პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

N 1-2,2025

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

№1-2, 2025

მთავარი რედაქტორი:

ასოც. პროფ. დოქტ. დოქტ. ლელა ჯანაშვილი
(თსუ; ბარსელონის ავტონომიური უნივერსიტეტი)

სარედაქციო კოლეგია:

პროფ. დოქტ. გიორგი ხუბუა (თსუ)
პროფ. დოქტ. პაატა ტურავა (თსუ)
დოქტ. ოთარ ჩახუნაშვილი (თსუ)
პროფ. დოქტ. ნორბერტ ბერნსდორფი (მარბურგის ფილიპეს სახელობის უნივერსიტეტი)
პროფ. დოქტ. როსერ მარტინეს (ბარსელონის ავტონომიური უნივერსიტეტი)
პროფ. დოქტ. ხოსე ხულიო ფერნანდეს როდრიგეს (სანტიაგო-დე-კომპოსტელას უნივერსიტეტი)
დოქტ. ენდრე გიოზო სზაბო (ევროსტატის იურიდიული და პოლიტიკის ოფიცერი, მონაცემთა დაცვის კოორდინატორი)

აღმასრულებელი რედაქტორი:

ანა თოხაძე (ასისტენტი, თსუ)

ტექნიკური რედაქტორები:

ნინო ხუბულია (დოქტორანტი, თსუ)
ირაკლი ლეონიძე (დოქტორანტი, თსუ)

თარჯიმანი:

თეო კვატაშიძე

© პერსონალურ მონაცემთა დაცვის სამსახური, 2025

P-ISSN 2720-8753

E-ISSN 2720-8761

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის მეხუთე და მეექვსე ნომრების გაერთიანებული გამოცემა ეძღვნება პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების 33-ე ევროპულ საგაზაფხულო კონფერენციას ("European Conference of Data Protection Authorities – Spring Conference") და „ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის" რიგით 75-ე შეხვედრას (ე.წ. „ბერლინის სამუშაო ჯგუფს", "IWGDPT")

სარჩევი

ლელა ჯანაშვილი
მთავარი რედაქტორისაგან **..... 3**

შერონ აზარია
სახის ამომცნობი ტექნოლოგია: პირადი ცხოვრების ხელშეუხებლობის უფლებები და საკანონმდებლო გამოწვევები **..... 8**

შერონ აზარია
მონაცემთა დაცვა და კონფიდენციალობა ჭკვიან ქალაქებში: ტექნოლოგიების სფეროში მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის დოკუმენტის კრიტიკული ანალიზი **..... 15**

ნორბერტ ბერნსდორფი
პერსონალურ მონაცემთა დაცვის ისტორიული ფესვები - როგორ გაჩნდა ის! **22**

ნორბერტ ბერნსდორფი
საქართველოში პერსონალურ მონაცემთა დაცვის არსებული მდგომარეობა — 2024 წლის კომუნიკაცია ევროკავშირის გაფართოების პოლიტიკის შესახებ **.. 33**

მაქსიმ გენარტი
პირადი ცხოვრების ხელშეუხებლობა, ეთიკა და თანამშრომლობა: პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების როლი ხელოვნური ინტელექტის განვითარებაში **..... 44**

აგნიესკა გრზელაკი
მონაცემთა მინიმიზაციისა და მოდელის მაქსიმიზაციის თავსებადობა: მარეგულირებელი და ეთიკური წინააღმდეგობები ხელოვნური ინტელექტის განვითარებაში **..... 53**

კობა გრიალაშვილი
პერსონალური მონაცემების დაცვა სამართალდამცავი ორგანოების საქმიანობაში **..... 71**

პამ დიქსონი
ჯგუფის პირადი ცხოვრების ხელშეუხებლობა, მონაცემები და ხელოვნური ინტელექტი: პირადი ცხოვრების ხელშეუხებლობის კოლექტიური ფორმები და მისი კავშირი ტექნოლოგიასა და საკანონმდებლო ჩარჩოებთან **..... 87**

ჯუზეპე დ'აკვისტო, ლუდოვიკა დე ბენედეტი
კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვის ჩარჩო მონაცემთა სანდო გაზიარების მიზნით **..... 128**

დევიდ ვაინკაუფი
სამუშაო დოკუმენტი დიდი ენობრივი მოდელების (“LLMs”) შესახებ..... **156**

პეტრუ ემანუელ ზლატესკუ
საერთაშორისო თანამშრომლობის რჩეული ასპექტები შვეიცარიის მონაცემთა დაცვის ახალი ფედერალური აქტის მიხედვით **183**

რეიჩელ მასტერტონი
საერთაშორისო თანამშრომლობა: შესაძლებლობების გაფართოება და გავლენის გაძლიერება **196**

ჯოვანი მარია რიჩიო
ბრიუსელის ეფექტი, პერსონალურ მონაცემთა დაცვა და ხელოვნური ინტელექტის შესახებ აქტი..... **213**

ენდრე გიოზო სზაბო
მონაცემთა დაცვის საზედამხედველო ორგანოდან მონაცემთა დამუშავებისთვის პასუხისმგებელ პირამდე — გამოცდილება ევროსტატის ფარგლებში..... **238**

იულია სზიკლეი
ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცე (“EHDS”) **247**

თამარ სამნიაშვილი
მონაცემთა სუბიექტის თანხმობა, როგორც სამართლებრივი საფუძველი: თეორიული და პრაქტიკული ასპექტები..... **255**

ჯინევრა სერინა ფერონი
ხელოვნური ინტელექტის მართვა მონაცემთა დაცვის მეშვეობით: დამოუკიდებელი უწყებების სტრატეგიული როლი ალგორითმული ძალაუფლების ეპოქაში..... **274**

ოთარ ჩახუნაშვილი, სალომე სიგუა
ხელოვნური ინტელექტისა და პერსონალურ მონაცემთა დაცვის რეგულირების სამართლებრივი ასპექტები: ეროვნული და საერთაშორისო პრაქტიკის მიმოხილვა..... **284**

გიორგი ხორბალაძე
ფიზიკური პირის მიერ მონაცემთა სუბიექტის პერსონალური მონაცემების გამჟღავნების გზით დამუშავება სოციალურ ქსელებში..... **313**

მთავარი რედაქტორისაგან

ძვირფასო მკითხველო,

წარმოგიდგენთ „პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ მიმდინაწე წლის პირველ და მეორე გაერთიანებულ გამოცემას, რომელიც ეძღვნება პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების 33-ე ევროპულ საგაზაფხულო კონფერენციას (“European Conference of Data Protection Authorities – Spring Conference”) და „ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის“ რიგით 75-ე შეხვედრას (ე.წ. „ბერლინის სამუშაო ჯგუფს“, ‘’IWGDPT“). აღსანიშნავია, რომ მიმდინარე წელს პერსონალურ მონაცემთა დაცვის სამსახური ორივე საერთაშორისო ღონისძიების მასპინძელი უწყება გახლდათ.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების 33-ე ევროპულ საგაზაფხულო კონფერენციას — პერსონალურ მონაცემთა დაცვის სფეროში უმაღლესი დონის საერთაშორისო ღონისძიებას პერსონალურ მონაცემთა დაცვის სამსახურმა ქალაქ ბათუმში უმასპინძლა. „საგაზაფხულო კონფერენცია“ 1991 წლიდან იმართება და იგი მნიშვნელოვან როლს ასრულებს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის ახალი ტენდენციების განვითარებაში. ღონისძიების მთავარი მიზანია დიალოგი ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოებსა და დარგის პრაქტიკოსებს შორის, რაც ქმნის ძლიერ ფორუმს მონაცემთა დაცვის სფეროში არსებული გამოწვევებისა და შესაძლებლობების განსახილველად. კონფერენცია საუკეთესო პლატფორმაა პერსონალურ მონაცემთა დაცვის ევროპული სტანდარტების განსახილველად და საუკეთესო პრაქტიკის გასაზიარებლად.

პერსონალურ მონაცემთა დაცვის სამართალი სამართლის შედარებით ახალ დარგს წარმოადგენს, თუმცა პირადი სივრცის, პირადი ცხოვრების დაცვას საუკუნეების ისტორია აქვს. ილია ჭავჭავაძის სიტყვები – „ადამიანის უდიდესი საუნჯე მისი ვინაობაა“ – კონფერენციის მთავარი სლოგანი, ასახავს ჩვენს ღირებულებებს პიროვნების იდენტობისა და პირადი სივრცის მიმართ. სამი დღის განმავლობაში ჩვენ გვქონდა შესაძლებლობა ევროპელ კოლეგებთან ერთად გვესაუბრა პერსონალურ მონაცემთა დაცვის სფეროს ისეთ მნიშვნელოვან საკითხებზე, როგორებიცაა: რეგიონალურ, ევროპულ და გლობალურ დონეზე ხელოვნური ინტელექტის რეგულირება და მონაცემთა დაცვის საკანონმდებლო ჩარჩო, თანამედროვე ტექნოლოგიური პროგრესის ეპოქა და ხელოვნური ინტელექტის ზეგავლენა პირადი ცხოვრების ხელშეუხებლობაზე, ბავშვთა პირადი ცხოვრების ხელშეუხებლობა, პირის ჯანმრთელობასთან დაკავშირებული პერსონალურ მონაცემთა დაცვის თანამედროვე სირთულეები, მონაცემთა დაცვის ოფიცრებისა და პირადი ცხოვრების ხელშეუხებლობის დაცვის პრაქტიკოსთა როლი და სხვა.

„ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის“ რიგით 75-ე შეხვედრას, რომელიც 1983 წელს იქნა დაფუძნებული, სამსახურმა თბილისში, ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტში უმასპინძლა. ღონისძიების ფარგლებში განხილულ იქნა პერსონალურ მონაცემთა დაცვის სამართლისა და ტექნოლოგიების სფეროში მიმდინარე გამოწვევები და აქტუალური საკითხები, მათ შორის: ნეირომონაცემები, 6G ტექნოლოგია, ციფრული იდენტობა, და სხვა. შეხვედრას თოთხმეტი ქვეყნის, ასევე ევროკავშირის მონაცემთა დაცვის ზედამხედველისა (“EDPS”) და ელექტრონული პირადი ცხოვრების ხელშეუხებლობის საინფორმაციო ცენტრის (“EPIC”) ოცდახუთი წარმომადგენელი დაესწრო.

„პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის“ წინამდებარე გამოცემა აერთიანებს ზემოაღნიშნული ორი საერთაშორისო ფორმატის, ღონისძიების ფარგლებში წარმოდგენილ მოხსენებებს, აგრეთვე, პერსონალურ მონაცემთა დაცვის სამართლის დარგის პრაქტიკოსთა, მკვლევართა სამეცნიერო ნაშრომებს. მადლობას ვუხდი ღონისიძიებების მონაწილეებს წარმოდგენილი სტატიებისთვის, რომელთა საშუალებითაც მკითხველს კონფერენციაზე განხილული საკითხების გაცნობის უნიკალური შესაძლებლობა ეძლევა. ვიმედოვნებთ, რომ გამოცემაში გამოქვეყნებული შრომები, ერთი მხრივ, საინტერესო, ხოლო მეორე მხრივ, ერთგვარი დამხმარე მასალა იქნება პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობით დაინტერესებული პირებისათვის და დარგის წარმომადგენელი პრაქტიკოსი იურისტებისთვის.

დოქტ., დოქტ. ლელა ჯანაშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

ბარსელონის ავტონომიური უნივერსიტეტის ასოცირებული პროფესორი

შერონ აზარია*

სახის ამომცნობი ტექნოლოგია: პირადი ცხოვრების ხელშეუხებლობის უფლებები და საკანონმდებლო გამოწვევები**

1. შესავალი

სახის ამომცნობი ტექნოლოგია სწრაფად გარდაიქმნა სამომავლო კონცეფციიდან ყოველდღიურ რეალობად, რომელიც მსოფლიოს მასშტაბით როგორც საჯარო, ასევე კერძო სექტორში გამოიყენება. მიუხედავად იმისა, რომ ტექნოლოგიის გამოყენების მომხრეები აღნიშნავენ მის პოტენციალს უსაფრთხოების გაუმჯობესებისა და მომსახურების პროცესის გამარტივების თვალსაზრისით, კრიტიკოსები ხაზს უსვამენ ტექნოლოგიის გამოყენებასთან ასოცირებულ კონფიდენციალობის, ადამიანის უფლებებისა და სოციალური თანასწორობის უპრეცედენტო საფრთხეებს. ტექნოლოგიების სფეროში მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფმა, რომელიც ცნობილია, როგორც „ბერლინის ჯგუფი“, მოამზადა კონკრეტული საკითხის შესახებ დოკუმენტი. წინამდებარე ნაშრომი შეისწავლის საკითხს და გვთავაზობს ტექნოლოგიის პასუხისმგებლიანი მმართველობის ჩარჩოს.[1]

წინამდებარე სტატია აანალიზებს ბერლინის ჯგუფის დასკვნებს სახის ამომცნობ ტექნოლოგიასთან დაკავშირებით, იკვლევს მის ტექნიკურ მახასიათებლებს, გამოყენების შესაძლებლობებს, მასთან ასოცირებულ რისკებს და ფუნდამენტურ უფლებათა დასაცავად აუცილებელ საკანონმდებლო მიდგომებს.

2. სახის ამომცნობი ტექნოლოგიის მნიშვნელობა

სახის ამომცნობი ტექნოლოგია ადამიანის სახეების ამსახველ ფოტო და ვიდეომასალას მათემატიკურ შაბლონებად გარდაქმნის, რომელთა შედარებაც შესაძლებელია მონაცემთა ბაზებთან. ტექნოლოგია ოთხ ძირითად ფუნქციას

---

* ისრაელის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს საერთაშორისო ურთიერთობების დეპარტამენტის ხელმძღვანელი.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. თბილისში გამართულ „ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის“, რიგით 75-ე შეხვედრაზე წარდგენილი მოხსენების ტექსტს.

[1] International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, 2023,1.

ასრულებს: აღმოჩენის, დადასტურების, იდენტიფიკაციის და ანალიზის.[2] აღმოჩენის ფუნქციის მიზანია დაადგინოს, რომ გამოსახულებაში იდენტიფიცირებადია სახე. ვერიფიკაციის ფუნქცია ამოწმებს, ემთხვევა თუ არა ადამიანის იდენტობა კონკრეტული პირის ვინაობას. იდენტიფიკაციის ფუნქცია უცნობი პირის სახეს მონაცემთა ბაზაში არსებულ სხვა პირთა სახეებს ადარებს. სახის ანალიზის ფუნქციის გამოყენების მიზანია არა მხოლოდ პირის იდენტობის დადგენა, არამედ მისი სახის მახასიათებლებზე დაყრდნობით ადამიანის შესახებ დასკვნების გაკეთება, თუმცა აღნიშნული დასკვნების მეცნიერული სანდოობის საკითხი საკამათოა.

თანამედროვე სისტემების უმეტესობა მანქანური სწავლების მოდელებს ეყრდნობა, რომლებიც გაწვრთნილია სახის გამოსახულების შემცველი დიდი ბაზების საფუძველზე. რაც უფრო მეტ მონაცემს ამუშავებს აღნიშნული ბაზები, უმჯობესდება სახეების ერთმანეთისაგან გარჩევის ფუნქციონალი, თუმცა სიზუსტე მრავალ საკითხს მოიაზრებს, მათ შორის, არასწორად იდენტიფიცირება, იდენტიფიცირების შეუძლებლობა, და სხვადასხვა დემოგრაფიული ჯგუფის თანაბარი ხარისხით გარჩევის საკითხი.[3]

3. გამოყენება და სადავო საკითხები

ბერლინის ჯგუფი სახის ამომცნობი ტექნოლოგიების გამოყენების სხვადასხვა მეთოდს განიხილავს, ტექნოლოგიის როგორც კერძო, ასევე საჯარო სექტორში გამოყენების კონტექსტში. კერძო სექტორში ტექნოლოგია გამოიყენება შენობა-ნაგებობებსა და მოწყობილობებზე უსაფრთხო წვდომის მიზნებით, უსაფრთხოების მონიტორინგისთვის ისეთ ადგილებში, როგორებიცაა კაზინოები და მაღაზიები, მარკეტინგული და მომხმარებელთა მომსახურების აპლიკაციები და სამსახურში გამოცხადების მონიტორინგი.[4] თუმცა ტექნოლოგიის გამოყენების წინამდებარე მაგალითებს ოპონენტებიც ჰყავს. ნიდერლანდების სამეფოსა და კანადის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებმა რიგი სახის ამომცნობი სისტემები უკანონოდ მიიჩნიეს სავაჭრო ცენტრებში გამოყენების შემთხვევაში, რაც პირადი ცხოვრების ხელშეუხებლობის დაცვის თვალსაზრისით მნიშვნელოვან პრეცედენტებს წარმოშობს.[5]

სამთავრობო უწყებები სახის ამომცნობ ტექნოლოგიებს სასაზღვრო კონტროლის, ციფრულ მომსახურებაზე წვდომის, სამართალდამცავი ორგანოებისა და საგანმანათლებლო დაწესებულებების მიზნებისათვის იყენებენ.[6] სამართალდამცავი ორგანოების მიერ მსგავსი აპლიკაციების

[2] იქვე, 4-5.
[3] იქვე, 5-6.
[4] იქვე, 7-10.
[5] იქვე, 8.
[6] იქვე, 11-12.

გამოყენება განსაკუთრებულად საყურადღებოა, რადგან საპოლიციო დაწესებულებები სახის ამომცნობ ტექნოლოგიებს იყენებენ ეჭვმიტანილების იდენტიფიცირებისთვის, რომლებიც უარს აცხადებენ მათთან თანამშრომლობაზე, აგრეთვე, დამნაშავეთა ფოტოსურათების მონაცემთა ბაზების შესადგენად, დანაშაულების გამოსაძიებლად და ძებნილი პირების ვინაობის რეალურ დროში დასადგენად.[7] აზრთა სხვადასხვაობას იწვევს სახის ამოცნობის სისტემების სკოლებში დანერგვის საკითხიც. კრიტიკოსთა მტკიცებით, არასრულწლოვანთა უწყვეტი ბიომეტრიული მეთვალყურეობის ქვეშ ყოფნამ შესაძლოა, უარყოფითად იმოქმედოს მათ განვითარებაზე და გამოიწვიოს აუტიზმის სპექტრის ან სხვადასხვა ფიზიკური მდგომარეობის მქონე მოსწავლეთა (რომლებიც გავლენას ახდენენ სახის გარეგნულ ნიშნებზე ან მახასიათებლებზე) დისკრიმინაცია.[8]

4. პირადი ცხოვრების ხელშეუხებლობასა და ფუნდამენტურ უფლებებზე ზემოქმედების რისკები

საზოგადოებრივ სივრცეებში განთავსებული სახის ამომცნობი სისტემები ყველა გამვლელის სახეს აღბეჭდავს, აღნიშნული მუდმივი მეთვალყურეობის რეჟიმი მონაცემთა სუბიექტებს ანონიმურობის შესაძლებლობას უკარგავს.[9] წინამდებარე ტიპის სისტემებმა შესაძლოა, გამოავლინოს ან შესაძლებელი გახადოს დასკვნების გაკეთება მონაცემთა სუბიექტების პოლიტიკური ან რელიგიური შეხედულებების, ჯანმრთელობის მდგომარეობისა და სექსუალური ორიენტაციის შესახებ. მხოლოდ იმის ცოდნამაც კი, რომ სახის ამოცნობის სისტემები განთავსებულია, შესაძლოა, გავლენა იქონიოს მონაცემთა სუბიექტების სურვილზე, მონაწილეობა მიიღონ საპროტესტო აქციებში, რელიგიურ ან სამედიცინო დაწესებულებებში ვიზიტის თვალსაზრისით, რაც ნეგატიურ ზეგავლენას ახდენს ადამიანების ძირითად უფლებებზე.[10]

გამოწვევაა მონაცემთა სიზუსტის დაცვის საკითხი. კვლევების თანახმად, ალბათობა იმისა, რომ რიგი სახის ამომცნობი სისტემების მიერ აზიელი და აფროამერიკული წარმომავლობის პირები თეთრკანიან მამაკაცებთან შედარებით არასწორად იდენტიფიცირდნენ, ასჯერ მეტია.[11] არასწორად იდენტიფიცირების რისკები მეტად მაღალია ქალების, ტრანსგენდერთა, არაბინარული ადამიანებისა და შეზღუდული შესაძლებლობების მქონე პირების შემთხვევაშიც. კანადის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ხელმძღვანელის განცხადების თანახმად, სახის ამომცნობი სისტემების დასკვნები ვინაობის შესახებ მხოლოდ სავარაუდოა და

[7] იქვე, 13-14.
[8] იქვე, 12.
[9] იქვე, 14-15.
[10] იქვე, 15.
[11] იქვე, 16.

არა დადასტურებული ფაქტები.[12] ტრენინგის მონაცემების ხარისხი ფუნდამენტურად განსაზღვრავს ალგორითმის მუშაობას; არაწარმომადგენლობით მონაცემთა ბაზებზე დაყრდნობით გაწვრთნილი სახის ამომცნობი სისტემები სხვადასხვა დემოგრაფიულ ჯგუფთან მიმართებით ამოცნობის სიზუსტის სხვადასხვა ხარისხს უზრუნველყოფს.

