რამდენად აღიქმება ჯგუფი, როგორც ერთიანი კოლექტიური სუბიექტი? არსებობს თუ არა ფაქტორები, რომლებიც ზრდის ან ამცირებს ამ რისკს? ნაშრომის ჰიპოთეზა ასეთია: თუ არსებობს მაღალი “entitativity”-ის მქონე, მკაფიოდ განსაზღვრული ჯგუფი, რომლის მიმართაც ისტორიულად ფიქსირდება სტიგმა ან დისკრიმინაცია, მაშინ ასეთი ჯგუფის ფარგლებში იდენტიფიცირება თავისთავად შეიძლება წარმოადგენდეს რისკს. აღნიშნული ჰიპოთეზა აჩენს რიგ დამატებით კითხვებს.

მიუხედავად იმისა, რომ მაუტჰაუზენის საკონცენტრაციო ბანაკიდან გათავისუფლებული პირების საერთო რაოდენობა დაახლოებით 20,000-ს შეადგენდა, შესაძლებელი იყო ჯგუფის გარკვეულ წევრთა იდენტიფიცირება და რისკები, როგორც არის — ბანაკთან კავშირის გამო სტიგმის რისკი. დიდი ჯგუფის ფარგლებში „დამალვა“ ყოველთვის არ უზრუნველყოფს კონფიდენციალურობის დაცვას - ეს ნათელია როგორც მაგალითად საკონცენტრაციო ბანაკს გადარჩენილი პირების შემთხვევაში, ასევე თანამედროვე, ციფრულ სამყაროში. ჩნდება შეკითხვა: როდის უნდა ემყარებოდეს კონფიდენციალურობის დაცვა კოლექტიურ საფუძველს? მხოლოდ მაშინ, როდესაც ჯგუფი მცირეა? მხოლოდ მაშინ, როდესაც შესაძლებელია მისი წევრების იდენტიფიცირება?

“NIH”-ის ანგარიშში “entitativity” განხილულია, როგორც პოტენციური სტიგმის განმსაზღვრელი კრიტერიუმი. თუ ამ მიდგომას ჰიპოთეზად ავიღებთ, მაშინ კონფიდენციალურობის დარღვევის რეალური რისკი არ განისაზღვრება ჯგუფის ზომით, არამედ ინდივიდის კონტექსტუალური კავშირით ჯგუფთან. შესაბამისად, “entitativity” შეიძლება არსებობდეს როგორც მცირე, ისე დიდი მოცულობის ჯგუფებში. ერთი რამ ცხადია: ბატონ ლევიტს, საკუთარი უფლებების დასაცავად, მოუწია დაემტკიცებინა კავშირი ჯგუფთან, რომლის

წევრთა რაოდენობა იმდენად შემცირებული იყო, რომ მისი იდენტიფიცირება შესაძლებელი ხდებოდა მაღალი „რიცხოვნული იშვიათობის“ პირობებში.

მიუხედავად იმისა, რომ ლევიტის საქმეზე კონკრეტული ფაქტობრივი გარემოებებიდან გამომდინარე მართებული გადაწყვეტილება მიიღეს, საქმე ასევე წარმოაჩენს პირადი ცხოვრების ხელშეუხებლობის დაცვის მნიშვნელოვან სისტემურ ხარვეზს. თანამედროვე ციფრულ გარემოში, ჯგუფის რაოდენობრივად მცირე მოცულობა ან მასთან დაკავშირებული ინფორმაციის სიმწირე არ უნდა იყოს კონფიდენციალურობის დაცვის განმსაზღვრელი კრიტერიუმი, რადგან მონაცემთა დამუშავების თანამედროვე ტექნოლოგიები და მასშტაბური ანალიზის მეთოდები შეუძლებელს ხდიან ინდივიდის სწრაფ და მასობრივ იდენტიფიცირებას — მაშინაც კი, როდესაც ჯგუფი დიდი ზომისაა. ამდენად, სტიგმისა და პოტენციური ზიანის რისკი შესაძლოა არსებობდეს დიდი, მრავალრიცხოვანი ჯგუფების შემთხვევაშიც. მაგალითად, მაუტჰაუზენის საკონცენტრაციო ბანაკს გადარჩენილთა ფართო ჯგუფის შემთხვევაშიც შესაძლებელი იყო კონკრეტული ინდივიდების იდენტიფიცირება და მათი სტიგმატიზირება, მიუხედავად ჯგუფის რაოდენობრივი მოცულობისა.