ზოგიერთი აპლიკაცია სიზუსტის და მიკერძოების თვალსაზრისით იმდენად პრობლემურია, რომ მათი ეთიკური გამოყენება ფაქტობრივად შეუძლებელია. ემოციების ამომცნობი სისტემები ეფუძნება ვარაუდს, რომ სხვადასხვა ადამიანები ემოციებს ერთგვარად გამოხატავენ, რაც კვლევებით არ დასტურდება.[13] ხშირ შემთხვევაში, აღნიშნული სისტემები ფერადკანიანი პირების სახეებს უფრო აგრესიულად მიიჩნევს, რაც საზიანო სტერეოტიპებს წარმოშობს. რიგი სისტემები, რომლებიც სახის მახასიათებლებზე დაყრდნობით სექსუალობის, კრიმინალურობის ან სხვა მახასიათებლების პროგნოზირებას უზრუნველყოფს, ეფუძნება ისეთ დებულებებს, რომლებიც პრაქტიკულად არ განსხვავდება ფსევდომეცნიერებებისგან.[14]

სახის ბიომეტრიული მონაცემების მუდმივი და უცვლელი ბუნების გამო მონაცემთა უსაფრთხოების დარღვევების შედეგები მეტად საზიანოა. პაროლებისა და საკრედიტო ბარათის ნომრებისგან განსხვავებით, მონაცემთა უსაფრთხოების დარღვევის შემდეგ სახეების გადატვირთვა ან შეცვლა შეუძლებელია.[15] ჰაკერებს, რომლებსაც აღნიშნულ მონაცემებზე წვდომა შეუძლიათ, ეძლევათ მონაცემთა სუბიექტის იდენტობის მოპარვის, პიროვნების იდენტობის გაყალბების - თავის მსხვერპლად წარმოჩენის ან უკანონო საქმიანობის საშუალება. პრაქტიკაში უკვე დაფიქსირდა აღნიშნული ტიპის მნიშვნელოვანი დარღვევები, მათ შორის, უსაფრთხოების დარღვევა ჩინურ მონაცემთა ბაზაში, რომელიც მილიონობით ბიომეტრიულ მონაცემს შეიცავს, და თვეების განმავლობაში იყო ხელმისაწვდომი ინტერნეტსივრცეში.[16]

რეალურ დროში სახის ამომცნობი ტექნოლოგიები დამატებით რისკებს წარმოშობს. აღნიშნული სისტემები ავტომატურად აგროვებს ბიომეტრიულ მონაცემებს რეალურ დროში, ამუშავებს ინფორმაციას ყველა იმ პირის შესახებ, რომლებიც მონიტორინგის ზონებში სისტემების ხედვის არეალში ექცევიან.[17] ერთ-ერთი პოტენციური ძალადობის ფაქტის ამსახველი შემთხვევა ლონდონის მეტროპოლიტენის პოლიციას უკავშირდება. პოლიციის დეპარტამენტის თანამშრომლებმა სისტემის მიერ დადგენილი მცდარი შესაბამისობის საფუძველზე გააჩერეს და დაკითხეს თოთხმეტი წლის სკოლის მოსწავლე.

[12] იქვე, 18-19.
[13] იქვე, 16-17.
[14] იქვე, 17-18.
[15] იქვე, 21
[16] იქვე, 22.
[17] იქვე, 23.

მოგვიანებით აღნიშნული სისტემა არასანდოდ იქნა მიჩნეული.[18]

5. საკანონმდებლო მიდგომები და რეკომენდაციები

ბერლინის ჯგუფი სახის ამოცნობასთან დაკავშირებული რისკების შესამცირებლად სხვადასხვა სტრატეგიას გვთავაზობს, ტექნოლოგიის გამოყენების სრულად აკრძალვებიდან ტექნიკური და პროცედურული დაცვის ზომების გატარებამდე. ნებისმიერი სისტემის დანერგვამდე მონაცემთა დამუშავებისთვის პასუხიმგებელმა პირებმა საჭიროა შეაფასონ რისკები, მათ შორის: დაზარალებულ პირთა წრე, მონაცემთა შენახვის ცენტრალიზებულობა, საძიებო სისტემის შესაძლებლობები, შაბლონების შენახვის საკითხი, მონაცემთა შეგროვების ნებაყოფლობითობა, სისტემის გამჭვირვალობისა და თანხმობის საკითხები და იმ გარემოს მახასიათებლები, რომლებშიც სისტემა იქნება გამოყენებული.[19]

ცალკეული საკანონმდებლო სისტემების თანახმად, ფუნდამენტური უფლებების ხელყოფის თვალსაზრისით გარკვეული აპლიკაციები იმდენად სერიოზულ საფრთხეს წარმოშობს, რომ აუცილებელია მათი გამოყენების სრულად აკრძალვა. მონაცემთა დაცვის ევროპულმა საბჭომ და ევროკავშირის მონაცემთა დაცვის ზედამხედველმა საჯარო სივრცეებში ავტომატური ამოცნობის სისტემების აკრძალვის შესახებ მოსაზრება გამოაქვეყნეს.[20] ევროპარლამენტმა მხარი დაუჭირა საჯარო სივრცეებში ავტომატური ამოცნობის სისტემების აკრძალვას და ...სახის ამოცნობის კერძო მონაცემთა ბაზების აკრძალვას, მაგალითად, ისეთისას, როგორიცაა Clearview AI.[21] წინამდებარე წინადადებები ევროპულ, ავსტრალიურ და კანადურ მონაცემთა დაცვის საზედამხედველო ორგანოთა მიერ აღსრულების პრაქტიკას დაეფუძნა კომპანიების წინააღმდეგ სათანადო სამართლებრივი საფუძვლის ან დაცვის ზომების გარეშე მონაცემთა დამუშავებისათვის.

აკრძალვები აშშ-ის რამდენიმე შტატმაც დააწესა: ვერმონტი, მენი, ნიუ ჰემფშირი, ორეგონი და კალიფორნია ზღუდავენ ან კრძალავენ სახის ამოცნობას სხვადასხვა კონტექსტში.[22] ასზე მეტმა ორგანიზაციამ და ასობით ექსპერტმა ორმოცზე მეტი ქვეყნიდან მხარი დაუჭირა რეკომენდაციებს, რომ ქვეყნებმა შეაჩერონ სახის ამოცნობის სისტემათა შემდგომი გამოყენება სამართლებრივი საფუძვლისა და მონაცემთა დაცვის შესაბამისი ზომების დანერგვამდე.[23]

იმ შემთხვევაში, თუ სახის ამოცნობის სისტემის დანერგვა სრულად არ

[18] იქვე, 24.
[19] იქვე, 25-27.
[20] იქვე, 28.
[21] იქვე, 28-29.
[22] იქვე, 30.
[23] იქვე, 30

არის აკრძალული, ბიომეტრიული მონაცემების დამუშავებისთვის უნდა არსებობდეს მკაფიო და კონკრეტული სამართლებრივი საფუძველი.[24] მაღალი რისკის მქონე სისტემების დანერგვის შემთხვევაში ორგანიზაციებმა მის დანერგვამდე საჭიროა გაიარონ კონსულტაცია კომპეტენტურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან. სახის ამოცნობა საზოგადოებრივ ადგილებში უნდა ემსახურებოდეს აუცილებელ და მნიშვნელოვან საზოგადოებრივ ინტერესებს, რომელთა დაცვა ნაკლებად ინვაზიური საშუალებებით შეუძლებელია.

როგორც წესი, საზოგადოებრივ ადგილებში სახის ამომცნობი სისტემების გამოყენებაზე მონაცემთა სუბიექტის თანხმობა არ წარმოადგენს მონაცემთა დამუშავებისთვის სათანადო სამართლებრივ საფუძველს, აღნიშნულ პირობებში ნამდვილი თანხმობის გაცემის შეუძლებლობის გამო.[25]

საჭიროა საზოგადოების ინფორმირება საზოგადოებრივ ადგილებში სახის ამოცნობის სისტემის დანერგვის შესახებ.[26] გამჭვირვალობა მოიცავს მონაცემთა დაცვაზე ზეგავლენის შეფასებებზე წვდომასა და სისტემის სიზუსტისა და მიკერძოების შესახებ ტესტირების შედეგებზე წვდომას. სისტემის არსებობის შესახებ ნიშნები საჭიროა იქნეს თვალსაჩინო, მოთავსებული იმგვარად, რომ აღიქმებოდეს პირთა სისტემის მუშაობის არეალში მოქცევამდე და ნათლად მიუთითებდეს, რომ სახის ამომცნობი ტექნოლოგია ფუნქციონირებს.

საჭიროა, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა გაატარონ ტექნიკური ზომები რისკების შესამცირებლად. აგრეთვე, მონაცემთა ბაზები, კამერები, განათება და ფოტოს გადაღების რეჟიმი უზრუნველყოფდეს სურათების მაღალ გარჩევადობას.[27] მონაცემთა სიზუსტისათვის აუცილებელია, შემუშავდეს სისტემის წვრთნის ოპტიმალური პირობები. სისტემის წვრთნისა და შედარების მიზნებით არსებული მონაცემთა ბაზები უნდა უზრუნველყოფდეს მონაწილეთა მრავალფეროვნებას ასაკის, სქესის და კანის ფერის მიხედვით. საჭიროა მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა დაადგინონ შესაბამისი სანდოობის ზღვრები და სანდოობის ხარისხი რეგულარულად გადაამოწმონ. ამავდროულად, მონაცემთა დამუშავება უნდა შეწყდეს, თუკი სისტემები ვერ აკმაყოფილებს აღნიშნულ მოთხოვნებს. იმ შემთხვევაში, თუ სახის ამომცნობი სისტემის მიერ მიღებული გადაწყვეტილებები გავლენას ახდენს მონაცემთა სუბიექტებზე, საბოლოო გადაწყვეტილებები საჭიროა გადამოწმებულ იქნეს ადამიანის მიერ და არ ეფუძნებოდეს მხოლოდ მონაცემთა ავტომატიზირებულ დამუშავებას.[28]

სისტემის შექმნის ეტაპზე და ფუნქციონირების პროცესში საჭიროა

[24] იქვე, 30-31.
[25] იქვე, 32.
[26] იქვე, 32.
[27] იქვე, 32-33.
[28] იქვე, 33.

გამოყენებულ იქნეს მონაცემთა მინიმიზაციის სტრატეგიები.[29] აგრეთვე, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეინახონ პერსონალური მონაცემები მხოლოდ აუცილებელი საჭიროების შემთხვევაში, წაშალონ ორიგინალი სურათები მათგან შაბლონების შექმნის შემდეგ, დანერგონ ავტომატური წაშლის მექანიზმები განსაზღვრული შენახვის ვადის ამოწურვის შემდეგ, თავიდან აიცილონ სხვა მონაცემთა წყაროებთან კავშირის შესახებ ინფორმაციის გაცემა, შეინახონ შაბლონები მაიდენტიფიცირებელი ინფორმაციისგან განცალკევებით, განახორციელონ მონაცემთა დაშიფვრა და ანონიმიზაცია, შეინახონ მონაცემები მხოლოდ განსაზღვრული მიზნებისთვის საჭირო ვადით და უზრუნველყონ მონაცემთა დაცვა მთელი სასიცოცხლო ციკლის განმავლობაში.[30]

6. დასკვნა

ბერლინის χგუფის სამუშაო დოკუმენტი გვთავაზობს მნიშვნელოვან ჩარჩოს სახის ამოცნობის ტექნოლოგიის მიერ კონფიდენციალობის, ადამიანის უფლებებისა და სოციალური თანასწორობის წინაშე არსებული სერიოზული გამოწვევების ანალიზისთვის და დასახელებული საკითხების გადასაჭრელად. დოკუმენტის თანახმად, ტექნოლოგია შესაძლოა, გამოყენებულ იქნეს იმგვარად, რომ იყოს სარგებლიანი, თუმცა ამავდროულად დოკუმენტი ცხადყოფს, რომ სახის ამოცნობის სისტემები შეიძლება იყოს ინვაზიური, დისკრიმინაციული და მონაცემთა სუბიექტებზე ფართომასშტაბიანი მეთვალყურეობა მკაცრ რეგულირებას საჭიროებს, რომელიც პრიორიტეტს მიანიჭებს ადამიანის ფუნდამენტური უფლებების დაცვას.

მსოფლიოში არსებული საკანონმდებლო მიდგომების მრავალფეროვნება მიანიშნებს, რომ დემოკრატიულ საზოგადოებებში ბიომეტრიული მეთვალყურეობის შესაბამისი საზღვრების შესახებ მსჯელობა მიმდინარე პროცესია. სამუშაო დოკუმენტის მიერ აქცენტირებული საკითხები – რისკების შეფასება, მკაფიო სამართლებრივი ჩარჩოები, გამჭვირვალობა, სიზუსტე, ანგარიშვალდებულება და ტექნიკური დაცვა – კანონმდებლებს, მონაცემთა დაცვის საზედამხედველო ორგანოებს და ორგანიზაციებს პრაქტიკულ მიმართულებას სთავაზობს.

ბიბლიოგრაფია:

1. International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, 2023.

[29] იქვე, 34.
[30] იქვე, 35.

შერონ აზარია*

მონაცემთა დაცვა და კონფიდენციალობა ჭკვიან ქალაქებში: ტექნოლოგიების სფეროში მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის დოკუმენტის კრიტიკული ანალიზი**

1. შესავალი

ურბანული გარემოს სწრაფმა დიგიტალიზაციამ ქალაქები მონაცემთა შეგროვების, ანალიზისა და ავტომატიზებული გადაწყვეტილებების მიღების რთულ ეკოსისტემებად გადააქცია. ტექნოლოგიების სფეროში მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფი ("IWGDPT") ამ ტრანსფორმაციას განიხილავს დოკუმენტში „ჭკვიანი ქალაქები", რომელიც წარმოადგენს ყოვლისმომცველ ჩარჩოს „ჭკვიანი ქალაქის" კონცეფციაში მონაცემთა დაცვის გამოწვევების უკეთ გასაგებად.[1] წინამდებარე ნაშრომი იკვლევს სამუშაო ჯგუფის დოკუმენტის წვლილს ურბანული დიგიტალიზაციის პროცესში, აფასებს მონაცემთა შეგროვების, ანალიზისა და გადაწყვეტილების მიღების სამმხრივ ჩარჩოს, ამავდროულად, დოკუმენტის პრაქტიკულ შედეგებს ქალაქების, ინდუსტრიებისა და მარეგულირებლებისთვის.

2. ჭკვიანი ქალაქები: განმარტებითი დებატების ფარგლებს გარეთ

„ჭკვიანი ქალაქის" შესახებ საკამათო დებატებში ჩართვის ნაცვლად, სამუშაო ჯგუფი პრაგმატულ მიდგომას იყენებს და დიგიტალიზაციის პროცესზე აკეთებს აქცენტს.[2] აღნიშნული მეთოდოლოგიური არჩევანი მნიშვნელოვანია იმ თვალსაზრისით, რომ ამ ფორმით შესაძლებელია აბსტრაქტული განმარტებებიდან მონაცემთა დაცვის კონკრეტულ გამოწვევებზე კონცენტრირება. სამსაფეხურიანი ჩარჩო - მონაცემთა შეგროვება, ანალიზი და გადაწყვეტილების მიღება - სტრუქტურირებულ ერთეულს წარმოადგენს, რომლის მეშვეობითაც შესაძლებელია ურბანულ კონტექსტში მონაცემთა

* ისრაელის პირადი ცხოვრების ხელშეუხებლობის სამსახურის საერთაშორისო ურთიერთობის დეპარტამენტის ხელმძღვანელი.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. თბილისში გამართულ „ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის", რიგით 75-ე შეხვედრაზე წარდგენილი მოხსენების ტექსტს.

[1] International Working Group on Data Protection in Technology, Working Paper on "Smart Cities", Adopted at the 70th Meeting on 29th-30th November 2022, Written Procedure Prior to 71st Meeting on 7th-8th June 2023, 1.

[2] იქვე.

დამუშავების სასიცოცხლო ციკლის შესწავლა.

უნდა აღინიშნოს, რომ მონაცემთა შეგროვება ეფუძნება მრავალფეროვან ტექნოლოგიას, რომელთა შორისაა „ნივთების ინტერნეტი“, სენსორული ქსელები და ვიდეომეთვალყურეობის სისტემები. ასევე, იგი მოიაზრებს სახელმწიფო ორგანოებისა და მუნიციპალიტეტების მიერ შენახული მონაცემების ხელახალ გამოყენებას.[3] მონაცემთა ანალიზი გულისხმობს დახვეწილი დამუშავების სისტემას, მათ შორის, მონაცემთა შესაბამისობას, ხელოვნურ ინტელექტს, პროფაილინგსა და ე.წ. „ციფრულ ტყუპებს“.[4] და ბოლოს, გადაწყვეტილების მიღების ეტაპი მოიცავს ანალიტიკური შედეგების გამოყენებას ქალაქის რესურსების სამართავად, ურბანული ფუნქციების კონტროლისა და პოლიტიკის დოკუმენტების შემუშავებისთვის. დასახელებული ყოვლისმომცველი რუკა ქმნის საფუძველს იმის გასაგებად, თუ სად წარმოიქმნება მონაცემთა დაცვის რისკები და როგორ შეიძლება მათი შემცირება.

3. ანგარიშვალდებულება და მმართველობა: ეთიკური ჭკვიანი ქალაქების საფუძველი

ჭკვიანი ქალაქის ინიციატივების წინაპირობად ანგარიშვალდებულებასა და მმართველობაზე ყურადღების გამახვილება მის მნიშვნელოვან მონაპოვრად შეიძლება ჩაითვალოს. სამუშაო ჯგუფი ამტკიცებს, რომ ქალაქებმა მონაცემთა ნებისმიერი დამუშავების დაწყებამდე უნდა ჩაატარონ მკაცრი შეფასებები, მათ შორის მონაცემთა დაცვაზე ზეგავლენის შეფასება.[5] ეს პროაქტიული მიდგომა ეჭქვეშ აყენებს არსებულ სისტემებზე კონფიდენციალობის დაცვის მექანიზმების მორგების გავრცელებულ პრაქტიკას, რომელიც არაერთხელ დადასტურდა, რომ არასაკმარისია უფლებების დაცვის თვალსაზრისით.

იდენტიფიკაციის კონცეფციას განსაკუთრებული ყურადღება ეთმობა ანგარიშვალდებულების ნაწილში. ნაშრომში სწორად არის აღნიშნული, რომ იდენტიფიკაციის შესაძლებლობა უნდა შეფასდეს არა მხოლოდ კონკრეტულ დამუშავების ოპერაციებთან მიმართებით, არამედ ზოგადად, დამუშავებასთან დაკავშირებითაც, რამაც შეიძლება არაპირდაპირი იდენტიფიკაციის შესაძლებლობა მოგვცეს.[6] იდენტიფიკაციის აღნიშნული მეთოდი ასახავს კონფიდენციალობის კუმულაციური რისკების გაგებას, რომლებიც მონაცემთა სისტემების ურთიერთქმედებისას წარმოიქმნება.

„ენშედეს შემთხვევის“ კვლევა ასახავს არასაკმარისი ანგარიშვალდებულების შედეგებს. ენშედეს მუნიციპალიტეტმა ქალაქის

[3] იქვე, 2.
[4] იქვე.
[5] იქვე, 3.
[6] იქვე, 4.

ცენტრში 24/7 Wi-Fi თვალთვალი დანერგა იმ დასაბუთებით, რომ ანონიმიზაციის გამო მონაცემები არ იყო პერსონალური.[7] თუმცა ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ მოწყობილობების პროგრამული მისამართების, დროის ნიშნულების და მდებარეობის ინფორმაციის კომბინაცია პერსონალურ მონაცემებს წარმოადგენდა, რადგან ანონიმიზაციის მეთოდი საკმარისად არ გამორიცხავდა პირთა იდენტიფიკაციის რისკს.[8] ეს შემთხვევა ადასტურებს მკაცრი შეფასებისა და ხელახალი იდენტიფიკაციის რისკების სათანადო გათვალისწინების მნიშვნელობას.

4. მონაცემთა მინიმიზაცია: ინოვაციისა და კონფიდენციალობის შეთავსება

მონაცემთა მინიმიზაციის პრინციპი განსაკუთრებულ მნიშვნელობას იძენს ჭკვიანი ქალაქის კონტექსტში, როდესაც განუსაზღვრელი მიზნებისთვის ყოვლისმომცველი მონაცემთა ნაკრებების შეგროვება ეწინააღმდეგება კონფიდენციალობის დაცვის ფუნდამენტურ პრინციპს. ნაშრომში დასაბუთებულია, რომ, როდესაც მიზანი მონაცემთა ანალიზია, ქალაქებმა მონაცემები უნდა გააერთიანონ და იდენტიფიკაციის მანიშნებლები ამოიღონ შეგროვების ეტაპზევე, რაც შეიძლება დროულად.[9] ეს მიდგომა წარმოადგენს სისტემიდან გადახვევას, რომელიც ფართოდ ვრცელდება ტექნოლოგიური სექტორის ურბანული დიგიტალიზაციის პროცესში.

ლონდონის ტრანსპორტის მონაცემთა შეგროვების ინიციატივა პრაქტიკაში მონაცემთა მინიმიზაციის დადებით მაგალითს წარმოადგენს. ლონდონის ტრანსპორტის კომპანიამ სცადა, გაეგო მომხმარებელთა გადაადგილების შესახებ ინფორმაცია სადგურებში კონკრეტული პირების იდენტიფიცირების გარეშე.[10] შეგროვებისთანავე კრიპტოგრაფიული ფუნქციების გამოყენებით ავტომატური დაშტრიხვის განხორციელებით და Wi-Fi მონაცემების სხვა მონაცემთა ნაკრებებთან, მაგალითად, როგორიცაა სამგზავრო ბარათის ინფორმაცია, შესაბამისობისგან თავის შეკავებით, სატრანსპორტო კომპანიამ მიიღო ღირებული ურბანული ინფორმაცია მონაცემთა მინიმიზაციის პრინციპის დაცვით.[11]

რეკომენდაცია, რომ ქალაქებმა ტექნიკური ზომების მეშვეობით უზრუნველყონ პირის იდენტიფიკაციის გამორიცხვის ფუნქციის მქონე სენსორების შეძენა და მინიმიზაციის პრინციპის ფართოდ დანერგვა - მნიშვნელოვანი ნაბიჯია „კონფიდენციალობის პრინციპის“ დისკურსში.[12] ეს

[7] იქვე, 6.
[8] იქვე.
[9] იქვე, 8.
[10] იქვე.
[11] იქვე, 9.
[12] იქვე, 8.

მიდგომა მონაცემთა დაცვაზე პასუხისმგებლობას ინდივიდუალური არჩევანიდან ან შეგროვების შემდგომი მოქმედებიდან უშუალოდ სისტემის გამართულობაზე გადაიტანს, რაც მას უფრო ეფექტიანს ხდის და უნარჩუნებს შედეგს პერსონალის ან ორგანიზაციული პრიორიტეტების ცვლილებების მიუხედავად.

5. მიზნის შეზღუდვა: ფუნქციის წინააღმდეგ ბრძოლა

მრავალმხრივი როლი, რომელსაც ქალაქები ასრულებენ მოქალაქეთა ცხოვრებაში, მიზნის შეზღუდვის განსაკუთრებულ გამოწვევებს ქმნის. ნაშრომში აღნიშნულია მნიშვნელოვანი რისკი მუნიციპალური ფუნქციისთვის - როგორიცაა საგზაო მოძრაობის მართვა, როდესაც შეგროვებული მონაცემები შეიძლება გამოყენებულ იქნეს სხვა ფუნქციისთვის, შესაბამისი შეფასების ან სამართლებრივი საფუძვლის გარეშე.[13] ეს ფენომენი, რომელსაც ხშირად „ფუნქციის ცვლას“ უწოდებენ, სერიოზულ საფრთხეს უქმნის ინდივიდუალურ ავტონომიას და ინსტიტუციურ ნდობას.

ჭკვიანი სახლების შემთხვევის შესწავლა პრაქტიკაში მიზნის შეზღუდვის სირთულეს ასახავს, როდესაც საცხოვრებელში ტენისა და ნესტის დონის მონიტორინგისთვის დამონტაჟებული სენსორები - ტექნიკური მომსახურების მიზნით - უზრუნველყოფს ოჯახების გარკვეული ჯგუფის გარკვევას მათთვის სოციალური კეთილდღეობის მიზნით კონკრეტული მომსახურების შესათავაზებლად, რაც თავსებადობასთან დაკავშირებით აჩენს კითხვებს.[14] ნაშრომში სწორად არის აღნიშნული, რომ ინდივიდების ცხოვრებაში კეთილი განზრახვით ჩარევაც კი მოითხოვს ან მკაფიო იურიდიულ საფუძველს, ან მონაცემთა სუბიექტის თანხმობას, თუ ისინი გადაუხვევენ თავდაპირველ მიზანს.[15]

თავსებადობის შეფასების რეკომენდაცია მონაცემების გამოყენების იმ მიზნებისთვის, რომელთათვისაც ისინი თავდაპირველად შეგროვდა, ერთგვარ საფუძველს ქმნის ფუნქციების ცვლილების თავიდან ასაცილებლად.[16] თუმცა ნაშრომში შეიძლებოდა უფრო დეტალური ინსტრუქციების ჩამოყალიბება იმის შესახებ, თუ როგორ უნდა ჩაატარონ ქალაქებმა ასეთი შეფასებები, განსაკუთრებით მაშინ, როდესაც ახალი მიზანი შეიძლება იყოს საზოგადოებრივი ინტერესების დაცვა.

6. უსაფრთხოება და გამჭვირვალობა: ახალი გამოწვევები

ნაშრომში ხაზგასმულია „ნივთების ინტერნეტის“ უსაფრთხოებასთან

[13] იქვე, 10.
[14] იქვე, 11.
[15] იქვე.
[16] იქვე, 12.

დაკავშირებული გამოწვევები. ახალი საკანონმდებლო ინიციატივები, მაგალითად, როგორიცაა გაერთიანებული სამეფოს „პროდუქტის უსაფრთხოებისა და ტელეკომუნიკაციების ინფრასტრუქტურის შესახებ“ კანონპროექტი, აჩვენებს ნივთების ინტერნეტის უსაფრთხოების ნაკლოვანებების მზარდ აღიარებას.[17] ნაგულისხმევი პაროლების აკრძალვა, დაუცველობის გამჟღავნების მოთხოვნები და სავალდებულო უსაფრთხოების განახლება წარმოადგენს მნიშვნელოვან ნაბიჯებს სისტემური სისუსტეების მოგვარებისკენ.

გამჭვირვალობის რეკომენდაციებში ხაზგასმულია, რომ ჭკვიანი ქალაქის მონაცემების შეგროვება ხშირად „პასიურია“ - ხდება ინდივიდუალური თანხმობის გარეშე და უხილავია.[18] ნაშრომში გამჭვირვალობის მრავალი მექანიზმის მხარდაჭერა, მათ შორის, შეგროვების წერტილების, დამუშავების საჯარო რეესტრებისა და ალგორითმების ჩათვლით, აღიარებს, რომ სხვადასხვა შინაარსი და აუდიტორია მოითხოვს განსხვავებულ საკომუნიკაციო სტრატეგიას.[19]

ამსტერდამის ალგორითმების რეესტრი მიიჩნევა ყველაზე ინოვაციურ მიდგომად გამჭვირვალობის თვალსაზრისით, რადგან ქალაქში მოქმედი ალგორითმული დამუშავებების საჯაროდ ხელმისაწვდომ ჩამონათვალს მოიცავს.[20] მსგავსი ინიციატივები მნიშვნელოვანი წინგადადგმული ნაბიჯია პერსონალურ მონაცემთა დამუშავების შესახებ სტანდარტულ ინფორმირების ფორმასთან შედარებით, რომელიც, როგორც წესი, ინფორმაციას მხოლოდ მონაცემთა სუბიექტებს აწვდის. ქალაქის მასშტაბით გამჭვირვალობის მექანიზმების შექმნის საშუალებით მუნიციპალიტეტებს შესაძლებლობა აქვთ, ხელი შეუწყონ საზოგადოების ცნობიერების ამაღლებას და ქალაქის ციფრული განვითარების მიმართულებით მსჯელობებს.

7. მიგნებები და სამომავლო მიმართულებები

ტექნოლოგიების სფეროში მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის დოკუმენტი წარმოადგენს ღირებულ სახელმძღვანელოს ჭკვიან ქალაქებში მონაცემთა დაცვის თვალსაზრისით, რომელიც ურბანული გაციფრულებისთვის არის მნიშვნელოვანი. სახელმძღვანელოში ასახული პრაქტიკული რეკომენდაციები ქალაქებს, ინდუსტრიას და მარეგულირებლებს სთავაზობს გზებს, რომელთა საშუალებითაც შეუძლიათ, წარადგინონ პირადი ცხოვრების ხელშეუხებლობის უფლების პატივისცემაზე ორიენტირებული ინიციატივები.

[17] იქვე, 13.
[18] იქვე, 14.
[19] იქვე, 15-16.
[20] იქვე, 15.

დოკუმენტში ანგარიშვალდებულებასა და მმართველობაზე ხაზგასმა წარმოაჩენს სამომავლო ხედვას, რომელიც აღიარებს თანამედროვე ურბანული მონაცემების ეკოსისტემების კომპლექსურობას. ჭკვიანი ქალაქების დაგეგმარების პროცესში მონაცემთა ეფექტიანი დაცვის უზრუნველსაყოფად საჭიროა არა რეაქტიული, არამედ პროაქტიული ზომების მიღება. აღნიშნული პრევენციული ზომებით შესაძლებელია საზოგადოების ნდობის შენარჩუნება, რაც გრძელვადიან პერსპექტივაში ჭკვიანი ქალაქის წარმატების არსებით კომპონენტს წარმოადგენს.

რეალური მაგალითების გათვალისწინება (მაგალითად, როგორებიცაა Enschede Wi-Fi მიდევნება; მონაცემთა შეგროვების პროცესში პირადი ცხოვრების დაცვაზე ორიენტირებული ლონდონის ტრანსპორტი), წარმოადგენს პრაქტიკულ სახელმძღვანელოს ქალაქებისთვის. აღნიშნული მაგალითები წარმოაჩენს როგორც გამოწვევებს, ასევე შესაძლებლობებს, რომლებიც გაციფრულების სხვადასხვა ეტაპზე ჭკვიანი ქალაქების განვითარების თანმდევი პროცესია.

წინამდებარე ნაშრომში ასახული პრინციპები ქმნის ჭკვიანი ქალაქების მართვისა და ამ სფეროში დიალოგის ხელშეწყობის საფუძველს. ნაშრომში არისტოტელეს სიტყვების მოშველიება, რომლის შესაბამისადაც ქალაქები არსებობს იმისათვის, რომ მოქალაქეებს მისცეს „სრულყოფილი ცხოვრების“[21] შესაძლებლობა, გვახსენებს, რომ ტექნოლოგიური პროგრესი უნდა ემსახურებოდეს ადამიანის კეთილდღეობას. გამომდინარე იქიდან, რომ ჭკვიანი ქალაქის ტექნოლოგიები მუდმივად ვითარდება, ამ ნაშრომით დადგენილი სტანდარტები შეიძლება, იყოს დამხმარე საშუალება ინოვაციების ადამიანის ძირითად უფლებებსა და დემოკრატიულ ღირებულებებთან შესაბამისობაში მოყვანის თვალსაზრისით.

სტატიაში ქალაქების, ინდუსტრიის, მარეგულირებლებისა და მოქალაქეთა თანამშრომლობის აუცილებლობაზე ხაზგასმა წარმოაჩენს, რომ ქალაქის წარმატებული განვითარება საჭიროებს მრავალმხრივ ჩართულობას.[22] აღნიშნული პოზიციის შესაბამისად, ჭკვიანი ქალაქების მომავალი ფორმირდება არა მხოლოდ ტექნოლოგიური საშუალებებით, არამედ ეთიკური პრინციპების დაცვით და ადამიანზე ორიენტირებული მიდგომების უზრუნველყოფით.

[21] იქვე, 1.
[22] იქვე, 5.

8. დასკვნა

ჭკვიანი ქალაქების შესახებ "IWGDPT"-ის ფარგლებში მომზადებული ნაშრომი წარმოადგენს მნიშვნელოვან წყაროს ურბანული გაციფრულებისა და მონაცემთა დაცვის სფეროებში. მონაცემთა ნაკადების ანალიზის სტრუქტურირებული ჩარჩოს შექმნით, მონაცემთა დამუშავების თითოეულ ეტაპზე კონფიდენციალობის რისკების იდენტიფიცირებით და ქალაქების, ინდუსტრიისა და მარეგულირებლებისთვის კონკრეტული რეკომენდაციების შეთავაზებით, ნაშრომი როგორც თეორიულ, ასევე პრაქტიკულ დონეზე ხელს შეუწყობს ურბანულ კონტექსტში მონაცემთა დაცვის სტანდარტების გათვალისწინებას.

ნაშრომში აქცენტი პროაქტიულ ანგარიშვალდებულებაზე, მონაცემთა მინიმიზაციაზე, მიზნის შეზღუდვისა და გამჭვირვალობის პრინციპებზე ქმნის საფუძველს ჭკვიანი ქალაქების განვითარებისთვის, რა პროცესშიც არსებითად მნიშვნელოვანია კონფიდენციალობის დაცვა და, ასევე, ლეგიტიმური მიზნების გათვალისწინება ურბანული მართვის უზრუნველსაყოფად. კონკრეტული საქმეების შესწავლა, განსაკუთრებით "Enschede-ს" არასათანადო ანონიმიზაციისა და ლონდონის ტრანსპორტის კონფიდენციალობის დაცვის მიდგომის კონტრასტული მაგალითები, მუნიციპალიტეტებისთვის ციფრული ინიციატივების ეტაპზე დამხმარე საშუალებას წარმოადგენს.

თუმცა, გამომდინარე იქიდან, რომ ქალაქები მუდმივად ვითარდება დიდი მოცულობის მონაცემთა დამუშავების პირობებში, ახალი გამოწვევების საპასუხოდ აუცილებელი იქნება საკითხის სათანადო შესწავლა და პოლიტიკის დოკუმენტის შემუშავება. სტატიაში წარმოდგენილი რეკომენდაციები უნდა მივიჩნიოთ როგორც საწყისი ჩარჩო, რომელიც მოითხოვს მუდმივ დახვეწას ტექნოლოგიური განვითარების, მარეგულირებელი ორგანოების ევოლუციისა და ჭკვიანი ქალაქის ინიციატივების გამოცდილების საპასუხოდ. ჭკვიანი ქალაქების საბოლოო წარმატება დამოკიდებული იქნება არა მხოლოდ ტექნიკურ გამართულობაზე, არამედ შესაძლებლობაზე, შეინარჩუნოს იმ მოქალაქეების ნდობა და მხარდაჭერა, რომლებსაც ის ემსახურება - მიზანი, რომლის მიღწევაც მხოლოდ მონაცემთა დაცვისა და ძირითადი უფლებების პატივისცემით არის შესაძლებელი.

ბიბლიოგრაფია:

1. *International Working Group on Data Protection in Technology*, Working Paper on "Smart Cities", Adopted at the 70th Meeting on 29th-30th November 2022.

ნორბერტ ბერნსდორფი[*]

პერსონალურ მონაცემთა დაცვის ისტორიული ფესვები — როგორ გაჩნდა ის!

სტატიაში განხილულია პერსონალურ მონაცემთა დაცვის ისტორიული საწყისები, რომლებიც სათავეს ანტიკური ხანიდან იღებს. ნაშრომი შეეხება მონაცემთა დაცვის ტერმინოლოგიის საფუძვლებს, მის ადრეულ და თანამედროვე ფორმებსა და განვითარებას წლების განმავლობაში. განსაკუთრებული ყურადღება ეთმობა მონაცემთა დაცვის მარეგულირებელი ჩარჩოების ჩამოყალიბებას 1970 წლიდან, გერმანიით დაწყებული იმ თანამედროვე სამართლებრივი ინსტრუმენტებით დამთავრებული, რომლებიც ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის ჩარჩოს ქმნის.

საკვანძო სიტყვები: *მონაცემთა დაცვის ფესვები, მონაცემთა დაცვის ტერმინოლოგია, პირადი ცხოვრების ხელშეუხებლობის უფლება.*

1. შესავალი

შესაბამის ლიტერატურაში პერსონალურ მონაცემთა დაცვა ხშირად „ისტორიის არმქონე დისციპლინად“ განიხილება. ეს არ არის სიმართლე მხოლოდ ამ კონკრეტული მნიშვნელობით. მართალია, რომ პერსონალურ მონაცემთა დაცვის კანონმდებლობის თანამედროვე კონცეფცია, ანუ პერსონალურ მონაცემთა დაცვის სამართალი, როგორსაც მას დღეს ვიცნობთ, მხოლოდ ბოლო ათწლეულების განმავლობაში განვითარდა. თუმცა პირადი ცხოვრების დაცვას დიდი ისტორია აქვს. პრინციპში, მისი საწყისი ანტიკურ ხანას უკავშირდება. მიუხედავად ამისა, ზედმეტად შორს წავალთ, თუ ადამისა და ევას მიერ სამოთხიდან განდევნის შემდეგ გამოყენებულ ლეღვის ფოთოლს პერსონალურ მონაცემთა დაცვის ადრეულ ფორმად მივიჩნევთ. თუმცა უძველეს დროშიც არსებობდა ქცევის დასჯადი ფორმები, რომლებსაც დღეს

[*] მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის სარედაქციო კოლეგიის წევრი.

პიროვნების დამცველად დავახასიათებდით. არსებობდა ე.წ. „ტაბუ“ და „თავშესაფარი“ - ლათინურად: “Refugium“. ეს უკანასკნელი განმარტებულია, როგორც უკან დახევის ადგილი, მათ შორის ფიზიკური. ძველი აღთქმის ათ მცნებაში მეორე მცნება მოიცავს ე.წ. გამოსახულების აკრძალვას - „არა ჰქმნე თავისა შენისა კერპი!“

2. პერსონალურ მონაცემთა დაცვის ტერმინოლოგია

პერსონალურ მონაცემთა დაცვის ისტორიულ ფესვებზე საუბრის დაწყებამდე საჭიროა მისი ცნების განმარტება. ტერმინი „მონაცემთა დაცვა" ზუსტად ვერ აღწერს მის შინაარსს. ეს სიტყვა ლინგვისტურად თითქოს იმაზე მიუთითებს, რომ საუბარი უშუალოდ მონაცემების დაცვაზეა. თუმცა ეს ტერმინი არაზუსტია, რადგან პერსონალურ მონაცემთა დაცვა მიზნად ისახავს არა თავად მონაცემების, არამედ ამ მონაცემების უკან მდგომი პირის დაცვას. რომ დავრჩეთ თანამედროვე რეალობაში (მაგალითად, კორონავირუსის კრიზისი), აქ საუბარი არაა ტერმინის - „ვაქცინირებული ან გამოჯანმრთელებული“ - დაცვაზე, არამედ ინფორმაციის დაცვაზე - „ბატონი ან ქალბატონი მილერი არის ვაქცინირებული ან გამოჯანმრთელებული“. შესაბამისად, პერსონალურ მონაცემთა დაცვა ეხება ე.წ. პერსონალურ მონაცემებს, ანუ ნებისმიერ ინფორმაციას, რომლითაც შესაძლებელია ფიზიკური პირის იდენტიფიცირება ან რომელიც შეიძლება მას მიეკუთვნოს. პერსონალურ მონაცემთა დაცვის სფეროს გერმანელმა პიონერებმა, ულრიხ ზაიდელმა და ვილჰელმ შტაინმიულერმა, ამ ზუსტ დიფერენციაციაზე ჯერ კიდევ 1970-იან წლებში მიუთითეს, როდესაც პერსონალურ მონაცემთა დაცვის კანონმდებლობა ახალი შექმნილი იყო.

3. საიდუმლოების დაცვიდან პროფესიული კონფიდენციალობის ვალდებულებებამდე და პიროვნების თანამედროვე უფლებამდე

3.1. საწყისი წერტილი: საიდუმლოების დაცვა წინარე მოდერნისტულ ეპოქაში

პირადი ცხოვრების ხელშეხებლობის დაცვა, როგორც სამართლებრივი კატეგორია, თანამედროვე ეპოქის მოვლენაა. ეს კატეგორია მხოლოდ 100 წელია არსებობს. თუმცა მონაცემთა დაცვის საწყისები გაცილებით ძველ დროში, კერძოდ, ქრისტიანობამდელ საიდუმლოების დაცვაში უნდა ვეძიოთ.

იცით თუ არა, რომ მონაცემთა დაცვა ე.წ. „ჰიპოკრატეს ფიცს“ უკავშირდება? ჯერ კიდევ ქრისტეს შობამდე 400 წელს ექიმები იღებდნენ ვალდებულებას, რომ მესამე პირისთვის არ გაემჟღავნებინათ პაციენტის ინტიმური სფეროს საიდუმლოებები. სხვა სიტყვებით რომ ვთქვათ, ეს ეხებოდა სამედიცინო კონფიდენციალობას, რომელიც დღემდე მოქმედებს.

აღიარებული იყო, რომ ადამიანები უფრო მეტს გაამჟღავნებდნენ საკუთარ თავზე და ამით გააადვილებდნენ მკურნალობას, თუ ეცოდინებოდათ, რომ ექიმები მათ საიდუმლოს შეინახავდნენ. ქცევის ეს წესი, რომელიც იმ დროს წმინდა მოვალეობად ითვლებოდა, რელიგიურ და ეთიკურ მოსაზრებებს ეფუძნებოდა.

შუა საუკუნეებიდან ცოდვილი კათოლიკეებიც კი ითვალისწინებდნენ მონაცემთა დაცვას. ეს იმიტომ, რომ ქრისტეს შობიდან 1215 წელს ე.წ. „აღსარების საიდუმლოება“ საეკლესიო კანონში შევიდა. ეს დაადგინეს კათოლიკური ეკლესიის მეთაურებმა იმ დროის ყველაზე მნიშვნელოვან გადაწყვეტილების მიმღებ კრებაზე - ლატერანის მეოთხე საეკლესიო კრებაზე. აღსარების საიდუმლოება ავალდებულებს სასულიერო პირებს, დაიცვან აბსოლუტური საიდუმლოება ყველაფრის შესახებ, რაც მათ აღსარების დროს გაანდეს. თვით აღმსარებელსაც კი არ შეუძლია გაათავისუფლოს თავისი მოძღვარი პირადი ცხოვრების ხელშეუხებლობის ვალდებულებისგან. სასულიერო პირებს, რომლებიც არღვევენ აღსარების საიდუმლოებას, შესაძლოა ემუქრებოდეთ ყველაზე უარესი სასჯელი: ეკლესიიდან განდევნა. აქვე, ერთი საინტერესო დეტალი: კათოლიკური ეკლესიის სააღსარებოებში, ხისგან გამოკვეთილი ვარდი დამსწრეებს აღსარების საიდუმლოებას ახსენებს. ლათინურად: „sub rosa dictum“ — „ის, რაც ვარდის ქვეშ ითქმება, საიდუმლოდ უნდა დარჩეს“.

გერმანიაში საიდუმლოებათა ამ კატეგორიის ყოველ შემთხვევას ასევე მიეკუთვნება კორესპონდენციის, საფოსტო გზავნილებისა და მოგვიანებით ტელეკომუნიკაციის ე.წ. „საიდუმლოება“, ისევე, როგორც გერმანული საგადასახადო საიდუმლოება. ცნობისმოყვარეობა ადამიანური ბუნების ნაწილია, მაგრამ ყოველთვის არ არის სოციალურად მისაღები. მაცნეების მიერ პირადი საქმეებში ცხვირის ჩაყოფის თავიდან ასაცილებლად, 1712 წლის პრუსიის ფოსტის ზოგადმა წესებმა კორესპონდენციის საიდუმლოება ოფიციალურ დაცვას დაუქვემდებარა. ფოსტის თანამშრომლებს, რომლებიც ამ რეგულაციას დაარღვევდნენ, გათავისუფლება და სისხლისსამართლებრივი დევნა ემუქრებოდათ. ზემოხსენებული საიდუმლოებების დაცვა მოგვიანებით გერმანიის კონსტიტუციებმაც განამტკიცეს. დღეს ისინი გერმანიის ძირითადი კანონის მე-10 მუხლითაა რეგულირებული.

თანამედროვე სახელმწიფოს გაჩენასთან ერთად, ის იყენებდა ყველა შესაძლებლობას, რათა სრულყოფილად განეხორციელებინა თავისი ძალაუფლება. ეს ასევე ეხებოდა გადასახადების შეგროვებას: ძველად შეუძლებელი იყო მოქალაქეების იძულება, გაემჟღავნებინათ საგადასახადო მიზნებისთვის რელევანტური მონაცემები. საგადასახადო ორგანოების უფლებამოსილების გასაფართოებლად პარალელურად უნდა გაძლიერებულიყო საიდუმლოების დაცვაც. დღემდე ეს იცავს მოქალაქეების შესახებ ინფორმაციას, რომელიც საგადასახადო წარმოების დროს ხდება ცნობილი. საგადასახადო საიდუმლოება თავდაპირველად მხოლოდ ზოგადი - დაუსჯელი - ოფიციალური საიდუმლოება იყო, მაგრამ მოგვიანებით

სავალდებულო გახდა. დღეს საგადასახადო საიდუმლოებას ფუნდამენტური უფლების მსგავსი მნიშვნელობა აქვს.

3.2. კონფიდენციალურობის ვალდებულებები, როგორც მონაცემთა დაცვის წინარე ფორმა?

გერმანიის ქვემო საქსონიის სასამართლო სისტემაში პერსონალურ მონაცემთა დაცვის ოფიცრობისას, ხშირად მიწევდა მუშაობა სამართლებრივ საკითხზე, რომელიც პირადი ცხოვრების ხელშეუხებლობის დაცვის ვალდებულებასა და პერსონალურ მონაცემთა დაცვას შორის ურთიერთკავშირს ეხებოდა. არის თუ არა პირადი ცხოვრების ხელშეუხებლობის ვალდებულებები პერსონალურ მონაცემთა დაცვის განსაკუთრებული ფორმა, რომელსაც უპირატესობა ენიჭება მონაცემთა დაცვის ზოგად რეგულაციებთან შედარებით? წარმოადგენს თუ არა ის სექტორულ მონაცემთა დაცვის კანონმდებლობას?