რაც შეეხება “entitativity”-ის, ნაშრომში განხილულ ორ სხვა მაგალითში ჯგუფებს მაღალი “entitativity” ახასიათებდათ ეთნიკური და ტომობრივი კავშირების საფუძველზე. ბატონი ლევიტის საქმეში კი ჯგუფის “entitativity” განპირობებული იყო მათი საერთო ისტორიული გამოცდილებით: მაუტჰაუზენის საკონცენტრაციო ბანაკში დატყვევებით,[88] გათავისუფლებითა და შემდგომ ხანგრძლივი ურთიერთობით — როგორც საერთო ტრავმის მატარებელი პირები. კვლევები მიუთითებს, რომ “entitativity” შეიძლება ჩამოყალიბდეს სხვადასხვა საფუძველზე და ჯგუფები ერთიანი კოლექტიური სუბიექტურობის ხარისხს განსხვავებული გზებით აღწევენ. მაუტჰაუზენის ბანაკში იმყოფებოდნენ სხვადასხვა ეთნიკური წარმოშობის პირები, მათ შორის რომა წარმოშობის ადამიანები და სხვა ჯგუფები,[89] რაც მიუთითებს, რომ ჯგუფის “entitativity” მხოლოდ ეთნიკური ჰომოგენობით არ განისაზღვრებოდა. შესაბამისად, მისი ძირითადი წყარო შესაძლოა ყოფილიყო ჯგუფის უნიკალური ისტორიული გამოცდილება და მისი განსაკუთრებული მნიშვნელობა. მიუხედავად ამისა, გადარჩენილთა უშუალო გამოკითხვის გარეშე რთულია საბოლოოდ დადგენა, კიდევ რა დამატებით ფაქტორებს შეიძლებოდა ხელი შეეწყო ამ ჯგუფის “entitativity”-ის გაძლიერებისთვის.

2016 წლისთვის, როდესაც საკონცენტრაციო ბანაკს გადარჩენილთაგან მხოლოდ მცირე ნაწილი იყო ცოცხალი, გაჩნდა კითხვა, როგორ შეიცვალა ამ ჯგუფის “entitativity” დროთა განმავლობაში. კონკრეტულად, როგორ იმოქმედა ჯგუფის რაოდენობრივმა შემცირებამ და ინფორმაციის სიმწირემ მის

[88] *76 yearslater, we remember Simon Wiesenthal's liberation from Mauthausen*, Simon Wiesenthal Center, 6 May 2021, <https://www.wiesenthal.com/about/news/76-years-later-we-remember.html> [12.11.2025].
[89] Mauthausen Concentration Camp, Wikipedia, <https://en.wikipedia.org/wiki/Mauthausen_concentration_camp> [12.11.2025].

"entitativity"-ზე? შესაძლებელი იყო თუ არა, რომ საერთო ტრავმული და ისტორიულად მნიშვნელოვანი გამოცდილება კვლავაც დარჩენილიყო ჯგუფის "entitativity"-ის ძირითად საფუძვლად?

5. დასკვნა

დღესდღეობით, კოლექტიური კონფიდენციალურობის დაცვის ყველაზე ძლიერი მექანიზმები მოქმედებს ტომობრივი და ადგილობრივი თემებისთვის, რომელთაც აქვთ უფლებები "UNDRIP"-ის საფუძველზე, ხოლო დამატებითი უფლებები შესაძლებელია განისაზღვროს სპეციალური კანონმდებლობით, ხელშეკრულებებითა და სხვა შეთანხმებებით. საილუსტრაციოდ, როგორც მოცემულ ანალიზშია განხილული, მაორის ხალხს კოლექტიური კონფიდენციალურობის ფორმალურად აღიარებული უფლებები გააჩნია ახალი ზელანდიის მთავრობასთან დადებული ხელშეკრულების საფუძველზე. ასევე, "NIH"-ის კვლევამ, სახელწოდებით: „ყველა ჩვენგანი" ("All of Us") განსაკუთრებულად გამოკვეთა, რომ თუნდაც კონკრეტული ინდივიდი ფორმალურად არ იყოს იდენტიფიცირებადი ჯგუფში, თუ მისი დაკავშირება შესაძლებელია მაღალი "entitativity"-ის მქონე ჯგუფთან, მას შეიძლება დაემუქროს სტიგმატიზაციის ან „ასოციაციური დისკრიმინაციის" საფრთხე.