ამიტომ ჩნდება კითხვა: წარმოადგენს თუ არა პირადი ცხოვრების ხელშეუხებლობის ვალდებულებები მონაცემთა დაცვის ისტორიულ ფესვებს?

პასუხი ასეთია: მხოლოდ ნაწილობრივ! - საჯარო მოხელეების ზოგად საიდუმლოებას ყოველთვის განსხვავებული მიზანი ჰქონდა. ის არასდროს შექმნილა ინდივიდის დასაცავად, არამედ ყოველთვის ემსახურებოდა სახელმწიფოსა და საჯარო დამსაქმებლის ინტერესების უზრუნველყოფას. შესაბამისად, საჯარო მოხელეების ზოგადი პირადი ცხოვრების ხელშეუხებლობის ვალდებულებები არ იყო მონაცემთა დაცვის წინამორბედი.

პირადი ცხოვრების ხელშეუხებლობის ვალდებულება განსხვავებულად უნდა შეფასდეს, თუ ის ეხება კონკრეტულ პროფესიულ ჯგუფებს: ექიმებს, იურისტებს, ნოტარიუსებს, სოციალურ მუშაკებს, ასევე პერსონალურ მონაცემთა დაცვის ოფიცრებს. ჩემი აზრით, ამ პროფესიული პირადი ცხოვრების ხელშეუხებლობის ვალდებულებებს სამართლიანად ეწოდება პერსონალურ მონაცემთა დაცვის ისტორიული პროტოტიპები.

3.3. პერსონალური მონაცემების დაცვა და პიროვნების უფლებები - თანამედროვე ეპოქა

რაც დრო გადიოდა, თანამედროვე სახელმწიფო სულ უფრო მეტ მონაცემს აგროვებდა საკუთარი მოსახლეობის შესახებ. ამის შესაძლებლობა ტექნოლოგიურმა განვითარებამ მისცა. ძველი არქივები, რომლებიც იმ დროს მოუწესრიგებელი „დოკუმენტების სასაფლაოები“ იყო, რეესტრებმა ჩაანაცვლა. საკუთარი მოსახლეობის შესახებ მონაცემების შეგროვება ახალი არ იყო, როგორც გვახსოვს ბიბლიური საშობაო ამბიდან: ქრისტეს დაბადებას წინ უძღოდა იმპერატორ ავგუსტუსის ბრძანება, რომ „მთელი მსოფლიო აღწერილიყო“. შუა საუკუნეებში, უსაფრთხოებისა და წესრიგის დასაცავად, სისტემატიური ჩანაწერები კეთდებოდა ე.წ. „მოგზაური ხალხის“ შესახებ,

მაგალითად, ნიურნბერგში ჯერ კიდევ 1449 წელს. თუმცა, საინფორმაციო ტექნოლოგიების გაფართოებასთან ერთად, მონაცემთა შეგროვება სულ უფრო და უფრო სრული ხდებოდა: ფართომასშტაბიანი გამოძიებები, ონლაინ ძიებები, ავტომობილის სანომრე ნიშნების ამოცნობა, მონაცემების შენახვა და ა.შ. სახელმწიფო „დიდი ძმა“ (“big brother”) გახდა.

ამჯერად არ მსურს გერმანიაში ნაცისტური დიქტატურის პერიოდზე საუბარი. ეს რეჟიმი მიზნად ისახავდა მოსახლეობის სრულ ზედამხედველობას იმ დროისთვის ხელმისაწვდომი საშუალებებით. ე.წ. კვლევითი ოფისი - გერმანულად: Forschungsamt, რომელიც ჰერმან გერინგს ეკუთვნოდა, ყველა არსებული საიდუმლოების დაცვის ვალდებულებას უგულებელყოფდა. ყოვლისმომცველი ეროვნული მონაცემთა ბაზა უნდა შექმნილიყო ე.წ. გერმანული კოშკის – გერმანულად: “Deutscher Turm“ – სახით. არც იმ მონაცემთა ძალაუფლებაზე მინდა რამის თქმა, რომელსაც ყოფილი გერმანიის დემოკრატიული რესპუბლიკა ახორციელებდა თავის მოსახლეობაზე. ამის ყველაზე თვალსაჩინო ნიშანია ე.წ. “Stasi“ ფაილები, აღმოსავლეთი გერმანიის სახელმწიფო უსაფრთხოების ვრცელი საქმეები. ექსპერტები თანხმდებიან, რომ ორივე პერიოდი მონაცემთა დაცვის ისტორიის პერსპექტივიდან ცალ-ცალკე უნდა განიხილებოდეს.

იმ დრომდე, სანამ მონაცემთა დაცვა სამართლებრივი რეგულაციების საგანი გახდებოდა, რისგან შედგებოდა ის?

პასუხი აშკარაა: მანამდე მონაცემთა დაცვა უბრალოდ მონაცემთა დამუშავების ტექნიკური შეზღუდვებით მიიღწეოდა. მონაცემთა შენახვისა და დამუშავების შესაძლებლობების სიმცირის გამო სახელმწიფოს ხელი ეშლებოდა ყოვლისმომცველი წვდომის მოპოვებაში. არც ნაცისტურ დიქტატურას და არც მოგვიანებით გერმანიის დემოკრატიული რესპუბლიკის სახელმწიფო უსაფრთხოებას არ შეეძლო თავისი მოსახლეობის ეფექტიანად მონიტორინგი, რადგან მათ აკლდათ საინფორმაციო და ადმინისტრაციული ტექნოლოგიები - უნდა ითქვას, მადლობა ღმერთს!

3.3.1. ახალი სამშენებლო მოედანი: მონაცემთა დამუშავება კერძო სუბიექტების მიერ

მე-19 საუკუნის მეორე ნახევრამდე კერძო სუბიექტების მიერ მონაცემთა შეგროვებას დიდი მნიშვნელობა არ ჰქონდა. თუმცა 1840 წლიდან კერძო საკრედიტო და დეტექტივების სააგენტოებმა ე.წ. შავი სიების წარმოება დაიწყეს: 1841 წელს – Dun&Bradstreet ფლორიდაში; 1872 წელს – “Schimmelpfeng“ გერმანიაში; 1879 წელს – “Creditreform“ შვეიცარიაში; 1885 წელს – “Bürgel“ გერმანიაში; 1927 წელს - “SCHUFA“, ზოგადი საკრედიტო დაცვის ასოციაცია – გერმანულად: “Schutzgemeinschaft für allgemeine Kreditsicherung“. ამ პერიოდში დაფუძნებული საკრედიტო სააგენტოების ნაწილი დღესაც არსებობს. შენახვის გაუმჯობესებული ტექნიკები, რომლებიც Leitz-ის სახელს

უკავშირდება - ყველასთვის ცნობილია “Leitz“-ის საქაღალდეები, რომელიც ძალიან კარგი დამხმარე საშუალება იყო.

როგორც კომერციული მოთამაშეები, მედია და პრესაც მოექცა ყურადღების ცენტრში. პიროვნების უფლებების დარღვევამ განაპირობა გერმანიის ხელოვნების საავტორო უფლებების შესახებ კანონის - გერმანულად: “Kunsturheberrechtsgesetz“ – და 1907 წელს საკუთარ გამოსახულებაზე უფლების მიღება. ამის მიზეზი იყო ე.წ. პაპარაცული ფოტო გერმანიის იმპერიის კანცლერის, ოტო ფონ ბისმარკის, გარდაცვალების შემდეგ, გერმანულად: Reichskanzler - Otto von Bismarck: ორმა ფოტოგრაფმა უკანონოდ შეაღწია გარდაცვლილის ოთახში, გადაიღო ის და ფოტოების გამოქვეყნება სცადა. საზოგადოების აღშფოთება დიდი იყო. თუმცა იმ დროის კანონმდებლობით მათ მხოლოდ საცხოვრებელში უკანონო შეღწევისთვის შეეძლოთ პასუხისგება. ამიტომ გადაწყდა, რომ მომავალში გარდაცვლილის ღირსება უკეთ დაცული ყოფილიყო. მას შემდეგ, საკუთარ გამოსახულებაზე უფლებასთან ერთად, გარანტირებულია ე.წ. „პოსტ-მორტემ“ პიროვნების უფლება, რაც სიკვდილის შემდეგ პიროვნების უფლებების დაცვას გულისხმობს.

3.3.2. თანამედროვე პერსონალურ მონაცემთა დაცვის დებატების საწყისი წერტილი ამერიკაში

თუ წარმოიდგენდით, რომ თანამედროვე პერსონალურ მონაცემთა დაცვის ფესვები ამერიკის შეერთებულ შტატებშია? ეს აღსანიშნავია, რადგან დღეს ეს ქვეყანა უკონტროლოდ აგროვებს და ამუშავებს პერსონალურ მონაცემებს. საკმარისია გავიხსენოთ მონაცემთა გადაცემის შესახებ ე.წ. „უსაფრთხო ნავსადგურის“ (“Safe Harbor“) და „პირადი ცხოვრების ხელშეუხებლობის ფარის“ (“Privacy Shield“) შესახებ შეთანხმებები.

ჯერ კიდევ 1890 წელს ამერიკელი იურისტები, როგორებიც იყვნენ სამუელ უორენი და შემდგომში უზენაესი სასამართლოს მოსამართლე ლუის ბრანდეისი, მხარს უჭერდნენ „კონფიდენციალური განმარტოების“ უფლებას. თავიანთ ნოვატორულ ესეში, „პირადი ცხოვრების ხელშეუხებლობის უფლება“ (“The Right to Privacy“), რომელიც ცნობილ “Harvard Law Review“-ში გამოაქვეყნეს, მათ შექმნეს „მარტო დარჩენის უფლება“, როგორც ყოველი ადამიანის ბუნებრივი უფლება. 70 წელზე მეტი ხნის შემდეგ იგივე შეხედულება გამოთქვეს ვენს პაკარდმა თავის 1964 წლის წიგნში „შიშველი საზოგადოება“ (“The Naked Society“) და ალან უესტინმა 1967 წლის ნაშრომში „პირადი ცხოვრების ხელშეუხებლობაა და თავისუფლება“ (“Privacy and Freedom“). ეს პუბლიკაციები შთაგონებული იყო ადამიანების პირადი ცხოვრების ინტიმური დეტალების სულ უფრო ხშირი გამოქვეყნებით, რაც გაზეთების მასობრივი ტირაჟირებისა და ფოტოგრაფიის განვითარების შედეგი იყო. მათ თქვეს, რომ სამართლებრივი დაცვა საჭირო იყო ე.წ. არამატერიალური საკუთრებისთვისაც, როგორიცაა პირადი ცხოვრების ხელშეუხებლობაა. თუმცა

მონაცემთა დაცვის პოლიტიკის შესახებ ეს დებატები ამერიკისთვის ნაადრევი აღმოჩნდა; ამ დისკუსიების პირველი მნიშვნელოვანი შედეგი იყო 1974 წლის პირადი ცხოვრების ხელშეუხებლობის აქტი.

ამერიკის შეერთებულ შტატებში მონაცემთა დაცვის შესახებ დებატებმა გერმანიაში იურისპრუდენციას იმპულსი მისცა!

3.3.3. პერსონალურ მონაცემთა დაცვის „სამშობლო“ პიროვნების ზოგად უფლების კონტექსტში

მაშინ, როცა გერმანიაში, დღევანდელი კონცეფციისგან განსხვავებით, ყურადღება თავდაპირველად გამახვილებული იყო სახელმწიფოსა და კერძო პირების მონაცემებზე ძალაუფლების ობიექტურ-სამართლებრივ შეზღუდვებზე - რაც გულისხმობდა მხოლოდ პროგრამულ დებულებებს, რომლებიც გავლენას ახდენდა სახელმწიფო საქმიანობაზე - ისინი მოგვიანებით ჩანაცვლდა პერსონალურ მონაცემთა დაცვის სუბიექტური უფლებით: პიროვნების ზოგადი უფლებით, როგორც სამართლებრივი კატეგორიით. ვინაიდან ის არც გერმანიის ძირითად კანონში (გერმანულად: “Grundgesetz“) და არც გერმანიის სამოქალაქო კოდექსშია (გერმანულად: “Bürgerliches Gesetzbuch“) მოხსენიებული, 1960-იანი წლების დასაწყისიდან ის სასამართლოების, უპირველეს ყოვლისა კი გერმანიის ფედერალური საკონსტიტუციო სასამართლოს, მიერ შემუშავდა.

4. პერსონალურ მონაცემთა დაცვის კანონმდებლობის დასაწყისი – ჰესენიდან მსოფლიომდე

პერსონალურ მონაცემთა დაცვის გლობალური კანონმდებლობის სამშობლო - და აქ შეგვიძლია, თავი მოვიწონოთ - გერმანია იყო. სწორედ აქ შეიქმნა მსოფლიოში პირველი მონაცემთა დაცვის კანონი, რომელიც ძალაში 1970 წელს შევიდა, ფედერალურ მხარე ჰესენში. ამას მოჰყვა მონაცემთა დაცვის კანონები ბავარიასა და რაინლანდ-პფალცში 1974 წელს.

ეს ყველაფერი იმ დროს მოხდა, როდესაც კომპიუტერები ჯერ კიდევ წიგნის თაროების ზომა იყო და ისეთივე სიმძლავრის, როგორიც დღევანდელი ჯიბის კალკულატორებია. ეს ასევე იყო ის დრო, როდესაც ოპტიკურ-ბოჭკოვანი კაბელი და ტექსტი ტელევიზიის ეკრანზე სიახლეს წარმოადგენდა. თუმცა იმ დროს გერმანიაში უკვე 7,500 ელექტრონული მონაცემთა დამუშავების სისტემა არსებობდა.

შემდეგი ინფორმაცია შესაძლოა განსაკუთრებით საინტერესო იყოს კომპანიაში მომუშავე პერსონალურ მონაცემთა დაცვის სამსახურისთვის: დამოუკიდებელი პერსონალურ მონაცემთა დაცვის ოფიცრის დაარსება ასევე ჰესენური „გამოგონება“ იყო. ჰესენის მონაცემთა დაცვის კანონმა ამისთვის სამართლებრივი საფუძველი შექმნა. მსოფლიოში პირველი მონაცემთა

დაცვის ოფიცერი იყო ვილი ბირკელბახი. ის ჰესენის მხარის მთავრობამ 1971 წელს დანიშნა.

მას შემდეგ, რაც ეს გზა ჰესენის ფედერალურ მხარეში დაიწყო, გერმანიის კანონმდებლები დაახლოებით ექვსი წლის შემდეგ მიჰყვნენ ამ მაგალითს და 1977 წელს მთელი გერმანიისთვის მიიღეს მონაცემთა დაცვის კანონი.

5. 1983 წლის დეკემბერი – გერმანიის ფედერალური საკონსტიტუციო სასამართლოს ე.წ. „აღწერის გადაწყვეტილება“

კარგად მახსოვს გერმანიის ქუჩებში გამართული პროტესტი. იმ დროს სტუდენტი ვიყავი. პროტესტი ეხებოდა სტატისტიკური მონაცემების მოსახლეობის რეესტრებთან დაგეგმილ შედარებას, რაც 1980 წლიდან დაწყებული საყოველთაო აღწერის გზით უნდა გამხდარიყო შესაძლებელი. გერმანული სახელმწიფოს მიმართ პლაკატებზე ეწერა: „ჩვენ ნუ დაგვითვლით, თქვენი დღეები დათვალეთ!“

გერმანიის ფედერალური საკონსტიტუციო სასამართლოს მიერ 1983 წელს მიღებული ე.წ. „აღწერის გადაწყვეტილება“ სენსაცია იყო და გზა გაუხსნა პერსონალურ მონაცემთა დაცვის ფუნდამენტური უფლებების დონეზე აყვანას. ჩემ მიერ უკვე ნახსენები ვილჰელმ შტაინმიულერის წინასწარი ნაშრომების საფუძველზე, მან აღიარა ე.წ. ინფორმაციული თვითგამორკვევის ფუნდამენტური უფლება. ორი რამ იყო ახალი: მას შემდეგ არ არსებობს ადამიანების შესახებ პერსონალური მონაცემები, რომლებიც თავიდანვე არარელევანტურად მიიჩნევა. გარდა ამისა, მონაცემთა ნებისმიერი დამუშავება კანონს ექვემდებარება. დაიბადა მონაცემთა დაცვის სამართლის ახალი გაგება! ამის შემდეგ ეს გადაწყვეტილება „გენიალურ ნაბიჯად“ აღინიშნა მონაცემთა დაცვის სამართალში, არა მხოლოდ გერმანიაში, არამედ საზღვარგარეთაც.

დასასრულს, ნება მიბოძეთ, შემდეგი საკითხი აღვნიშნო: 2006 წლამდე გერმანიის მოქალაქეებს არ ჰქონდათ სამთავრობო დოკუმენტებზე წვდომის ზოგადი უფლება. როგორ შეეძლოთ მათ ესარგებლათ მონაცემთა დაცვის უფლებებით, თუ არც კი იცოდნენ, რა მონაცემებს ინახავდა მათ შესახებ სახელმწიფო ადმინისტრაცია? ეს შეიცვალა ე.წ. ინფორმაციის თავისუფლების შესახებ კანონით – გერმანულად: “Informationsfreiheitsgesetz“. ის გერმანიაში ყველა ადამიანს ანიჭებს უპირობო უფლებას, გაეცნოს ყველა საჯარო დაწესებულების ოფიციალურ ინფორმაციას. მონაცემთა დაცვა და ინფორმაციის თავისუფლება არ არის წინააღმდეგობრივი. როგორც ამბობენ, ისინი ერთი მედლის ორი მხარეა.

6. მონაცემთა დაცვა ევროპაში

შესაძლოა, გაინტერესებთ, როდის გახდა პერსონალურ მონაცემთა დაცვის კანონი ევროპული? სწორედ ამ ევროპულ მონაცემთა დაცვის კანონმდებლობასთან გაქვთ საქმე თქვენ აქ, საქართველოში!

ევროკავშირზე ბევრად ადრე ევროპის საბჭო გახდა სტანდარტების დამდგენი. მისი 1981 წლის კონვენცია (ETS No. 108) მსოფლიოში პირველი საერთაშორისო შეთანხმება იყო მონაცემთა დაცვის სფეროში. თუმცა ის მხოლოდ მინიმალურ სტანდარტებს ადგენს, რაც თავიდანვე იყო მიზანი. ზემოხსენებულ კონვენციას ხელი მოაწერეს ევროპის საბჭოს წევრმა სახელმწიფოებმა 1981 წლის 28 იანვარს. ამიტომაც „მონაცემთა დაცვის საერთაშირისო დღე“ ყოველწლიურად ამ თარიღში აღინიშნება. ეს დღე დღეს არის.

1995 წლიდან ასევე აღსანიშნავია ევროკავშირი. აქ გერმანულმა და ფრანგულმა მაგალითებმა „პრეცედენტი შექმნა“. მას შემდეგ, რაც ევროკავშირი დაარსდა, შიდა საზღვრებს თავისუფლად კვეთდა არა მხოლოდ საქონელი, არამედ პერსონალური მონაცემებიც. ამიტომ საჭირო გახდა მონაცემთა დაცვის ერთიანი მინიმალური დონის დადგენა. ევროკავშირმა მიიღო ე.წ. მონაცემთა დაცვის დირექტივა 95/46/EC 1995 წელს, ხოლო 2002 წელს, რადგან მას სურდა სატელეკომუნიკაციო სექტორში მონაცემთა დაცვის პროცედურული გამოყოფა, მიიღო ე.წ. “e-Privacy“ ან ქუქი-დირექტივა 2002/58/EC. ვფიქრობ, ორივე თქვენთვის ნაცნობია.

მონაცემთა დაცვის სფეროში ბოლო სიტყვა ევროკავშირის ცნობილი მონაცემთა დაცვის ზოგადი რეგულაციაა (“GDPR“), რომელიც ძალაში შევიდა 2018 წელს. სხვათა შორის, დაახლოებით ათი წლით ადრე, ევროპული მონაცემთა დაცვის კანონმდებლობა ფუნდამენტური უფლებების დონეზე იქნა აყვანილი ევროპის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლით, რაც ლოგიკური შუალედური ნაბიჯი იყო. მონაცემთა დაცვის ზოგადი რეგულაცია აწესებს უფრო მკაცრ წესებს პერსონალური მონაცემების დამუშავებისთვის და აძლიერებს მონაცემთა სუბიექტების უფლებებს. საინტერესოა, რომ ეს არ არის დირექტივა, არამედ რეგულაცია და, შესაბამისად, დირექტივისგან განსხვავებით, პირდაპირ მოქმედებს. ბოლო წლების გამოცდილებიდან გამომდინარე, ევროკავშირს დიდი ნდობა აღარ ჰქონდა თავისი წევრი ქვეყნების მიმართ, როდესაც საქმე „მონაცემთა დაცვის სტანდარტების ადაპტირებას“ ეხებოდა.

ამის შემდგომ პერსონალურ მონაცემთა დაცვის სამყაროს შოკურმა ტალღამ გადაუარა. რატომ მოხდა ასე?

გერმანელი მონაცემთა დაცვის აქტივისტები შეძრწუნდნენ, რადგან მათ ეშინოდათ, რომ გერმანიაში უკვე მოქმედი მონაცემთა დაცვის სტანდარტები მნიშვნელოვნად დაიწევდა. ამის საპირისპიროდ, სხვა წევრი ქვეყნები მიიჩნევდნენ, რომ რეგულაცია მონაცემთა დაცვას აბსურდულად მაღალ დონეზე აიყვანდა. სინამდვილეში, ევროკავშირის ზოგიერთ წევრ

სახელმწიფოს სურდა მონაცემთა დაცვის მინიმუმამდე დაყვანა, რათა ეროვნული უპირატესობა მოეპოვებინა. ამ კონტექსტში ჩნდება შემდეგი კითხვა: რომელ წევრ სახელმწიფოში აქვს ყველაზე მეტ საერთაშორისო IT ჯგუფს ევროპული შტაბ-ბინა? გაქვთ რაიმე ვერსია? ირლანდიის რესპუბლიკაში! ამბობენ, რომ იმ დროს სწორედ ამგვარი წევრი სახელმწიფოები იყო განხილვის საგანი. მონაცემთა დაცვის ზოგადი რეგულაცია უმიზეზოდ არ ითვალისწინებს ე.წ. ბაზრის ადგილის პრინციპს, რაც მსგავსი ჯგუფების მიერ მონაცემთა დაცვის აქტიური დარღვევების ჯაჭვზე რეაქცია იყო.

7. ევროპული პერსონალურ მონაცემთა დაცვა - ექსპორტის ჰიტი და გლობალური ტენდენცია

ძალაში შესვლიდან შვიდი წლის შემდეგაც კი პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია ევროპული ეკონომიკებისთვის მნიშვნელოვან გამოწვევად რჩება. ბოლოს და ბოლოს, პერსონალური მონაცემები ეკონომიკური აქტივიც არის! მიუხედავად ამისა, ბევრი ამ რეგულაციას წარმატებულ საექსპორტო პროდუქტად და მონაცემთა დაცვის სფეროში ეგრეთ წოდებულ „ოქროს სტანდარტად“ მიიჩნევს.

აქედან გამომდინარე, გასაგებია, რომ მრავალი მესამე ქვეყანა, მათ შორის ბრაზილია, იაპონია, სამხრეთ კორეა და ასევე საქართველო, ახალ მონაცემთა დაცვის კანონებს იღებენ, რომლებიც ძირითადი რეგულაციის პრინციპებს ეფუძნება. ადაპტაცია ბევრი ქვეყნისთვის მნიშვნელოვანია, რადგან ის მათ საშუალებას აძლევს, მოიპოვონ ევროკომისიის ე.წ. „შესაბამისობის გადაწყვეტილება“ - გადაწყვეტილება მონაცემთა დაცვის დონის შედარების მიზნით, რაც აუცილებელია მონაცემთა გადაცემისთვის. გავიხსენოთ „ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის“ 45-ე მუხლი.

8. დასკვნა

ეს იყო მონაცემთა დაცვის ისტორიის სწრაფი მიმოხილვა. მართალია, მისი თანამედროვე კონცეფცია მხოლოდ ბოლო ათწლეულების განმავლობაში განვითარდა, თუმცა მონაცემთა დაცვა სულ მცირე 2000 წელს ითვლის და იმედი მაქვს, ამის თქვენთვის გადმოცემა შევძელი. მისი ისტორია ეკლესიებს, ომებსა და სახელმწიფოს მიერ ძალაუფლების ბოროტად გამოყენებას უკავშირდება. მოგზაურობა არ დასრულებულა, ის გაგრძელდება! პერსონალურ მონაცემთა დაცვის საკითხები სულ უფრო მნიშვნელოვან როლს შეასრულებს. მონაცემთა დამუშავება გიგანტური ნაბიჯებით მიიწევს წინ. შუა საუკუნეებში აღსარებისას ნათქვამი მოძღვარს, სასულიერო პირს, შესაძლოა სიტყვიერად გაევრცელებინა ან სხვას მოესმინა, მაგრამ მისი მუდმივად

შენახვა და მასობრივად გავრცელება შეუძლებელი იყო. დღევანდელ ციფრულ სამყაროში კი საქმე სხვაგვარადაა.

როგორი გამაღიზიანებელი და ბიუროკრატიულიც არ უნდა იყოს მონაცემთა დაცვა, ზოგჯერ ეს მართლაც „ბოროტად გამოყენებული“ უფლებაა, რომელიც საბოლოოდ შეუცვლელია. ანდაზად ქცეული „პირადი ცხოვრების ხელშეუხებლობის უფლება“, რაც „მარტო დარჩენის უფლებას“ ნიშნავს, მომავალშიც გარანტირებულად უზრუნველყოფილი უნდა იყოს.

ნორბერტ ბერნსდორფი*

საქართველოში პერსონალურ მონაცემთა დაცვის არსებული მდგომარეობა — 2024 წლის კომუნიკაცია ევროკავშირის გაფართოების პოლიტიკის შესახებ**

სტატიაში განხილულია ევროკომისიის მიერ ცოტა ხნის წინ გამოქვეყნებული სამუშაო დოკუმენტის „ანგარიში საქართველოს შესახებ 2024“ ძირითადი მიგნებები, რომლებიც აფასებს ქვეყნის მიერ 2023 წლის დეკემბრის შემდეგ მიღწეულ პროგრესს, მას შემდეგ, რაც ევროპულმა საბჭომ საქართველოს კანდიდატის სტატუსი მიანიჭა. ნაშრომი მიზნად ისახავს, გააანალიზოს ანგარიშში მოცემული ძირითადი მიგნებები და შეფასებები პერსონალურ მონაცემთა დაცვის სამართლებრივი ჩარჩოს ევროკავშირის სამართალთან დაახლოების კუთხით საქართველოს მიერ მიღწეული პროგრესის შესახებ. ამასთანავე, ნაშრომი გვთავაზობს ევროკომისიის დასკვნების სამართლებრივ ანალიზს საქართველოს მიერ პერსონალურ მონაცემთა დაცვის სფეროში ევროპის საბჭოს სამართლებრივ ინსტრუმენტებთან შესაბამისობასთან დაკავშირებით. დაბოლოს, ცალკე თავი ეთმობა საქართველოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ეფექტიანობისა და მისი საზედამხედველო როლის განხილვას პერსონალური მონაცემების დაცვის უზრუნველყოფის ნაწილში.

საკვანძო სიტყვები: *საქართველოს პერსონალურ მონაცემთა დაცვის კანონმდებლობა, პროგრესის ანგარიში, ევროკავშირის სამართალი (acquis), საქართველოს პერსონალურ მონაცემთა დაცვის სამსახური, სამართლებრივი შესაბამისობა.*

---

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, წინამდებარე ჟურნალის სარედაქციო კოლეგიის წევრი.

** პუბლიკაცია წარმოადგენს საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურთან თანამშრომლობის ფარგლებში წარდგენილ მოხსენებას. ის ეძღვნება საქართველოს ევროკავშირში ინტეგრაციის საკითხებს.

1. ამოსავალი წერტილი: „საქართველოს 2024 წლის ანგარიში“

2024 წლის ოქტომბერში ევროკომისიამ („ევროკავშირის კომისია“) წარმოადგინა თავისი სამუშაო დოკუმენტი - „საქართველოს 2024 წლის ანგარიში“[1]. „საქართველოს 2024 წლის ანგარიში“ თან ახლავს ევროკომისიის „2024 წლის კომუნიკაციას ევროკავშირის გაფართოების პოლიტიკის შესახებ“, რომელიც წარედგინება ევროპის პარლამენტს, ევროკავშირის საბჭოს, ევროპის ეკონომიკურ და სოციალურ კომიტეტსა და რეგიონების კომიტეტს. ანგარიში მოიცავს 2023 წლის 15 ივნისიდან 2024 წლის 1 სექტემბრამდე პერიოდს. მე-7 გვერდზე, ნაწილში „ძირითადი მიგნებები“, ევროკომისია მიიჩნევს, რომ მისი 2023 წლის რეკომენდაციები არ შესრულებულა და კვლავ რჩება ძალაში. 2025 წლისთვის ის საქართველოს აძლევს რეკომენდაციას, რომ „მოახდინოს პერსონალურ მონაცემთა დაცვის სამართლებრივი ჩარჩოს დაახლოება ევროკავშირის სამართალთან (acquis): რეგულაციასა (EU) 2016/679 და დირექტივასთან (EU) 2016/680.“ ანგარიშის 41-ე გვერდზე, სათაურით „თავი 23: მართლმსაჯულება და ფუნდამენტური უფლებები“, ევროკომისია აცხადებს, რომ, „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მიღების მიუხედავად, საქართველოში პერსონალურ მონაცემთა დაცვა სრულად არ არის შესაბამისობაში ევროკავშირის შესაბამის მეორად კანონმდებლობასთან[2] და რომ საქართველოს ჯერ კიდევ არ აქვს ხელი მოწერილი ევროპის საბჭოს 1981 წლის 28 იანვრის კონვენციაზე - პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, მის მოდერნიზებულ ვერსიაზე[3]. ევროკომისია ადასტურებს, რომ პერსონალურ მონაცემთა დაცვის სამსახური (“PDPS”) „ზოგადად დამაკმაყოფილებლად ახორციელებს მონაცემთა დამუშავებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ცენტრალურ ბაზაში განხორციელებული საქმიანობის კანონიერების მონიტორინგს“; თუმცა “PDPS”-მა უფრო აქტიური როლი უნდა შეასრულოს, განსაკუთრებით ფარული საგამოძიებო მოქმედებების მონიტორინგის ნაწილში. ევროკომისია ეყრდნობა 2022 და 2023 წლების სტატისტიკურ მონაცემებს, რომლებიც თავად “PDPS”-ის მიერ იქნა მოწოდებული.

[1] Brussels, 30 October 2024, SWD(2024) 697 final.

[2] ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების და 95/46/EC დირექტივის გაუქმების შესახებ („პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია“), OJ L 119, 2016 წლის 4 მაისი, გვ. 1 და შემდგომი; ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 კომპეტენტური ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის, ანდა სისხლისსამართლებრივი სასჯელის აღსრულების მიზნებისთვის პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების და საბჭოს 2008/977/JHA ჩარჩო გადაწყვეტილების გაუქმების შესახებ, OJ L 119, 2016 წლის 4 მაისი, გვ. 89 და შემდგომი.

[3] Basic document: European Treaty Series – No. 108.

სათაურით „თავი 10: ციფრული ტრანსფორმაცია და მედია“, ევროკომისია თავისი ანგარიშის 73-ე გვერდზე უკმაყოფილებას გამოთქვამს იმასთან დაკავშირებით, რომ ციფრული სერვისების სფეროში საქართველოს ეროვნული კანონმდებლობა მხოლოდ ნაწილობრივ არის დაახლოებული ევროპარლამენტისა და საბჭოს 2019 წლის 20 ივნისის დირექტივასთან (EU) 2019/1024 ღია მონაცემებისა და საჯარო სექტორის ინფორმაციის[4] ხელახლა გამოყენების შესახებ. ის ასევე ანალოგიურ უკმაყოფილებას გამოთქვამს ევროკავშირის სხვა, უფრო ახალ, მეორად კანონმდებლობასთან მიმართებით[5]. „ანგარიში საქართველოს შესახებ 2024-ის“ მომზადებისას ევროკომისია იყენებს „ახალ მეთოდს“, რომელიც 2020 წლის თებერვალში გაწევრიანების შესახებ მოლაპარაკებების წარმართვისთვის შემუშავდა. ეს მეთოდი მოლაპარაკებების ცალკეული თავების თემატურ კლასტერებად დაჯგუფებას გულისხმობს. ამ კონტექსტში მოლაპარაკებების 23-ე თავის — „მართლმსაჯულება და ფუნდამენტური უფლებები“ მოთხოვნებთან შესაბამისობა განსაკუთრებით მკაცრად კონტროლდება.

2. ზოგადი და დაუსაბუთებელი სამართლებრივი კრიტიკის დილემა

„საქართველოს 2024 წლის ანგარიში“-ს დოკუმენტში ევროკომისია რეგულარულად ვერ წარმოადგენს კონკრეტულ მტკიცებულებებს თავისი დასკვნების გასამყარებლად, მათ შორის, საქართველოში პერსონალურ მონაცემთა დაცვის „არსებული მდგომარეობის“ შეფასებისას. ამის ნაცვლად, ის მე-4 გვერდზე, მე-2 სქოლიოში, იძლევა შემდეგ ზოგად მითითებას:

„ის (ეს ანგარიში) ეფუძნება სხვადასხვა წყაროდან მიღებულ ინფორმაციას, მათ შორის, საქართველოს, ევროკავშირის წევრი სახელმწიფოების, ევროპარლამენტის ანგარიშებიდან და სხვადასხვა საერთაშორისო და არასამთავრობო ორგანიზაციიდან მიღებულ მონაცემებს. ის ასევე მოიცავს სხვა დაინტერესებული მხარეების მიერ შემუშავებული შედარებითი შეფასებებისა და ინდექსების შედეგებს, განსაკუთრებით კანონის უზენაესობის სფეროში.“

რა თქმა უნდა, არსებობს ტექნიკური შეზღუდვები იმ ანგარიშისთვის კონკრეტული მტკიცებულებების წარმოდგენისას, რომლებიც 30-ზე მეტ მოლაპარაკების თავსა და ექვს კლასტერში რეფორმების მიმდინარე მდგომარეობას ეხება. მიუხედავად ამისა, ზოგადი და დაუსაბუთებელი სამართლებრივი კრიტიკა, კონკრეტული მაგალითებისა და მტკიცებულებების

[4] OJ L 172, 26 June 2019, pp. 56 et seq.

[5] General Data Protection Regulation, OJ L 119, 4 May 2016, 1 et seq.; Regulation (EU) of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ("Digital Services Act"), OJ L 277, 27 October 2022, pp. 1 et seq.; Regulation (EU) of the European Parliament and of the Council of September 14, 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 ("Digital Markets Act"), OJ L 265, 12 October 2022, pp. 1 et seq.

გარეშე, რთულად გასაგებია და გაკრიტიკებულ ინსტიტუტებს გაუმჯობესების შესაძლებლობას არ უტოვებს.

ობიექტური სამართლებრივი კრიტიკის ერთ-ერთი ძირითადი მოთხოვნაა, ნათლად ჩამოაყალიბოს ის წინაპირობები, რომლებსაც კრიტიკა ემყარება. ის უნდა იყოს შემოწმებადი, დასაბუთებული და მოიცავდეს როგორც დადებით, ისე უარყოფით ასპექტებს. სამართლებრივი კრიტიკის ძირითადი ფუნქციაა ხარვეზების, შეცდომებისა და წინააღმდეგობების მეთოდური იდენტიფიცირება პრაქტიკული პროცედურებისა და პირობების გაუმჯობესების მიზნით. კანონის ზოგადი და დაუსაბუთებელი კრიტიკა რამდენიმე პრობლემას ქმნის. უპირველეს ყოვლისა, მან შეიძლება გამოიწვიოს თანამშრომლობის შემცირება, რადგან ის არ არის კონსტრუქციული და არ გვთავაზობს გაუმჯობესების გზებს. მას ასევე შეუძლია შეარყიოს ნდობა გამკრიტიკებელი ინსტიტუტის — ამ შემთხვევაში ევროკომისიის - მიმართ და შექმნას ნეგატიური ატმოსფერო. ზოგადმა კრიტიკამ, მათი გადაჭრის ნაცვლად, შეიძლება „დაფაროს“ რეალური პრობლემები. კანონის კონსტრუქციული კრიტიკა შეიძლება ამოვიცნოთ შემდეგი მახასიათებლებით: მას მოჰყავს კონკრეტული მტკიცებულებები გაკრიტიკებული ქმედებისათვის და გვთავაზობს ცვლილებების კონსტრუქციულ გზებს. ის მიზნად ისახავს ვითარების გაუმჯობესებას. ფორმალური თვალსაზრისით, ის პატივისცემითა და დაფასებით უნდა იყოს გამოხატული.

სამწუხაროდ, „საქართველოს 2024 წლის ანგარიში“ 41-ე და 73-ე გვერდებზე ვერ აკმაყოფილებს საქართველოს პერსონალურ მონაცემთა დაცვის კანონმდებლობისა და მისი აღმსრულებელი ინსტიტუტის “PDPS”-ის მიმართ ასეთი პოზიტიური მიდგომის კრიტერიუმებს - მათ შორის ატმოსფეროს თვალსაზრისითაც – შემდეგი მიზეზების გამო:

3. ევროპის საბჭოს მოდერნიზებული 108-ე კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“

108-ე კონვენციის თავდაპირველი ვერსია ხელმოსაწერად 1981 წლის 28 იანვარს გაიხსნა და ის იყო პირველი იურიდიულად სავალდებულო საერთაშორისო ხელშეკრულება, რომელმაც მონაცემთა დაცვის პრინციპები დაადგინა. 2001 წელს მას დამატებითი ოქმი დაემატა. უკვე გარკვეული ხანია, 108-ე კონვენციის მოდერნიზებული ვერსია რატიფიკაციისთვის ხელმისაწვდომია. ეს „108+ კონვენცია“ ძალაში შევა, როდესაც ევროპის საბჭოს 38 წევრი სახელმწიფო მოახდენს მის რატიფიცირებას.

გასაგებია, რომ ევროკომისია თავის ანგარიშში მოუწოდებს საქართველოს, ხელი მოაწეროს (და შემდგომში მოახდინოს რატიფიცირება) ევროპის საბჭოს 1981 წლის 28 იანვრის კონვენციას „პერსონალური

მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“, მის მოდერნიზებულ ვერსიას. საქართველოს მიერ 108+ კონვენციის რატიფიცირებით, მისი ძალაში შესვლა საბოლოოდ ერთი ნაბიჯით კიდევ უფრო დაახლოებაა.

თუმცა ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) – თავისი გადაწყვეტილებებით – დიდი ხანია, რაც იკისრა ცენტრალური გადაწყვეტილების მიმღები ორგანოს როლი ევროპის საბჭოს წევრი სახელმწიფოებისთვის მონაცემთა დაცვის საკითხებზე. ის დამხმარე საშუალებად იყენებს 108-ე კონვენციას თავისი განმარტებებით. მიუხედავად ამისა, 1987 წლიდან პერსონალურ მონაცემთა დაცვის უფლება დამოუკიდებლად და გადამწყვეტად მომდინარეობს ადამიანის უფლებებიდან, რომლებიც გათვალისწინებულია ადამიანის უფლებათა ევროპული კონვენციით (“ECHR”), კერძოდ, კონვენციის მე-8 მუხლიდან („პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და კორესპონდენციის დაცვის უფლება“), რადგან “ECtHR” გადაწყვეტილებას იღებს არა უშუალოდ 108-ე კონვენციის, არამედ “ECHR”-ით გათვალისწინებული ადამიანის უფლებების საფუძველზე. 108-ე კონვენციის სამართლებრივი მნიშვნელობა „უკანა მხარეს გადადის“. ამასთანავე, ეს საერთაშორისო ხელშეკრულება კვლავაც მხოლოდ ზოგად პრინციპებს ადგენს პერსონალურ მონაცემთა დაცვისთვის, როგორებიცაა დამუშავების სამართლებრივი საფუძვლის ქონის საჭიროება, დამუშავების გამჭვირვალობა, ინფორმაციისა და შესწორების უფლება და კონტროლის მექანიზმების შექმნა.

1987 წლის საქმეზე „ლეანდერი შვედეთის წინააღმდეგ“[6] მიღებული გადაწყვეტილების შემდეგ, რომელშიც “ECtHR”-მა პირველად გააანალიზა საჯარო ორგანოს მიერ ფიზიკური პირის პერსონალური მონაცემების შენახვის საკითხი, ამ სფეროში სასამართლო პრაქტიკა მნიშვნელოვნად განვითარდა. წლების განმავლობაში სასამართლომ განიხილა მრავალი სიტუაცია, რომლებშიც ამ საკითხთის მიმართ კითხვები დაისვა. ფართო სპექტრი პერსონალურ მონაცემებთან დაკავშირებული ოპერაციებისა, როგორებიცაა ასეთი მონაცემების შეგროვება, შენახვა, გამოყენება და გავრცელება, ახლა უკვე “ECtHR”-ის პრეცედენტული სამართლის კორპუსით რეგულირდება. ეს სასამართლო პრაქტიკა საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სწრაფი ევოლუციის პარალელურად განვითარდა.

პერსონალურ მონაცემთა დაცვის უფლება არ არის ავტონომიური უფლება “ECHR”-ით გათვალისწინებულ სხვადასხვა უფლებასა და თავისუფლებას შორის. მიუხედავად ამისა, სასამართლომ აღიარა, რომ პერსონალურ მონაცემთა დაცვას ფუნდამენტური მნიშვნელობა აქვს პირის მიერ “ECHR”-ის მე-8 მუხლით გარანტირებული პირადი და ოჯახური ცხოვრების, საცხოვრისისა

[6] ECtHR, Case of *Leander v. Sweden*, Application no. 9248/81, hudoc.

და მიმოწერის პატივისცემის უფლებით სარგებლობისთვის[7]. ეს მუხლი არის მთავარი ვექტორი, რომლის მეშვეობითაც ხდება პერსონალური მონაცემების დაცვა "ECHR"-ის სისტემაში, თუმცა ამ დაცვასთან დაკავშირებული მოსაზრებები შეიძლება ECHR-ისა და მისი ოქმების სხვა დებულებების ფარგლებშიც იქნას გათვალისწინებული.

შედეგად, საქართველოს უკვე არ შეუძლია თავი აარიდოს ევროპის საბჭოს მიერ მონაცემთა დაცვის სფეროში დადგენილ სამართლებრივ სტანდარტებს. მიუხედავად იმისა, მოაწერს თუ არა ხელს (და შემდგომში მოახდენს თუ არა რატიფიცირებას) 108+ კონვენციას, საქართველო უკვე ვალდებულია, იხელმძღვანელოს "ECtHR"-ის მიერ მონაცემთა დაცვის სფეროში დადგენილი პრეცედენტული სამართლით, რაც ნიშნავს, რომ 108+ კონვენციის „მიღებას" მაქსიმუმ დამატებითი ხასიათი ექნება.

4. პერსონალურ მონაცემთა დაცვის ძირითად რეგულაციასთან, ციფრული სერვისების აქტთან და ციფრული ბაზრების აქტთან დაახლოება

„საქართველოს 2024 წლის ანგარიში"-ის 73-ე გვერდზე ევროკომისია არ განმარტავს, თუ რატომ მიიჩნევს, რომ ხსენებული სამი სამართლებრივი აქტი - რომლებიც ევროკავშირის რეგულაციებს წარმოადგენს („რეგულაცია", „აქტები") - გაწევრიანებამდე საქართველოსგან მოითხოვდა პერსონალურ მონაცემთა დაცვის კანონმდებლობის დაახლოებას. სამართლებრივი თვალსაზრისით, ევროკავშირის დირექტივები წევრი სახელმწიფოებისთვის მხოლოდ მისაღწევი შედეგის დადგენით შემოიფარგლება. ამ შედეგის მიღწევის გზებს თავად წევრი სახელმწიფოები განსაზღვრავენ; მათ დირექტივების იმპლემენტაცია გარკვეულ ვადებში, საკუთარი ეროვნული კანონმდებლობის მეშვეობით უნდა უზრუნველყონ. ამის საპირისპიროდ, ევროკავშირის რეგულაციები პირდაპირ და დაუყოვნებლივ სავალდებულოა ყველა წევრი სახელმწიფოსთვის და არა მხოლოდ მისაღწევ შედეგთან მიმართებით, როგორც ეს დირექტივის შემთხვევაშია. როგორც წესი, ევროკავშირის რეგულაციები არ საჭიროებს ეროვნულ კანონმდებლობაში გადმოტანას (ტრანსპოზიციას).