დღესდღეობით უმეტეს ქვეყანაში დანერგილია პირადი ცხოვრების ხელშეუხებლობის ისეთი სამართლებრივი ჩარჩო, სადაც ყურადღების ცენტრში ინდივიდუალური უფლებების დაცვაa. ამ მოდელის პირობებში კონფიდენციალურობა აღიქმება როგორც ინდივიდზე ორიენტირებული სამართლებრივი უფლება და არა როგორც კოლექტიური სუბიექტის მოთხოვნა. "NIH"-ის ანგარიშიც სწორედ ამას უსვამს ხაზს, როდესაც აღნიშნავს, რომ „იდენტიფიცირების განხილვა ინდივიდუალურ დონეზე არ ითვალისწინებს ჯგუფის იდენტიფიცირებადობის საკითხს". ლევიტის საქმეზე ადამიანის უფლებათა ევროპულმა სასამართლომ გადაწყვეტილება მომჩივნის სასარგებლოდ მიიღო, რადგან მან შეძლო ჯგუფში ინდივიდუალური იდენტიფიცირებადობის დამტკიცება და შესაბამისად კონვენციის ფარგლებში გათვალისწინებული დაცვის გავრცელება საკუთარ მდგომარეობაზე. იმავე დროს, მაუტჰაუზენის საკონცენტრაციო ბანაკის გადარჩენილთა ჯგუფი იმ პერიოდში სამართლებრივად არ იყო აღიარებული, როგორც კოლექტიური სუბიექტი, რომელსაც კონფიდენციალურობის დამოუკიდებელი, ჯგუფზე დაფუძნებული დაცვა ექნებოდა. სტრასბურგის სასამართლომ მიიღო ლევიტის სასარგებლოდ და გადაწყვეტილებაში იმსჯელა იმ დაძაბულობაზე, რომელიც არსებობს ინდივიდუალური კონფიდენციალურობის უფლებასა და იმ გარემოებას შორის, რომ ზოგიერთ შემთხვევაში ჯგუფის კონფიდენციალურობის დარღვევა შეიძლება ინდივიდზეც აისახოს.

ტრადიციულად, პერსონალური მონაცემების დაცვის ნორმატიული ჩარჩოები ინდივიდზე იყო ორიენტირებული, რაც ხანგრძლივი დროის

განმავლობაში ფუნქციონალურ და ეფექტიან მიდგომად ითვლებოდა. თუმცა, თანამედროვე ციფრულ გარემოში, სადაც ადამიანებისა და ჯგუფების შესახებ არსებული დიდი მოცულობის მონაცემები ურთიერთქმედებს ხელოვნურ ინტელექტთან და მანქანურ სწავლებასთან, ტექნოლოგიებს უკვე შეუძლიათ ჯგუფების ავტომატური ფორმირება, მათზე დასკვნების გამოტანა და ამ დასკვნების გამოყენება სწრაფად და მასშტაბურად. ხელოვნური ინტელექტი სულ უფრო მნიშვნელოვანი ნაწილი ხდება ყოველდღიური სოციალური და ტექნოლოგიური პროცესების; შესაბამისად, საჭიროა დავფიქრდეთ, კონფიდენციალურობის დაცვის რა ტიპის მექანიზმები შეიძლება დასჭირდეს ჯგუფებს, რა პირობებში უნდა ამოქმედდეს ეს დაცვა და რა სამართლებრივი ფორმით უნდა უზრუნველყოფდეს სისტემა კოლექტიური ინტერესების დაცვას.

კოლექტიური კონფიდენციალურობის განხილვისას ჩნდება რამდენიმე მნიშვნელოვანი კითხვა. ერთ-ერთი ძირითადი არის: როგორ შეიძლება განისაზღვროს, რომ კონკრეტულ ჯგუფს აქვს კოლექტიური კონფიდენციალურობის დაცვის აუცილებლობა? “entitativity”-ის კონცეფცია აქ მნიშვნელოვანია, თუმცა საჭიროა დამატებითი კვლევა იმის გასარკვევად, თუ რა წარმოადგენს „ჯგუფის იდენტობას“ (“group identitativity”) და როგორ შეიძლება მისი შეფასება. აღნიშნული ტერმინი ფართოდ დამკვიდრებული არ არის, თუმცა როგორც “NIH”-ის კვლევა და “Lewit”-ის საქმე მიუთითებს, „ჯგუფის იდენტობის“ (“group identitativity”) საკითხი კვლევის დამოუკიდებელ საგნად უნდა იქცეს.