ევროკავშირში გაწევრიანებისას ევროკავშირის კანონმდებლობის მიღება - ცნობილი როგორც „მიღება" ან „გადასვლა" - ავტომატური პროცესია[8]. ამის ტექნიკური ინსტრუმენტი კანდიდატი ქვეყნის „გაწევრიანებაა". ეს ხორციელდება ევროკავშირის ყველა სხვა წევრ სახელმწიფოსთან (საერთაშორისო) გაწევრიანების შეთანხმების მეშვეობით. გაწევრიანების დღიდან კანდიდატი ქვეყანა ხდება ევროკავშირის ყველა ხელშეკრულების

[7] ECtHR, Case of *Z v. Finland*, Application no. 22009/93, hudoc; Case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, hudoc; Case of *L.B. v. Hungary*, Application no. 36345/16, hudoc.

[8] იხ.: *Bernsdorff N.,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, 13 et seq.

მხარე, მათი მოქმედი რედაქციით. ამ ხელშეკრულებების საფუძველზე გაწევრიანების თარიღამდე მიღებული ევროკავშირის მთელი კანონმდებლობა ავტომატურად ხდება სავალდებულო გაწევრიანებული სახელმწიფოსთვის. მას უპირატესი იურიდიული ძალა აქვს ნებისმიერ ეროვნულ კანონთან შედარებით. ევროკავშირის მონაცემთა დაცვის კანონმდებლობისთვის ეს ნიშნავს, რომ გაწევრიანებისთანავე ისიც ავტომატურად ხდება ეროვნული სამართლებრივი სისტემის ნაწილი, როგორც პირველადი სამართალი. ის „ინერგება“ ეროვნულ სამართლებრივ წესრიგში.

ამ ფონზე ევროკომისიამ ვერ განმარტა, თუ რატომ მოეთხოვება კანდიდატ ქვეყანას, საქართველოს, ევროკავშირის არსებული წევრი სახელმწიფოებისგან განსხვავებით, გაწევრიანებამდე „ჩაანაცვლოს“ ზემოხსენებული ევროკავშირის რეგულაციების შინაარსი თავის ეროვნულ მონაცემთა დაცვის კანონმდებლობაში, ანუ, „წინასწარ გაითვალისწინოს“ ევროკავშირის რეგულაციები გაწევრიანებამდეც კი. თუ ევროკავშირის რეგულაციები ასევე მოითხოვს ეროვნულ კანონმდებლობაში მინიმალური დონის „ხელსაყრელი გარემოს“ შექმნას, სასურველი იქნებოდა ამ „ხელსაყრელი გარემოს“ შესახებ შესაბამისი განმარტებებისა და მისი მონახაზის წარმოდგენა.

თუმცა, რომც არსებობდეს ციფრული სერვისების აქტის საქართველოს ეროვნულ მონაცემთა დაცვის კანონმდებლობაში „ჩანაცვლების“, ან სულ მცირე, უფრო მეტად ასახვის საჭიროება, 2024 წლის ივნისში “TAIEX”-ის სამუშაო შეხვედრის შედეგების ცოდნის გარეშე გაუგებარი იქნებოდა, თუ სად და რა კუთხით უნდა განხორციელებულიყო შემდგომი დაახლოება 2024 წლის სექტემბრამდე:

ევროკავშირის ციფრული სერვისების აქტი ქმნის ონლაინ სერვისებისთვის წესების ერთიან ჩარჩოს უსაფრთხო ციფრული გარემოს ხელშეწყობისა და მომხმარებელთა დაცვის მიზნით[9]. ძირითადი ასპექტები მოიცავს უფრო მკაცრ ვალდებულებებს ონლაინ პლატფორმებისთვის, როგორებიცაა სოციალური ქსელები და სავაჭრო პლატფორმები, კონტენტის მოდერაციისა და მომხმარებელთა საჩივრების განხილვის კუთხით. ციფრული სერვისების აქტი ითხოვს მეტ გამჭვირვალობას მოდერაციის პროცესებსა და რეკლამასთან დაკავშირებით, შეიცავს ზომებს სიძულვილის ენისა და დეზინფორმაციის წინააღმდეგ და აძლიერებს არასრულწლოვანთა დაცვას. ძალიან დიდ პლატფორმებზე უფრო მკაცრი წესები ვრცელდება.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ვრცელი დებულებების გათვალისწინებითა და მისი მოქმედების სფეროსთან (მე-2 მუხლი) დაკავშირებით, გაუგებარია, რატომ არ ავალდებულებს კანონი ონლაინ შუამავლებს, როგორებიცაა ონლაინ პლატფორმები, სოციალური ქსელები, სავაჭრო პლატფორმები და აპლიკაციების მაღაზიები, აიღონ

[9] *დამატებით იხ.: Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, 7 et seq.

პასუხისმგებლობა უკანონო კონტენტზე. ასევე, საჭიროებს განმარტებას, თუ რატომ არ არის კანონის III თავში („მონაცემთა სუბიექტის უფლებები“) მოცემული საჩივრის მექანიზმები საკმარისი პლატფორმის ოპერატორების მიერ მიღებული გადაწყვეტილებების წინააღმდეგ სამართლებრივი ზომების მისაღებად. დაბოლოს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი შეიცავს მრავალ დებულებას მონაცემთა დამუშავებაზე პასუხისმგებელ პირებისა და დამუშავებაზე უფლებამოსილი პირების ვალდებულებების შესახებ (23-ე მუხლი და შემდგომი). “PDPS”-ის მეშვეობით ეროვნული საზედამხედველო ორგანო ახორციელებს მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის მონიტორინგს, მათ შორის, ციფრული სერვისის პროვაიდერების მიერ (49-ე მუხლი და შემდგომი).

ციფრული ბაზრების აქტი არის ევროკავშირის რეგულაცია, რომელიც მიზნად ისახავს ციფრულ ბაზრებზე კონკურენციის ხელშეწყობას დომინანტური საბაზრო პოზიციის მქონე დიდი ონლაინ პლატფორმების, ე.წ. „გეითკიპერების“ (“gatekeepers”), რეგულირებით. მისი მიზანია სამართლიანი პირობების შექმნა და ბაზარზე არსებული ძალაუფლების ბოროტად გამოყენების თავიდან აცილება. ციფრული ბაზრების აქტი კრძალავს ე.წ. „გეითკიპერების“ გარკვეულ ქმედებებს, როგორებიცაა საკუთარი სერვისებისთვის უპირატესობის მინიჭება ან მონაცემთა გადაცემის შეფერხება, და ამის ნაცვლად მოითხოვს მეტ თავსებადობასა და სამართლიან პირობებს.

არც აშკარაა და არც ევროკომისია განმარტავს, სამართლიანი კონკურენციის ინტერესებიდან გამომდინარე, თუ რატომ არ შეიძლება ციფრული ბაზრების აქტით ე.წ. „გეითკიპერებისთვის“ დაწესებული „ნებადართული“ და „აკრძალული“ ქმედებები აღსრულდეს საქართველოს მონაცემთა დაცვის კანონმდებლობის ჩვეულებრივი ინსტრუმენტებით (მე-13 მუხლი და შემდგომი, მე-18 მუხლი, 64-ე მუხლი, X თავი). მომხმარებლებისთვის მესამე მხარის ციფრული სერვისებით სარგებლობის შეზღუდვა ასევე შეიძლება აიკრძალოს საქართველოს მონაცემთა დაცვის კანონმდებლობით და ე.წ. „გეითკიპერებს“ კონფლიქტის შემთხვევაში შეიძლება მოეთხოვოთ გარკვეული კომპიუტერული აპლიკაციების ან პროგრამული უზრუნველყოფის დეინსტალაცია.

რაც შეეხება „ევროკავშირის პერსონალურ მონაცემთა დაცვის ძირითად რეგულაციას“, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დებულებები უკვე ძალიან ახლოსაა მის მოთხოვნებთან[10]. კანონი ითვალისწინებს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაციის ბევრ პრინციპს, მათ შორის: მონაცემთა სუბიექტის უფლებებს, გამჭვირვალობას, უსაფრთხოების ვალდებულებებსა და მონაცემთა დარღვევის შესახებ შეტყობინებებს.

[10] იხ.: *Bernsdorff N.,* the New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, 101 et seq.

5. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ეფექტიანი ზედამხედველობის განხორციელება

მონაცემთა დაცვის საზედამხედველო ორგანოებს, როგორც წესი, უწევთ პასუხის გაცემა მონაცემთა დაცვის ყველა სფეროდან, ყველა ინდუსტრიის მასშტაბით დასმულ შეკითხვებზე, აგრეთვე, ე.წ. „ჯვარედინი შემოწმებების“ ფარგლებში. იქ, სადაც მათ შეუძლიათ ნდობა გამოუცხადონ პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს, ნაკლები ზედამხედველობაა საჭირო, ხოლო სხვა სფეროებში რეგულარულად უნდა განხორციელდეს მიზნობრივი შემოწმებები. ამ სფეროში ყოველთვის არსებობს კონსულტაციისა და ცნობიერების ამაღლების დიდი საჭიროება. მონაცემთა დაცვასთან შესაბამისობის შემოწმებისას ყველა საკითხი ყოველთვის თანაბრად რელევანტური არ არის. არ არსებობს მონაცემთა დაცვის „მზა“ გადაწყვეტილებები; მონაცემთა დაცვის საზედამხედველო ორგანოების მიერ გამოყენებული ზომები უნდა შეესაბამებოდეს იდენტიფიცირებულ კონკრეტულ რისკს მონაცემთა დაცვის სფეროში. ასეთი ზომების მიღებამდე ასევე უნდა განხორციელდეს გავლენის შეფასება. ამ ფონზე თითქმის შეუძლებელია შეფასდეს მონაცემთა დაცვის საზედამხედველო ორგანოები – და, შესაბამისად, საქართველოს “PDPS” – აქტიურად მართავენ თუ არა მონაცემებს და ახორციელებენ თუ არა მონაცემთა დაცვის ეფექტიან კონცეფციას.

ნამდვილად არ არის დამაჯერებელი, რომ აქტივობის გასაზომად (და მომავალი პროგნოზების საფუძვლად) რამდენიმე წლის (2022, 2023) განმავლობაში „საქმეთა რაოდენობის“ არათანაბარი მაჩვენებლების გამოყენება, როგორც ეს ევროკომისიამ გააკეთა „საქართველოს შესახებ 2024 წლის ანგარიშის“ 41-ე გვერდზე დართულ გრაფიკზე. ეს გრაფიკი ყველა მიმართულებით ხაზოვან ზრდას აჩვენებს. “PDPS”-ის 2025 წლის პირველი ექვსი თვის[11] საქმიანობის შესახებ „სპეციალური ანგარიშის“ გათვალისწინებით, ევროკომისიის მოსაზრება, რომ “PDPS”-მა ამ მიმართულებით „უფრო აქტიური როლი“ უნდა შეასრულოს, არ ჩანს დასაბუთებული. 2025 წლის პირველ ნახევარში ინსპექტირებების/შემოწმებების რაოდენობა 155 იყო. მისივე სტატისტიკის მიხედვით, “PDPS”-მა 496 განცხადება/შეტყობინება მიიღო. სამსახურმა 278 ადმინისტრაციული სამართალდარღვევა გამოავლინა და 277 შემთხვევაში ადმინისტრაციული სახდელი გამოიყენა. გაიცა 369 დავალება და რეკომენდაცია. ასევე აღსანიშნავია “PDPS”-ის საერთაშორისო საქმიანობა,

[11] საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის 2025 წლის 6 თვის სტატისტიკა /იანვარი-ივნისი.

რომლის შესახებაც მან სხვა „სპეციალურ ანგარიშში“[12] ისაუბრა. “PDPS”-ის 2025 წლის პირველი ექვსი თვის საქმიანობის შესახებ „სპეციალურ ანგარიშში“ აღწერილი ფარული საგამოძიებო მოქმედებების[13] მონიტორინგის სფეროში განხორციელებული მრავალრიცხოვანი შემოწმებების გათვალისწინებით, რომელთა განხორციელებაც “PDPS”-ს ევალება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის VII თავის შესაბამისად, გაუგებარია, თუ რატომ არსებობს, ევროკომისიის აზრით, ამ სფეროში კვლავ გაძლიერებული მოქმედების საჭიროება.

ბიბლიოგრაფია:

1. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 სისხლისსამართლებრივი დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის, ან სისხლისსამართლებრივი სასჯელის აღსრულების მიზნებისთვის კომპეტენტური ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, ასეთი მონაცემების თავისუფალი გადაადგილებისა და საბჭოს 2008/977/JHA ჩარჩო-გადაწყვეტილების გაუქმების თაობაზე.
2. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების შესახებ და 95/46/EC დირექტივის გაუქმების თაობაზე („პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია“).
3. ევროპის საბჭო, კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ (108-ე კონვენცია), ევროპულ ხელშეკრულებათა სერია №108 (1981).
4. სამსახურის მიერ 2022-2024 წლებში განხორციელებული საერთაშორისო აქტივობები პერსონალურ მონაცემთა დაცვის კანონმდებლობის საუკეთესო ევროპული პრაქტიკისა და სტანდარტების იმპლემენტაციის მიზნით.
5. საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის 2025 წლის 6 თვის (იანვარი-ივნისი) საქმიანობის სტატისტიკა, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახური.
6. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and

[12] სამსახურის მიერ 2022-2024 წლებში განხორციელებული საერთაშორისო აქტივობები პერსონალურ მონაცემთა დაცვის კანონმდებლობის საუკეთესო ევროპული პრაქტიკისა და სტანდარტების იმპლემენტაციის მიზნით.
[13] იქვე, 8-11.

amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
8. *Bernsdorff N.,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, 13 et seq.
9. *Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, 7 et seq.
10. *Bernsdorff N.,* the New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, 101 et seq.
11. Case of *L.B. v. Hungary*, Application no. 36345/16, hudoc.
12. Case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, hudoc.
13. ECtHR, Case of *Leander v. Sweden*, Application no. 9248/81, hudoc.
14. ECtHR, Case of *Z v. Finland*, Application no. 22009/93, hudoc.
15. European Commission**,** Staff Working Document SWD (2024) *697 final* (Brussels, 30 October 2024).
16. OJ L 119, 4 May 2016, 1 et seq.
17. OJ L 172, 26 June 2019, 56 et seq.

მაქსიმ გენარტი*

პირადი ცხოვრების ხელშეუხებლობა, ეთიკა და თანამშრომლობა: პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების როლი ხელოვნური ინტელექტის განვითარებაში**

უპირველეს ყოვლისა, მინდა მადლობა გადავუხადო საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურს ამ მეტად საინტერესო სამი დღისთვის და ბათუმში თბილი დახვედრისთვის. ასევე, მადლობას ვუხდი მათ შესაძლებლობისთვის, წარვდგე ასეთ გამორჩეულ მომხსენებლებთან ერთად თემაზე: „პირადი ცხოვრების ხელშეუხებლობა, ეთიკა და თანამშრომლობა: პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების როლი ხელოვნური ინტელექტის განვითარებაში“.

მათთვის, ვისთანაც შეხვედრის პატივი არ მქონია, ჩემი სახელია მაქსიმ გენარტი, ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს იურიდიული მრჩეველი და მისი ხელოვნური ინტელექტის სამუშაო ჯგუფის წევრი. მე ამ როლში ჩართული ვარ ხელოვნური ინტელექტის მმართველობის ბელგიის ეროვნული ჩარჩოს ჩამოყალიბებაში და სწორედ ამ თემაზე მინდოდა დღეს თქვენთან საუბარი.

საკვანძო სიტყვები: *პირადი ცხოვრების ხელშეუხებლობა, ეთიკა, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოები, ხელოვნური ინტელექტი (AI), ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება ("Privacy-by-Design“), ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინება (“Ethics-by-design”).*

---

* ბელგიის მონაცემთა დაცვის საზედამხედველო ორგანოს იურიდიული მრჩეველი.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე“) წარდგენილი მოხსენების ტექსტს.

1. შესავალი

წინამდებარე სტატია იკვლევს, თუ როგორ შეუძლიათ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს ("DPA") განავითარონ ხელოვნური ინტელექტი პირადი ცხოვრების ხელშეუხებლობასა და, ზოგადად, ადამიანის უფლებების დაცვის პრინციპების გათვალისწინებით. ამ მიზნით, სტატია, პირველ რიგში, პრაქტიკული მაგალითის გამოყენებით, წარმოაჩენს იმ ტიპის ინტერდისციპლინურ აზროვნებას, რომელსაც ხელოვნური ინტელექტის განვითარება მოითხოვს. შემდეგ სტატია განმარტავს, თუ როგორ წარმოადგენს „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება" (privacy-by-design) — კონცეფცია ღირებულ ინსტრუმენტს ტექნოლოგიების პასუხისმგებლიანი განვითარებისთვის და რატომ უნდა განიხილებოდეს მისი გაფართოება „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინების" ("ethics-by-design") უფრო ფართო ცნებამდე. აქედან გამომდინარე, სტატიაში ხაზგასმულია, თუ რამდენად მნიშვნელოვანია პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების გამოცდილება პრინციპის, „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება", დანერგვის კუთხით, რათა ხელი შეეწყოს ისეთი ჩარჩოს განვითარებას, როგორიცაა „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინება". დაბოლოს, სტატიაში განხილულია, თუ როგორ შეუძლია ხელოვნური ინტელექტის აქტის გარკვეულ დებულებებს, ხელი შეუწყოს კერძო და საჯარო სექტორების თანამშრომლობას ხელოვნური ინტელექტის განვითარების პროცესში, რითაც ის მხარს უჭერს ერთობლივი, წინასაბაზრო ღირებულებების განსაზღვრის იდეას.

2. ინტერდისციპლინური აზროვნება და ხელოვნური ინტელექტის სექტორთაშორისი საკითხები

ხელოვნური ინტელექტის სისტემების მიღმა მდგარი ინტერდისციპლინური აზროვნებისა და მათ მიერ წამოჭრილი სექტორთაშორისი საკითხების საილუსტრაციოდ გადავწყვიტე, მოკლედ გესაუბროთ "Amazon"-ის 2018 წლის ხელოვნურ ინტელექტზე დაფუძნებული თანამშრომელთა შერჩევის ინსტრუმენტის შესახებ.

თანამშრომელთა შერჩევის ეს ექსპერიმენტული მეთოდი იყენებდა ხუთვარსკვლავიან შეფასების სისტემას იმის ალბათობის შესაფასებლად, თუ რამდენად შეძლებდნენ კანდიდატები "Amazon"-ში პროგრამული უზრუნველყოფისა და ტექნიკური მიმართულებით პოზიციების დაკავებას.

ის წლების განმავლობაში იწვრთნებოდა ვრცელი მონაცემთა ბაზების გამოყენებით, რომლებიც შეიცავდა სამუშაო განაცხადებს, რეზიუმეებს ("CV"), სამოტივაციო წერილებს და ა. შ. ხელოვნურ ინტელექტზე დაფუძნებული ინსტრუმენტის მიზანი იყო "Amazon"-ის ტექნიკური და პროგრამული უზრუნველყოფის პოზიციებისთვის საუკეთესო კანდიდატების შერჩევა.

ამ მიზნის მისაღწევად ინსტრუმენტი მონაწილეებს შორის მსგავსებებს პოულობდა და საუკეთესოებს არჩევდა. საყოველთაოდ ცნობილი ფაქტია, რომ კაცები ჭარბად არიან წარმოდგენილი პროგრამული უზრუნველყოფისა და ტექნიკურ სამუშაოებზე და ხელოვნური ინტელექტის სისტემა სწორედ ამ ფაქტზე დაყრდნობით იწვრთნებოდა.

ამის გამო ინსტრუმენტმა დაიწყო მსჯელობის ამ პრეფერენციისკენ გადახრა და მალევე გამოავლინა სექსიზმის ნიშნები, რაც გამოიხატებოდა ქალების რეზიუმეებისთვის ქულების დაწევაში და უპირატესობის მამრობითი სქესის კანდიდატებისთვის მინიჭებაში. საბოლოოდ, და ნაწილობრივ ამ დისკრიმინაციული პრაქტიკის გამო, "Amazon"-მა ეს ინსტრუმენტი გაიწვია.

ამ მაგალითზე დაყრდნობით, უკვე ვხედავთ, თუ როგორ იმოქმედებს ხელოვნური ინტელექტი არაერთ სექტორზე და მოითხოვს სხვადასხვა დისციპლინის ჩართულობას. ამ შემთხვევაში უკვე ნათელია ის საკითხები, რომლებიც უკავშირდება შრომის სამართალს, პირადი ცხოვრების ხელშეუხებლობასა და პერსონალურ მონაცემთა დაცვას, დისკრიმინაციის სამართალს და ტექნიკური ექსპერტების ჩართულობის აუცილებლობას ინსტრუმენტის ადაპტირებისა და მსგავსი მიკერძოებების აღმოსაფხვრელად.

3. „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება" ("Privacy-by-Design"): ძირითადი უფლებების კოლექტიური პასუხისმგებლობა

აღნიშნული მაგალითი ასევე აჩვენებს, რომ ხელოვნური ინტელექტის სისტემები გავლენას მოახდენს ადამიანების ცხოვრებაზე უფრო ფართო საზოგადოებრივ ღირებულებებზე ზემოქმედებით, რომლებიც ტექნიკურმა ექსპერტებმა უნდა დანერგონ.

ეს არ არის პირველი შემთხვევა, როდესაც მსგავს საკითხებს ვაწყდებით. ჩვენ ანალოგიური ფაქტი ვიხილეთ რამდენიმე წლის წინ, პროგნოზირებადი ტექნოლოგიების განვითარების კვალდაკვალ. სნოუდენის მიერ ინფორმაციის გამჟღავნების შემდგომ საზოგადოებამ დაიწყო იმის გაცნობიერება, თუ როგორ გამოიყენებოდა მათი პერსონალური მონაცემები ონლაინ და როგორ ილახებოდა მათი ძირითადი უფლება ტექნოლოგიების დიზაინის მეშვეობით.