საკვანძო შეკითხვებია: როდის ხდება ჯგუფში წევრობა, ან მასთან იდენტიფიცირება, საკმარისად მნიშვნელოვანი იმისათვის, რომ კონფიდენციალურობის დაცვა ჯგუფურ დონეზეც გახდეს საჭირო? რომელი კონკრეტული კონტექსტი წარმოშობს კოლექტიური კონფიდენციალურობის მოთხოვნას და რა შემთხვევებში უნდა მიენიჭოს კოლექტიურ უფლებებს პრიორიტეტი? ამ დისკუსიაში აუცილებელია მრავალდარგობრივი ჩართულობა — მათ შორის ეთნიკური და ადგილობრივი თემების, ტექნიკური სპეციალისტების, იურისტებისა და აკადემიკოსების, მონაცემთა დაცვის სფეროს პროფესიონალების, პოლიტიკის შემმუშავებლების, ადამიანის უფლებების სფეროს წარმომადგენლებისა და სხვა დაინტერესებული მხარეების ჩართვა.

ჯგუფური კონფიდენციალურობის გამოწვევების დასარეგულირებლად შესაფერისი მოდელების ძიებისას განსაკუთრებულ მნიშვნელობას იძენს ადგილობრივი (ძირძველი) ხალხების ისტორიული გამოცდილება. ეს გამოცდილება ეფუძნება საუკუნეების განმავლობაში ჩამოყალიბებულ მმართველობით ფილოსოფიასა და ინსტიტუციურ ჩარჩოებს, რომელთა საფუძველიც კოლექტიური კონფიდენციალურობის პრინციპებია. შეიძლება ითქვას, რომ ისინი დღეს არსებულ ყველაზე მნიშვნელოვან — ან, სულ მცირე, სახელმძღვანელო — მოდელებს წარმოადგენენ. ახალი ზელანდიის მაორის მაგალითი განსაკუთრებით მნიშვნელოვანია ამ ჭრილში: იგი ეფუძნება

პატივისცემაზე აგებულ და პრაქტიკულად განხორციელებად მიდგომებს. ახალზელანდიასა და მაორის შორის დადებული ხელშეკრულება მოიცავს მკაფიო სამართლებრივ ენას, რომლის ანალიზიც კოლექტიური კონფიდენციალურობის კონტექსტში განსაკუთრებით მნიშვნელოვანია.

ბიო ბანკების კონტექსტი ასევე ერთ-ერთ ყველაზე მნიშვნელოვან გამოწვევას წარმოადგენს. ბიომედიცინური ანალიზის შესაძლებლობების ზრდასთან ერთად, აუცილებელია დავსვათ კითხვა: რა სახის დაცვის მექანიზმები იქნება საჭირო ჯგუფური კონფიდენციალურობის უზრუნველსაყოფად? ტომობრივი ჯგუფების შემთხვევაში უკვე დადასტურდა, რომ ფართო თანხმობის (“broad consent”) მოდელი კოლექტიური უფლებების დაცვის თვალსაზრისით ხარვეზიანია. აღნიშნული სხვა შეკითხვებს წარმოშობს: არსებობს თუ არა სხვა ჯგუფები, რომლებიც მსგავსი რისკის წინაშე დგანას? და თუ ასეთი გამოწვევები რეალურად არსებობს, შესაძლებელია თუ არა მათი რაოდენობრივად შეფასება და სისტემური აღწერა ისე, რომ საფუძველი შეიქმნას შესაბამისი პოლიტიკის, სამართლებრივი ჩარჩოებისა და დაცვის მექანიზმების შემუშავებისთვის?

კოლექტიური კონფიდენციალურობის შესახებ ჯერ არსებულ გამოცდილებაზე დაყრდნობით შეიძლება გაკეთდეს მრავალი დასკვნა: ბიო ბანკებში ადამიანის კვლევების ეთიკა; AI-ის მიერ გამოწვეული სოციალური და ტექნიკური რისკები; მონაცემების მმართველობის მოდელები; ტომობრივი სამართლებრივი პრაქტიკა სტრატეგიული დასაწყისის წერტილად შეგვიძლია გამოვიყენოთ ადგილობრივი ხალების გამოცდილება, რომელიც წარმოადგენს კოლექტიური უფლებების სამართლებრივ წყაროს.