ამ საზოგადოებრივმა ცნობიერებამ განაპირობა იმის გააზრება, რომ პირადი ცხოვრების ხელშეუხებლობა და პერსონალურ მონაცემთა დაცვა ვეღარ დაეყრდნობოდა მხოლოდ ინდივიდების მიერ საკუთარ მონაცემებთან დაკავშირებით მიღებულ გადაწყვეტილებებს. ამან გამოიწვია ცნობიერების

ცვლილება, რომლის მიხედვითაც პერსონალურ მონაცემთა დაცვა, მიუხედავად იმისა, რომ ინდივიდებს ეხება, იქცა კოლექტიურ პასუხისმგებლობად, რომელიც საჭიროებდა ჰოლისტიკურ გააზრებას და ტექნიკური პროფილის სპეციალისტების მიერ დაპროექტების ფაზაშივე განხორციელებას. სწორედ აქედან წარმოიშვა „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინების“ (“privacy-by-design”) კონცეფცია.

ეს გარდატეხა გადამწყვეტი იყო. ამით დაფიქსირდა მოსაზრება, რომ საერთო ღირებულებებთან, როგორებიცაა: პირადი ცხოვრების ხელშეუხებლობა და პერსონალურ მონაცემთა დაცვა, შესაბამისობის მიღწევა ან ხელშეწყობა პროდუქტის პროექტირების ეტაპზე უფრო ეფექტიანია, ვიდრე *ex post* — ფაქტის შემდგომ — აღსრულებისა და გამასწორებელი ზომების მეშვეობით.

ამგვარად, პრონციპის, „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება“, საფუძველი ერთდროულად პრაქტიკულიც არის და ფილოსოფიურიც. იგი ემყარება იმ მოსაზრებას, რომ საინფორმაციო სისტემების არქიტექტურა თავისთავად შეიძლება რეგულირების ერთ-ერთ ფორმად მოგვევლინოს.

4. „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინება“: უნივერსალური ღირებულებების საწყის ეტაპზე ინტეგრირება

დღესდღეობით აღნიშნული ლოგიკა კვლავ სრულად რელევანტურია. როგორც “Amazon”-ის თანამშრომელთა შერჩევის ინსტრუმენტის მაგალითმა გვიჩვენა, ხელოვნური ინტელექტის სისტემები ძირითადი ღირებულებებისთვის გამოწვევებს ქმნიან, რომლებიც სექტორთაშორის დონეზე უნდა გადაიჭრას.

თუმცა, „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება“, როგორც მისი სახელიც მიუთითებს, პირადი ცხოვრების ხელშეუხებლობის დაცვას ეხება — ერთ-ერთ ძირითად უფლებას მრავალ სხვას შორის. შესაბამისად, „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება“ თავისთავად უკვე საკმარისი არ არის. სწორედ აქ შემოდის „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინების“ (“ethics-by-design”) კონცეფცია. იგი გულისხმობს ხელოვნური ინტელექტის სისტემის დიზაინში ისეთი ღირებულებების ჩანერგვას, რომლებიც მას გადაწყვეტილების მიღების პროცესში უხელმძღვანელებს.

ამ გამოწვევების მასშტაბისა და პოტენციურად შელახული ძირითადი უფლებების რაოდენობის გათვალისწინებით, ლოგიკური ჩანს მცდელობა, რომ ხელოვნური ინტელექტის სისტემების მიერ მიღებულ გადაწყვეტილებებს მივანიჭოთ მნიშვნელობა ან თუნდაც მორალური ღირებულება.

მიუხედავად იმისა, რომ ეს თეორიულად მარტივია, ხელოვნური ინტელექტისთვის ტექნიკურად იმის მითითება, რომ მან წარმოადგინოს საუკეთესო კანდიდატი და ამავდროულად გაითვალისწინოს, რომ ეს პროცესი სქესის ნიშნით არ წარმართოს, რთული და კომპლექსური ამოცანაა, რომელიც სხვადასხვა სფეროს წარმომადგენლების ჩართულობას მოითხოვს.

პრაქტიკულად, ეს ცვლილება მოითხოვს რეაქტიული ტიპის რეგულირებიდან უფრო პროაქტიულზე გადასვლას, ისევე, როგორც „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება“ პრინციპი გვავალდებულებს ვიფიქროთ პირადი ცხოვრების ხელშეუხებლობაზე მონაცემთა დამუშავების საშუალებებისა და მეთოდების განსაზღვრისას, ასევე, იმ ღირებულებებზე, რომლებიც ხელოვნური ინტელექტის სისტემების გადაწყვეტილებებისთვის სახელმძღვანელო პრინციპი იქნება.

5. პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების (“DPA”) გამოცდილების მნიშვნელობა

როგორ შეიძლება დაეხმაროს „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინების“ კონცეფციის შემუშავებასა და დანერგვას ის გამოცდილება, რომელიც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს (“DPA”) „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინების“ პრინციპის განხორციელებისას დაუგროვდათ?

როგორც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს, ჩვენ გვაქვს ინტერესთა დაბალანსების კომპლექსური პროცესების წარმართვის დიდი გამოცდილება. ჩვენ ვაფასებთ მონაცემთა დამუშავების ოპერაციების აუცილებლობასა და პროპორციულობას მრავალ კონტექსტში, რა დროსაც მონაცემთა დაცვის უფლება უპირისპირდება გამოხატვის თავისუფლებას, ინფორმაციის თავისუფლებას, საჯარო ინტერესს და სხვას.

ინტერესთა დაბალანსების პროცესი, რომელსაც ჩვენ ვახორციელებთ, ხშირად მოითხოვს ინტერდისციპლინურ ცოდნას. ჩვენ ვითხოვთ ტექნიკური ექსპერტების ჩართულობას, რათა სრულად გავიაზროთ კონკრეტული დამუშავების ოპერაციის შესაძლო შედეგები. შემდეგ ვიყენებთ საკუთარ იურიდიულ კომპეტენციას, რათა განვსაზღვროთ მოცემული დამუშავებისთვის მოქმედი ვალდებულებები. ამ თანამშრომლობის წყალობით ვადგენთ, ნამდვილად იყო თუ არა პირადი ცხოვრების ხელშეუხებლობა

გათვალისწინებული დამუშავების ოპერაციის დაპროექტების ეტაპზე, თუ ის მოკვლევის ან საჩივრის შემდგომი, დაგვიანებული რეაგირების შედეგი იყო.

ეს უნარები გვაყენებს უნიკალურ მდგომარეობაში, რათა:

- განვსაზღვროთ ხელოვნური ინტელექტის სისტემებით გამოწვეული რისკები;
- ვიაზროვნოთ რაციონალურად და ეთიკურად არსებული უფლებების, ღირებულებებისა და ინტერესების დაბალანსებისას; და
- ვიპოვოთ ლეგიტიმური კომპრომისი ურთიერთსაწინააღმდეგო ღირებულებებს შორის.

შესაბამისად, ხელოვნური ინტელექტის სისტემების რეგულირებისა და „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინების“ პრინციპიდან „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინების“ პრინციპზე პოტენციური გადასვლის პროცესშიჩვენ, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს, გვაქვს საჭირო გამოცდილება, რათა გავაერთიანოთ შესაბამისი ცოდნის მქონე ადამიანები კონკრეტული ტექნოლოგიური გარემოს სირთულეების გააზრების მიზნით და ვცადოთ ისეთი ღირებულების დანერგვა, რომელიც ხელოვნური ინტელექტის სისტემებს მთელი მათი სასიცოცხლო ციკლის განმავლობაში უხელმძღვანელებს.

მაშ, როგორ შეგვიძლია პრაქტიკულად დავიწყოთ ამგვარი ცვლილების ხელშეწყობა და როგორი შეიძლება იყოს ეს ცვლილება?

ამ კითხვის საპასუხოდ დეტალურად განვიხილავ ხუთ სიტუაციას, სადაც ეს ცვლილება შეიძლება გამოვლინდეს. სამი მათგანი ბაზარზე განთავსების შემდგომი მონიტორინგის პრაქტიკას ეხება, ხოლო დანარჩენი ორი — ბაზარზე შესვლამდე ხდება.

6. პოსტ-საბაზრო თანამშრომლობის მექანიზმიდან

პირველ რიგში, მიმაჩნია, რომ “FRIA”[1] წარმოადგენს მაღალი რისკის მქონე ხელოვნური ინტელექტის სისტემების პირველად, *ex-ante* (წინასწარ) შეფასებას და უაღრესად ღირებულია. იგი უბიძგებს დიზაინერებს, შეაფასონ ეთიკური კომპრომისები დაპროექტების ადრეულ ეტაპზე და არა როგორც დაგვიანებული რეაგირება. შესაბამისად, არსებობს შესაძლებლობა, რომ

[1] ფუნდამენტურ უფლებებზე ზემოქმედების შეფასება (FRIA) აქ განხილულია ბაზარზე განთავსების შემდგომი მონიტორინგის კონტექსტში, რადგან ტექსტი დაწერილია სასამართლო დავების პერსპექტივიდან. ვაცნობიერებ, რომ ეს არის კერძო აქტორების მიერ განხორციელებული შიდა, წინასწარი შეფასება. თუმცა, როგორც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოები, ისინი პროცესში მხოლოდ საჩივრის შეტანის შემდეგ ერთვებიან.

ხელოვნური ინტელექტის შემუშავების პროცესში „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინების“ მიდგომა დაინერგოს. პრობლემა, თუ შეიძლება ასე ითქვას, მონაცემთა დაცვაზე ზეგავლენის შეფასების (“DPIA”) მსგავსია და იმაში მდგომარეობს, რომ მას სრულად ახორციელებენ კერძო აქტორები, რომლებიც თავად ქმნიან შეფასების ობიექტტექნოლოგიას.

მეორე, შეგვიძლია განვიხილოთ გაწეული სამუშაო ისეთი საერთაშორისო ორგანიზაციებისა, როგორებიცაა ევროკავშირი, ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (“OECD”), იუნესკო (“UNESCO”) და ა. შ. ეს ინიციატივები თანამშრომლობის შესანიშნავი მაგალითია, რადგან ისინი, როგორც წესი, ითვალისწინებენ როგორც კერძო, ისე საჯარო სექტორის ჩართულობას, რათა ფუნდამენტური უფლებები გარდაიქმნას იმ ღირებულებებად, რომელთა გათვალისწინებაც ხელოვნური ინტელექტის სისტემებს შეიძლება მოეთხოვოთ. თუმცა ეს სტანდარტები არ არის იძულებით აღსრულებადი და მათი დანერგვა სრულად არის მინდობილი კერძო აქტორების დისკრეციაზე.

აქედან უკვე ნათელია, რომ კვლავ არსებობს უზარმაზარი უფსკრული კერძო აქტორებსა (ტექნიკური ექსპერტები და ტექნოლოგიების მწარმოებლები) და საჯარო უწყებებს (ძირითადი უფლებების აღსრულებისა და დანერგვის მიმართულებით მომუშავე ექსპერტები) შორის.

79-ე მუხლის მე-2 პუნქტი უკვე იწყებს ამ უფსკრულის ამოვსებას. ამ მუხლის თანახმად, ბაზარზე ზედამხედველობის ორგანოებმა (“MSA”), რომლებიც ძირითადი უფლების შელახვის რისკს გამოავლენენ, უნდა აცნობონ შესაბამის უწყებას. ამის შემდეგ მათ, აღნიშნული ხელოვნური ინტელექტის სისტემის ოპერატორთან ერთად, უნდა ითანამშრომლონ რისკის აღმოსაფხვრელად. ამ სცენარში არსებობს თანამშრომლობის ვალდებულება კერძო სექტორს, ბაზარზე ზედამხედველობის ორგანოებსა და პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის, რათა მოხდეს ხელოვნური ინტელექტის სისტემის დიზაინის ადაპტირება და უზრუნველყოფილ იქნას პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის ფუნდამენტური უფლების პატივისცემა. თუმცა, შეიძლება ითქვას, რომ ამ შემთხვევაში ჩარევა დაგვიანებულია, რადგან რისკი უკვე იდენტიფიცირებულია და, პოტენციურად, რეალიზებულიც.

თუმცა, ხელოვნური ინტელექტის სისტემების მახასიათებლებისა და იმ რეალური გავლენის გათვალისწინებით, რაც მათ უკვე აქვთ, აუცილებელია, ხელი შეეწყოს თანამშრომლობის ისეთ მექანიზმს, რომელიც მოიცავს ეთიკურ კომპრომისებსა და ღირებულებების განსაზღვრის პროცესს, და რომელიც დაპროექტების ეტაპზევე განხორციელდება როგორც ხელოვნური ინტელექტის სისტემის შემქმნელის, ისე ფუნდამენტური უფლებების დამცველი უწყებების ჩართულობით.

იმის საჩვენებლად, რომ წინასაბაზრო, ღირებულებების განსაზღვრაზე დაფუძნებული თანამშრომლობის მექანიზმი პრაქტიკაში განხორციელებადია,

მსურს, თქვენი ყურადღება ხელოვნური ინტელექტის აქტის ორ დებულებაზე გავამახვილო.

7. წინასაბაზრო ღირებულებების განსაზღვრაზე დაფუძნებული თანამშრომლობა

პირველი დებულება ეხება ხელოვნური ინტელექტის აქტის (“AIA”) 57-ე მუხლით გათვალისწინებულ „რეგულაციურ სენდბოქსებს“ (“regulatory sandboxes”). მუხლი განმარტავს, რომ წევრ სახელმწიფოებს სულ მცირე ერთი „რეგულაციური სენდბოქსი“ უნდა ჰქონდეთ. ამ „სენდბოქსების“ მიზანია შესაძლო რისკების იდენტიფიცირება, კერძოდ, ფუნდამენტურ უფლებებთან მიმართებით. მათი დამატებითი მიზანია ისეთი ინოვაციების ხელშეწყობა, რომლებიც იცავს და პატივს სცემს ფუნდამენტურ უფლებებს, მათ შორის, პერსონალურ მონაცემთა დაცვის უფლებას.

საინტერესოა ისიც, რომ ამავე მუხლის მე-4 პუნქტი ეროვნული მარეგულირებელი სავარჯიშო სივრცის მართვაზე პასუხისმგებელ ორგანოს შესაძლებლობას აძლევს, ითანამშრომლოს სხვა უწყებებთან ხელოვნური ინტელექტის სისტემის ტესტირების პროცესში. ამ დებულებიდან გამომდინარე, ჩვენ გვიჩნდება შესაძლებლობა, განვახორციელოთ მაღალი რისკის მქონე ხელოვნური ინტელექტის სისტემების ერთგვარი წინასაბაზრო მონიტორინგი. კერძოდ, ჩვენ, როგორც ფუნდამენტური უფლებების დამცველ საჯარო უწყებებს, შეიძლება გვთხოვონ მონაწილეობა მაღალი რისკის მქონე ხელოვნური ინტელექტის სისტემების ტესტირებაში. ეს გზას გაუხსნის თანამშრომლობას საჯარო და კერძო აქტორებს შორის, რომლებიც ჩართულნი იქნებიან ხელოვნური ინტელექტის სისტემის ტესტირებაში, რათა მოხდეს მისი ადაპტირება ან მოდიფიცირება ფუნდამენტური უფლებების დასაცავად, მის ბაზარზე განთავსებამდე.

„რეგულაციური სენდბოქსების“ მსგავსს კონტროლირებად გარემოში, ტესტირების გარდა, ხელოვნური ინტელექტის აქტი ასევე იძლევა მაღალი რისკის მქონე სისტემების რეალურ პირობებში, „რეგულაციური სენდბოქსების“ გარეთ ტესტირების შესაძლებლობას. რა თქმა უნდა, ეს უნდა განხორციელდეს რიგი მკაცრი პირობების დაცვით, რომელთა შორისაა ხელოვნური ინტელექტის სისტემის ოპერატორის მიერ ეროვნული კომპეტენტური ორგანოსთვის ტესტირების გეგმის წარდგენა და რეალურ პირობებში ჩატარებული ამ ტესტირების საბოლოო შედეგის იმავე ორგანოსთვის გადაცემა.

თუ კომპეტენტური ორგანო საჭიროდ მიიჩნევს, მას შეუძლია მონიტორინგი გაუწიოს ტესტირების პროცესს, ტესტირების მიმდინარეობისას ადგილზე ან დისტანციურად ჩაატაროს ინსპექტირება

შესაბამისად, ეროვნულ კომპეტენტურ ორგანოს აქვს შესაძლებლობა, შეისწავლოს ხელოვნური ინტელექტის სისტემა ან უშუალოდ ტესტირების პროცესში, ან ტესტირების დასრულების შემდეგ, ოპერატორის მიერ გადაცემული საბოლოო შედეგების საფუძველზე.

ახლა წარმოიდგინეთ, რომ აღნიშნული ორგანო პერსონალურ მონაცემთა დაცვის უფლების შელახვის რისკს აღმოაჩენს — ხომ არ აამოქმედებდა ეს 79-ე მუხლის მე-2 პუნქტით გათვალისწინებულ შეტყობინებისა და რისკის აღმოფხვრის მექანიზმს? შესაბამისად, ხომ არ გამოიწვევდა ეს სხვა ტიპის წინასაბაზრო თანამშრომლობის მექანიზმის ამოქმედებას ფუნდამენტური უფლებების დამცველი ორგანოების, ბაზარზე ზედამხედველობის ორგანოებისა და კერძო აქტორების მონაწილეობით?

შესაძლებლობები ნამდვილად არსებობს.

8. დასკვნა

დასასრულს, აღვნიშნავ – მიუხედავად იმისა, რომ ხელოვნურ ინტელექტთან დაკავშირებული გამოწვევები და რისკები მრავალრიცხოვანია, მსგავსი შეშფოთება გაჩნდა პროგნოზირებადი ტექნოლოგიების განვითარებასთან ერთად იმ პერიოდში, როდესაც პერსონალურ მონაცემთა დაცვა ძლიერდებოდა.

გამოცდილება, რომელიც ჩვენ, როგორც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებმა, მივიღეთ რთულ ტექნოლოგიურ გარემოში ძირითადი ღირებულებების შესახებ რთული საკითხების გადაჭრისას, გადამწყვეტია იმისთვის, რომ დავიწყოთ ფიქრი ხელოვნური ინტელექტის განვითარებისა და ინოვაციებისთვის წინასაბაზრო „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის ეთიკის გათვალისწინების“ მიდგომების შემუშავებაზე.

აგნიესკა გრზელაკი*

მონაცემთა მინიმიზაციისა და მოდელის მაქსიმიზაციის თავსებადობა: მარეგულირებელი და ეთიკური წინააღმდეგობები ხელოვნური ინტელექტის განვითარებაში**

ფართომასშტაბიანი ხელოვნური ინტელექტის (AI) სისტემების, განსაკუთრებით კი დიდი ენობრივი მოდელების (LLM) სწრაფმა განვითარებამ, მონაცემთა დაცვის სფეროში ღრმა მარეგულირებელი წინააღმდეგობები წარმოშვა. ამ დისკურსის ცენტრშია კონფლიქტი მონაცემთა მინიმიზაციის პრინციპსა, რომელიც „მონაცემთა დაცვის ძირითად რეგულაციით“ არის განმტკიცებული, და ხელოვნური ინტელექტის მოდელების შემუშავების საფუძვლად არსებულ მონაცემთა ინტენსიურ ლოგიკას შორის. სტატია იკვლევს ამ წინააღმდეგობის სამართლებრივ, პრაქტიკულ და ეთიკურ ასპექტებს მონაცემთა დაცვის საზედამხედველო ორგანოების (DPA) პერსპექტივიდან, აანალიზებს აღსრულების მიმდინარე ტენდენციებს, მარეგულირებელ სახელმძღვანელო მითითებებსა და ევროკავშირის ხელოვნური ინტელექტის აქტის მოსალოდნელ გავლენას. სტატიაში წარმოდგენილია არგუმენტი, რომლის თანახმად, მონაცემთა დაცვის საზედამხედველო ორგანოები უნდა გასცდნენ ტრადიციული აღსრულების როლს და იქცნენ ეთიკურ ზედამხედველებად და ხელოვნური ინტელექტის მართვის პროაქტიულ კოორდინატორებად ევროპაში, რათა უზრუნველყონ, რომ პრინციპები არ დასუსტდეს ან იგნორირებულ იქნეს ინოვაციის სახელით.

საკვანძო სიტყვები: *მონაცემთა მინიმიზაცია, ხელოვნური ინტელექტის აქტი, დიდი ენობრივი მოდელები (“LLM”), მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”), ხელოვნური ინტელექტის ეთიკური მმართველობა.*

---

* სამართლის მეცნიერებათა ჰაბილიტირებული დოქტორი, ვარშავის კოზმინსკის უნივერსიტეტის პროფესორი (დოქტორის ხარისხი, 2000 წ., კრაკოვის იაგელონის უნივერსიტეტი; ჰაბილიტაცია, 2016 წ., პოლონეთის მეცნიერებათა აკადემია). პერსონალურ მონაცემთა დაცვის ოფისის პრეზიდენტის მოადგილე.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე“) წარდგენილი მოხსენების ტექსტს.

1. შესავალი: მონაცემთა დაცვა ფართომასშტაბიანი ხელოვნური ინტელექტის მოდელების ეპოქაში

ხელოვნური ინტელექტის ("AI") ტექნოლოგიების მზარდმა ინტეგრაციამ საჯარო სერვისებში, კერძო საწარმოებსა და ყოველდღიურ ცხოვრებაში გაამწვავა დიდი ხნის არსებული დაპირისპირება ინოვაციასა და ფუნდამენტური უფლებების დაცვას შორის. მათ შორის ერთ-ერთი ყველაზე მწვავეა ახლად წარმოშობილი კონფლიქტი "GDPR"-ის ფუძემდებლურ მონაცემთა მინიმიზაციის პრინციპსა და მონაცემთა ინტენსიურ ლოგიკას შორის, რომელიც თანამედროვე "AI" სისტემების, განსაკუთრებით კი დიდი ენობრივი მოდელების ("LLM") განვითარებას უდევს საფუძვლად.

"GDPR"-ი მონაცემთა მინიმიზაციას მონაცემთა კანონიერი დამუშავების ფუძემდებლურ პრინციპად აცხადებს[1]. მე-5 მუხლის პირველი პუნქტის „c" ქვეპუნქტის თანახმად, პერსონალური მონაცემები უნდა იყოს „ადეკვატური, რელევანტური და შეზღუდული იმით, რაც აუცილებელია" იმ მიზნებთან მიმართებით, რომელთათვისაც ის მუშავდება. აღნიშნული მანდატი მიზნად ისახავს არასაჭირო პერსონალური მონაცემების შეგროვებისა და გამოყენების შეზღუდვას და ხელს უწყობს ანგარიშვალდებულებას, გამჭვირვალობასა და მონაცემთა სუბიექტების უფლებების პატივისცემას. თუმცა "AI" მოდელების, განსაკუთრებით "LLM"-ების, შემუშავების კონტექსტში ეს პრინციპი მზარდი წნეხის ქვეშ ექცევა.