კოლექტიური კონფიდენციალურობის შესახებ უკვე არსებული გამოცდილება არაერთი მნიშვნელოვანი დასკვნის გამოტანის საშუალებას გვაძლევს. შესაბამისი გაკვეთილები შეიძლება მივიღოთ როგორც ხელოვნური ინტელექტის სფეროში არსებული სოციალური და ტექნიკური გამომწვევებიდან და მათ გადაჭრის გზებიდან, ისე ადამიანის კვლევის გარკვეული მიმართულებებიდან, განსაკუთრებით ბიო ბანკების შემთხვევაში. ამასთანავე, კოლექტიური კონფიდენციალურობის უკვე არსებული პოლიტიკის მაგალითები, მათ შორის ადგილობრივი ხალხების სამართლებრივი პრაქტიკები, შეიძლება წარმოადგენდეს მნიშვნელოვან საწყის წერტილს მომავალში რეგულირების ჩარჩოს გასავითარებლად.

კოლექტიური კონფიდენციალურობის საკითხი საჭიროებს სიღრმისეულ კვლევასა და შესაბამისი პოლიტიკის განვითარებას, მათ შორის ჯგუფური იდენტიფიცირებადობის რისკების შეფასებას ხელოვნური ინტელექტის პირობებში, შესაბამისი დაცვის მექანიზმების შემუშავებას და ადგილობრივი ხალხების არსებული პრაქტიკების ინტეგრირებას თანამედროვე სამართლებრივ ჩარჩოებში. ამ პროცესზე უარის თქმა ნიშნავს ტექნოლოგიური და ფილოსოფიური გარდატეხის უგულებელყოფას, რომელიც ჩვენს ეპოქაში უკვე მიმდინარეობს. შესაბამისად, კოლექტიური კონფიდენციალურობის რისკების პრევენცია და ამ რისკებზე რეაგირების მექანიზმების შექმნა

წარმოადგენს არსებით გამოწვევას, რომლის სათანადო მართვა თანამედროვე მონაცემთა დაცვის სისტემების განვითარებისთვის კრიტიკულად მნიშვნელოვანია.

ბიბლიოგრაფია:

1. Declaration on the Rights of Indigenous Peoples, United Nations, (adopted 2 October 2007 UNGA Res 61/295).
2. Directive 95/46/EC, 1995 O.J. (L 281) 31 and the EU General Data Protection Regulation.
3. *Ahuriri-Driscoll A.,* Enacting Kaitiakitanga: Challenges and Complexities in the Governance, 2014.
4. *Callison C.,* Material Culture in Flux: Law and Policy of Repatriation of Cultural Property, University of British Columbia Law Review, Special Issue, 1995, 165-181.
5. *Campbell D. T.,* Common Fate, Similarity and other Indices of the Status of Aggregates of Persons as Social Entities, Behavioral Science, 1958, <https://doi.org/10.1002%2Fbs.3830030103> [12.11.2025].
6. *Coll T., Taylor J. (eds.),* Indigenous Data Sovereignty: Toward an Agenda, 2016.
7. Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), *Feasibility Study*, 17/12/2020, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> [12.11.2025].
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, 5/12/2024, <https://rm.coe.int/1680afae3c> [12.11.2025].
9. Council of Europe, Overview of the Council of Europe Activities in the Field of Artificial Intelligence, <https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6> [12.11.2025].
10. Co-designing Māori Data Governance, (Stats NZ) Data.gov.nz, Fata toolkit, <https://data.govt.nz/toolkit/data-governance/maori/> [12.11.2025].
11. *Dixon P., Milanes V., et al.* The Twin Transition from a Global Perspective: Framing the Debate. Presentation of Preliminary Research regarding the Twin Transition - Summary Report from a Series of Global Roundtables. OECD Ministerial Meeting, Gran Canaria Span. World Privacy Forum and ADC tor los Derechos Civiles. 13/12/2022, <https://www.worldprivacyforum.org/wp-content/uploads/2022/12/Twin_Transition_Report1_WPF_ADC_13December2022_fs.pdf> [12.11.2025].
12. *Erueti A.,* The UN Declaration on the Rights on Indigenous Peoples: A New Interpretive Approach, Oxford University Press, 2022.
13. *Gonzalez C. G.,* Environmental Justice, Human Rights and the Global South, 13 Santa Clara Journal of International Law 151, 2015.

14. *Helfer L. R., Austin G. W.,* Human Rights and Intellectual Property: Mapping the Global Interface, Cambridge University Press, 2011, rev. 2017.
15. *Karjala D. S.,* Robert Kirkwood Paterson, Looking beyond Intellectual Property in Resolving Protection of Intangible Cultural Heritage of Indigenous Peoples, Cardozo Journal of International and Comparative Law, Vol. 11, 2003, 633.
16. *Kukutai T., Campbell-Kamariera K., Mead A., Mikaere K., Moses C., Whitehead J., Cormack D.,* Māori Data Governance Model Te Kāhui Raraunga, <https://tengira.waikato.ac.nz/__data/assets/pdf_file/0008/973763/Maori_Data_Governance_Model.pdf> [12.11.2025].
17. Maori Sovereignty Network, Te Mana Raraunga, Māori Data Audit Tool, <https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/59152b7db8a79bdb0e64424a/1494559615337/Māori+Data+Audit+Tool.pdf> [12.11.2025].
18. Mãori Data Sovereignty Network, Te Mana Raraunga, the <https://www.temanararaunga.maori.nz> [12.11.2025].
19. *Mercredi O.,* Aboriginal Languages Celebrated, Saskatchewan Indian, Vol. 22, no. 4, 1993, 8.
20. Model Development Lifecycle (MDL) Item 22, 13, <https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/mdl-governance-guide-for-effective-operational-algorithm-decision-making.pdf> [12.11.2025].
21. *Ouden D. A. E., O'Brien J. M.,* Recognition, Sovereignty Struggles, and Indigenous Rights in the United States: A Sourcebook, University of North Carolina Press, 2013.
22. *Phillips J.,* Australia's Heritage Protection Act: An Alternative to Copyright in the Struggle to Protect Communal Interests in Authored Works of Folklore, Pacific Rim and Policy Journal, Vol. 18 no. 3, 2009, 547-573.
23. Presentation of Jong-Sung Hwang, President, National Information Society Agency on Korea's Digital Bill of Rights and Evolution of Digital Inclusion and Presentation by Tahu Kukutai, Māori Data Governance Model, Data for Self Determination, at OECD event: Presentation of Charter on the Values and Principles for a Digital Shared Prosperity Society: Digital Bill of Rights, The Government of the Republic of Korea, 2023.
24. Remarks of Terina Fa'agau Devin Kamealoha Forrest, Presentation for Privacy tutorial hosted by World Privacy Forum and WACV Conference: AI Governance and data protection: Problem solving for Computer Vision and more, WACV conference, Hawaii, 8/01/2024.
25. *Skogstad L.,* Whose Artificial Intelligence? Design Assembly, <https://designassembly.org.nz/2023/05/08/whose-artificial-intelligence-reflecting-on-the-intersection-of-ai-and-te-ao-maori/> [12.11.2025].

26. The Government of New Zealand, Te Ao Māori Framework , Te Anga Ao Māori, <https://www.hqsc.govt.nz/assets/Misc/Te_Ao_Maori_Framework_FINAL.pdf> [12.11.2025].
27. The Government of New Zealand, Te Ao Māori Framework Implementation Guide, <https://www.hqsc.govt.nz/assets/Misc/Implementation_guide_Te_Ao_Maori_Framework_FINAL.pdf> [12.11.2025].
28. The First Nations Principles of OCAP, First Nations Information Governance Centre, <https://fnigc.ca/ocap-training/> [12.11.2025].
29. *Tsosie,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019)
30. U.S. Indigenous Data Sovereignty Network, <https://usindigenousdatanetwork.org/resources/> [12.11.2025].
31. Visit to Costa Rica – Report of the Special Rapporteur on the rights of indigenous peoples, A/HRC/51/28/ Add.1, United Nations. Human Right Council Fifty-first session, 12 Sept - 7 October 2022, <https://www.ohchr.org/en/documents/country-reports/ahrc5128add1-visit-costa-rica-report-special-rapporteur-rights-indigenous> [12.11.2025].
32. *Walter M., Kukutai T.,* Indigenous Data Sovereignty and Policy, Routledge: London, 2020.