"LLM"-ები ფუნქციონირებს მასშტაბურობის პრინციპით: რაც უფრო ფართო და მრავალფეროვანია მონაცემთა ბაზა, მით უფრო დახვეწილი და მძლავრი ხდება მოდელი[2]. ამის გამო დეველოპერები ხშირად მიმართავენ ვებ-სკრაპინგის განურჩევლად გამოყენებას, რათა შეაგროვონ უზარმაზარი მონაცემები, მათ შორის პერსონალური მონაცემები საჯარო ინტერნეტის მეშვეობით. წამყვანი ვარაუდი არის ის, რომ მეტი მონაცემი ნიშნავს მოდელის უკეთეს სიზუსტეს, კონტექსტურ გააზრებასა და ადაპტირების უნარს. თუმცა ეს ვარაუდი ქმნის სტრუქტურულ წინააღმდეგობას მონაცემთა მინიმიზაციასთან, რადგან ასეთი მოდელები შექმნილია არა შეტანილი მონაცემების მინიმიზაციისთვის, არამედ ინფორმაციის მოპოვებისა და განზოგადების შესაძლებლობების მაქსიმიზაციისთვის.

აღსანიშნავია, რომ წამყვანი LLM-ების უმეტესობა შემუშავებულია იმ ორგანიზაციების მიერ, რომელთა სათავო ოფისები ევროკავშირის ფარგლებს გარეთ მდებარეობს. ეს ქმნის დამატებით გამოწვევებს იურისდიქციას, აღსრულებასა და GDPR-ის ექსტრატერიტორიულ გამოყენებასთან დაკავშირებით. ევროპელი მომხმარებლების პერსონალურ მონაცემებს შესაძლოა ამუშავებდნენ არაევროკავშირის სუბიექტები, რომლებიც სრულად

[1] *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press, 2020.

[2] *Vaezi A.,* Legal Challenges in the Deployment of Large Language Models: A Comparative Analysis under the GDPR and EU AI Act, 2025.

არ ითავისებენ ევროკავშირის კანონმდებლობით დადგენილ ნორმატიულ და სამართლებრივ ვალდებულებებს. შედეგად, ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოები ("DPA") დგანან მზარდი აუცილებლობის წინაშე, დაამკვიდრონ ევროკავშირის მონაცემთა დაცვის პრინციპების შესაბამისობა გლობალურ ტექნოლოგიურ კონტექსტში.

ამ გამოწვევების საპასუხოდ, მონაცემთა დაცვის ევროპულმა საბჭო ("EDPB") სულ უფრო მეტად იხრება DPA-ების პასუხისმგებლობების უფრო ფართო ინტერპრეტაციისკენ. 2024 წლის ივლისში გამოქვეყნებულ თავის მე-3/2024 განცხადებაში "EDPB"-მ განმარტა, რომ DPA-ები არ არიან მხოლოდ რეაგირებაზე ორიენტირებული მარეგულირებლები, არამედ ასევე პროაქტიული მრჩევლები, კოორდინატორები და ეთიკური არბიტრები მომავალი ხელოვნური ინტელექტის აქტის ფარგლებში[3]. პასუხისმგებლობების ასეთი გადააზრება ხაზს უსვამს DPA-ების საჭიროებას, ჩაერთონ არა მხოლოდ აღსრულებაში, არამედ "AI" ტექნოლოგიების სტრატეგიულ მმართველობასა და პრევენციულ ზედამხედველობაში.

წინამდებარე სტატია მიზნად ისახავს, შეისწავლოს ამ ცვალებადი მარეგულირებელი ლანდშაფტის შედეგები, განსაკუთრებული აქცენტით მონაცემთა მინიმიზაციასა და მოდელის მაქსიმიზაციას შორის არსებულ წინააღმდეგობებზე. სტატია აანალიზებს, თუ როგორ შეუძლიათ DPA-ებს ეფექტიანად დაიცვან მონაცემთა დაცვის პრინციპები ეპოქაში, რომელშიც მონაცემთა მოცულობა და არა მონაცემთა დისციპლინა, სულ უფრო ხშირად განიხილება ტექნოლოგიური წარმატების საზომად. სამართლებრივი ანალიზის, მარეგულირებელი ნორმების ინტერპრეტაციისა და აღსრულების ახალი პრაქტიკის გათვალისწინების გზით ეს კვლევა ხელს უწყობს პასუხისმგებლიანი ხელოვნური ინტელექტის მომავლის შესახებ აქტუალურ დისკუსიას ევროკავშირსა და მის ფარგლებს გარეთ.

2. სტრუქტურული შეუთავსებლობა მონაცემთა მინიმიზაციასა და ხელოვნური ინტელექტის მოდელების შემუშავებას შორის

ფართომასშტაბიანი ხელოვნური ინტელექტის სისტემების სწრაფმა ევოლუციამ წინა პლანზე წამოწია თანამედროვე მონაცემთა დაცვის სამართლის ფუნდამენტური კითხვა: ვართ თუ არა სამართლებრივ პრინციპებსა და ტექნოლოგიურ პრაქტიკას შორის გარდაუვალი კონფლიქტის მომსწრენი? ამ დილემის საფუძველში დევს ფუნდამენტური დაპირისპირება "GDPR"-ის მონაცემთა მინიმიზაციის პრინციპსა და თანამედროვე მანქანური სწავლების მოდელების, განსაკუთრებით კი დიდი ენობრივი მოდელების ("LLM") ფუნქციონირების არქიტექტურას შორის.

[3] European Data Protection Board, Statement 3/2024 on the role of DPAs under the AI Act, 2024, <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> [23.07.2025].

“GDPR”-ი, კერძოდ, მისი მე-5 მუხლის პირველი პუნქტის „c“ ქვეპუნქტი, მონაცემთა მინიმიზაციის პრინციპს მონაცემთა კანონიერი დამუშავების ქვაკუთხედად აცხადებს[4]. ეს პრინციპი მოითხოვს, რომ შეგროვებული პერსონალური მონაცემები იყოს ადეკვატური, რელევანტური და მკაცრად აუცილებელი მოცულობით შემოიფარგლებოდეს იმ კონკრეტული მიზნებისათვის, რომელთათვისაც ის მუშავდება. პრაქტიკაში ეს ნიშნავს, რომ ორგანიზაციებმა თავი უნდა შეიკავონ მონაცემთა შეგროვებისგან ან შენახვისგან, თუკი ეს არ არის გამართლებული მიზნობრიობისა და აუცილებლობის თვალსაზრისით.

ამისგან მკვეთრად განსხვავებით, “LLM”-ის შემუშავების საფუძვლად გამოყენებული ლოგიკა მონაცემთა სიმრავლეს ემყარება. ხელოვნური ინტელექტის დეველოპერებს შორის გაბატონებული მოსაზრების თანახმად, ამ მოდელების ეფექტიანობა და განზოგადების უნარი უმჯობესდება სასწავლო მონაცემების მოცულობასა და მრავალფეროვნებასთან ერთად. შედეგად, “LLM”-ები, როგორც წესი, სწავლობენ უზარმაზარ მონაცემთა ბაზებზე დაყრდნობით, რომლებიც მილიარდობით ტექსტურ ნიმუშს მოიცავს — აკადემიური პუბლიკაციებიდან დაწყებული, ფორუმების პოსტებით, ბლოგებით, სოციალური მედიის კონტენტითა და სხვა საჯაროდ ხელმისაწვდომი წყაროებით დამთავრებული. სასურველი მიზანია ყოვლისმომცველი ლინგვისტური დაფარვისა და სემანტიკური სიმდიდრის მიღწევა, თუმცა ეს მონაცემებზე ორიენტირებული ფილოსოფია პირდაპირ ეწინააღმდეგება “GDPR”-ით დაწესებულ აუცილებლობისა და პროპორციულობის შეზღუდვებს.

ეს სტრუქტურული კონფლიქტი რამდენიმე კრიტიკული მიმართულებით ვლინდება. პირველ რიგში, ვებ-სკრაპინგის განურჩევლად გამოყენების პრაქტიკას, ხშირად აკლია მკაფიოდ განსაზღვრული მიზანი, რომელიც მონაცემთა მინიმიზაციასთან იქნებოდა თავსებადი. მხოლოდ ვარაუდი, რომ ყველა ხელმისაწვდომმა ტექსტურმა მონაცემმა შეიძლება შეუწყოს ხელი მოდელის გაუმჯობესებას, არასაკმარისია ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიხედვით, რომელიც კონკრეტულ და ლეგიტიმური დამუშავების მიზნებს მოითხოვს. მეტიც, შეგროვების მასშტაბი, როგორც წესი, მნიშვნელოვნად აღემატება იმას, რაც აუცილებლად ჩაითვლებოდა მოდელის დეკლარირებული ამოცანებისთვის, განსაკუთრებით მაშინ, როდესაც საქმე პერსონალურ მონაცემებს ეხება.

მონაცემთა დაცვის ევროპულმა საბჭომ (EDPB) თავის 28/2024 დასკვნაში ხაზი გაუსვა აუცილებლობის მკაცრი შეფასების მნიშვნელობას. საბჭო მიიჩნევს, რომ სასწავლო მონაცემთა ბაზებში ჩადებული პერსონალური მონაცემები მაშინაც კი, როდესაც მათი პირდაპირი იდენტიფიცირება შეუძლებელია, შეიძლება გახდეს ხელახალი იდენტიფიკაციის რისკების

[4] *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press, 2020.

საფუძველი[5]. ღრმა სწავლების მოდელებს, თავიანთი არქიტექტურიდან გამომდინარე, შეუძლიათ დაიმახსოვრონ და სიტყვასიტყვით ან პერიფრაზირებული ფორმით აღადგინონ სასწავლო მონაცემები. ეს ქმნის ფარულ საფრთხეს, რომ პერსონალური ინფორმაცია, რომელიც ერთხელ მოხვდა სასწავლო კორპუსში, შესაძლოა მოგვიანებით გამჟღავნდეს მოდელის შედეგების მეშვეობით, დეველოპერის მხრიდან შეგნებული განზრახვის არარსებობის შემთხვევაშიც კი.

“EDPB”-მ ასევე გაამახვილა ყურადღება ანონიმიზაციის შესახებ ზოგადი მტკიცებების არასაკმარისობაზე. მტკიცებულებები იმის შესახებ, რომ პერსონალური მონაცემები საკმარისად დეიდენტიფიცირებული ან ფსევდონიმიზებულია, დასაბუთებული უნდა იყოს კონკრეტული მოდელის შეფასებით და არ შეიძლება ეფუძნებოდეს აბსტრაქტულ ტექნიკურ ვარაუდებს. ინფერენს შეტევებმა, მოდელის ინვერსიამ და წევრობის ინფერენსის ტექნიკებმა ცხადყო, რომ გარკვეულ პირობებში ანონიმიზებული მონაცემები შესაძლოა რევერს-ინჟინერინგს დაექვემდებაროს ან მოხდეს მათი დაკავშირება კონკრეტულ პირებთან. ეს რისკები მოითხოვს მოდელის სწავლებისას გამოყენებული ტექნიკური უსაფრთხოების მექანიზმების ფრთხილ, ინდივიდუალურ ანალიზს.

გარდა ამისა, პროპორციულობის პრინციპი მონაცემთა დამუშავების კანონიერების ცენტრალური ელემენტია. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა დაასაბუთონ კავშირი დამუშავებული პერსონალური მონაცემების რაოდენობასა და “AI” სისტემის ეფექტიანობით მისაღებ სარგებელს შორის. თუმცა “LLM”-ების შემთხვევაში აუცილებლობისა და პროპორციულობის საზღვრები ხშირად ბუნდოვანია. დეველოპერები ხშირად ვერ ასაბუთებენ, თუ რატომ არის საჭირო მონაცემთა ბაზის კონკრეტული ზომა ან შემადგენლობა, ან რატომ არ განიხილეს უფრო მიზნობრივი და კონფიდენციალურობის დამცავი ალტერნატივები.

შესაბამისად, კონფლიქტი არა უბრალოდ თეორიული, არამედ ღრმად პრაქტიკულია. “AI” დეველოპერები მოქმედებენ პარადიგმაში, რომელიც მონაცემთა მაქსიმალურ ათვისებას ახალისებს მაშინ, როცა მონაცემთა დაცვის ჩარჩოები მოითხოვს შეზღუდვას, დასაბუთებასა და მომხმარებელზე ორიენტირებულ უსაფრთხოების მექანიზმებს. ამ ხარვეზის ამოსავსებად საჭირო იქნება არა მხოლოდ რეგულატორული სიცხადე და აღსრულება, არამედ პარადიგმის ცვლილებაც ხელოვნური ინტელექტის სფეროში ინოვაციების კონცეპტუალიზაციის პროცესში.

თავსებადობის მისაღწევად, “AI”-ის შემუშავების პროცესში სულ უფრო მეტად უნდა მოხდეს „შექმნის ეტაპზე კონფიდენციალურობის უზრუნველყოფისა“ და „ნაგულისხმევი პარამეტრებით კონფიდენციალურობის დაცვის“ პრინციპების ინტეგრირება, რომლებიც GDPR-

[5] European Data Protection Board, Opinion 28/2024 on Training Data for LLMs, 2024 <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en> [23.07.2025].

ის 25-ე მუხლით არის გათვალისწინებული. ეს გულისხმობს მონაცემთა მინიმიზაციის ლოგიკის ჩაშენებას "AI" სისტემების არქიტექტურაში მათი შექმნის საწყისი ეტაპიდანვე. ეს ასევე ნიშნავს ისეთი მეთოდოლოგიების დანერგვას, რომლებიც ამცირებს პერსონალურ მონაცემებზე დამოკიდებულებას — როგორებიცაა სინთეტიკური მონაცემების გენერირება, ფედერაციული სწავლება ან დიფერენციალური კონფიდენციალურობის მექანიზმები — რითაც ტექნოლოგიური პროგრესი სამართლებრივ ვალდებულებებს შეესაბამება.

დასასრულს, მონაცემთა მინიმიზაციასა და მოდელის მაქსიმიზაციას შორის აღქმული დიქოტომია ციფრულ ეპოქაში არსებული უფრო ფართო მმართველობითი გამოწვევების სიმბოლოა. მიუხედავად იმისა, რომ თავისი არსით შეუთავსებელი არ არის, ეს ურთიერთსაწინააღმდეგო ლოგიკები მიზანმიმართულ შეთანხმებას საჭიროებს მულტიდისციპლინური თანამშრომლობის, ტექნიკური ინოვაციებისა და მარეგულირებელი სიფხიზლის გზით. ამ ძალისხმევის გარეშე ფუნდამენტური უფლებების ხელშეუხებლობა შესაძლოა შეილახოს ტექნოლოგიური ოპტიმიზაციისკენ უკონტროლო სწრაფვით.

3. საჯაროდ ხელმისაწვდომი მონაცემები და პერსონალური ინფორმაციის სამართლებრივი სტატუსი "GDPR"-ის მიხედვით

"AI" დეველოპერებს შორის ფართოდ გავრცელებული მოსაზრების თანახმად, საჯაროდ ხელმისაწვდომი მონაცემები თავისი არსით თავისუფლდება მონაცემთა დაცვის რეგულაციების სრული მოქმედებისგან. ეს მცდარი წარმოდგენა საფუძვლად უდევს ბევრ არგუმენტს, რომლებიც ამართლებს ფართომასშტაბიანი მონაცემთა ბაზების შეგროვებასა და გამოყენებას "AI" მოდელების, მათ შორის, დიდი ენობრივი მოდელების ("LLM") შესასწავლად. დეველოპერები ხშირად ამტკიცებენ, რომ ვინაიდან გამოყენებული მონაცემები უკვე ხელმისაწვდომია ღია ინტერნეტში, მასზე მონაცემთა დაცვის ძირითადი რეგულაციის ("GDPR")[6] მარეგულირებელი დაცვის მექანიზმები არ ვრცელდება. თუმცა ასეთი მსჯელობა სამართლებრივად და ეთიკურად ხარვეზიანია.

"GDPR"-ის მიხედვით, მონაცემის „პერსონალურ" სტატუსს განსაზღვრავს მისი იდენტიფიცირებადობა და არა მისი ხელმისაწვდომობა. "GDPR"-ის მე-4 მუხლის პირველი პუნქტი განმარტავს პერსონალურ მონაცემებს, როგორც ნებისმიერ ინფორმაციას, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს, მიუხედავად იმისა, ეს ინფორმაცია კერძო

[6] პოლონეთის მონაცემთა დაცვის საზედამხედველო ორგანოსთან შეხვედრის დროს წარმოდგენილი მოსაზრებები. "OpenAI"-თან ან "Microsoft"-თან შეხვედრების შესახებ დამატებითი ინფორმაციისთვის იხილეთ <www.uodo.gov.pl>.

თუ საჯარო წყაროებიდან იქნა მოპოვებული. შესაბამისად, ის ფაქტი, რომ პერსონალური მონაცემები განთავსებულია საჯარო ფორუმებზე, სოციალურ მედიაში, კომენტარების სექციებში ან სხვა ღია წვდომის დომენებში, არ ართმევს მას დაცულ სტატუსს.

ამ სამართლებრივ პოზიციას მნიშვნელოვანი გავლენა აქვს "AI" სისტემების შემუშავებაზე, განსაკუთრებით იმ სისტემების, რომლებიც ინტერნეტიდან განურჩევლად შეგროვებულ მონაცემებზე სწავლობენ. მონაცემთა დაცვის ევროპულმა საბჭომ ("EDPB") ამ საკითხთან დაკავშირებით შეშფოთება გამოხატა რამდენიმე უახლეს დასკვნაში, განსაკუთრებით კი 28/2024 დასკვნაში. "EDPB" ხაზს უსვამს, რომ ასეთი მონაცემების "AI" მოდელების სასწავლებლად გამოყენების კანონიერება უნდა შეფასდეს ყოველი კონკრეტული შემთხვევის მიხედვით. ერთ-ერთი მთავარი საკითხია ის, რომ მონაცემთა ანონიმიზაციის პროცესი — რომელსაც დეველოპერები ხშირად შესაბამისობის უზრუნველყოფის ღონისძიებად ასახელებენ — არ შეიძლება ეფექტიანად ჩაითვალოს მკაცრი, კონკრეტული მოდელისთვის დამახასიათებელი ვალიდაციის გარეშე.

მაშინაც კი, თუ "AI" მოდელი არ არის შექმნილი პერსონალური მონაცემების პირდაპირ გამოსაცემად, რჩება მნიშვნელოვანი რისკი იმისა, რომ სასწავლო კორპუსში ჩადებული პერსონალური ინფორმაცია შენარჩუნებული იყოს მოდელის პარამეტრებში. ეს ფარული მონაცემები შესაძლოა უნებლიეთ აღდგეს მომხმარებლის მოთხოვნების საპასუხოდ, რითაც შეიქმნება კონფიდენციალურობის დარღვევის პოტენციალი დასკვნის გამოტანის ან ხელახალი იდენტიფიკაციის გზით. უახლესმა აკადემიურმა კვლევებმა და რეალურმა ინციდენტებმა აჩვენა, რომ "LLM"-ებს შეუძლიათ უნებლიეთ აღადგინონ კონკრეტული პერსონალური დეტალები, როგორებიცაა სახელები, მისამართები ან პირადი საუბრების ფრაგმენტები, რაც სერიოზულ კითხვებს აჩენს "AI" კონტექსტში სტანდარტული ანონიმიზაციის ტექნიკის საკმარისობასთან დაკავშირებით.

ამ რისკების ფონზე "DPA"-ები სულ უფრო მეტად ამოწმებენ ანონიმიზაციის შესახებ მტკიცებულებებს და ითხოვენ გამჭვირვალობას სასწავლო მონაცემთა შემადგენლობასთან დაკავშირებით. შესაბამისობის სათანადოდ შესაფასებლად მარეგულირებლებს უნდა ჰქონდეთ წვდომა დეტალურ ტექნიკურ დოკუმენტაციაზე, მათ შორის, მონაცემთა ბაზების წყაროებზე, წინასწარი დამუშავების მეთოდებსა და რისკების შემარბილებელ სტრატეგიებზე. ეს აძლიერებს მარეგულირებელი ორგანოების საჭიროებას, ინვესტიცია ჩადონ ტექნიკურ ექსპერტიზასა და მრავალდისციპლინური პოტენციალის განვითარებაში. ასეთი შესაძლებლობების გარეშე "DPA"-ები ვერ შეძლებენ იმ დეტალური შეფასებების ჩატარებას, რომლებიც აუცილებელია იმის დასადგენად, დაკმაყოფილებულია თუ არა მონაცემთა მინიმიზაციის, აუცილებლობისა და პროპორციულობის სტანდარტები.

გარდა ამისა, „შექმნის ეტაპზე კონფიდენციალურობის უზრუნველყოფის პრინციპი", რომელიც "GDPR"-ის 25-ე მუხლშია ჩამოყალიბებული, მოითხოვს,

რომ მონაცემთა დაცვის გარანტიები თავიდანვე იყოს ჩაშენებული დამუშავების პროცესებში. ეს გულისხმობს მონაცემთა დაცვაზე ზეგავლენის შეფასების (“DPIA”) საფუძვლიანად ჩატარებას სასწავლო ოპერაციების დაწყებამდე, მონაცემთა შეგროვების მიზნის, მასშტაბისა და შეზღუდვების განსაზღვრით. დეველოპერებმა უნდა განსაზღვრონ პერსონალური მონაცემების რომელი კატეგორიებია აუცილებელი მოდელის მიზნების მისაღწევად და დაასაბუთონ, რომ განიხილეს ნაკლებად ინვაზიური ალტერნატივები.

თანაბრად მნიშვნელოვანია პროპორციულობის კონცეფცია, რომელიც მოითხოვს დასაბუთებულ კავშირს დამუშავებული პერსონალური მონაცემების რაოდენობას, სენსიტიურობასა და დასახულ ლეგიტიმურ მიზნებს შორის. ონლაინ კონტენტის მასობრივი და განურჩეველი სკრაპინგი, განსაკუთრებით კონტექსტუალური ფილტრაციის ან თანხმობის გარეშე, არსებითად ეჭვქვეშ აყენებს პროპორციულობის პრინციპს და ძირს უთხრის მომხმარებლის ნდობას ციფრული ეკოსისტემებისადმი.

იდეა, რომ „საჯარო ნიშნავს დასაშვებს“, ცალსახად უნდა იქნეს უარყოფილი. ის ფაქტი, რომ ინფორმაცია ხელმისაწვდომია ონლაინ, არ ანიჭებს ლიცენზიას მისი მიზნის შესაცვლელად და მანქანური სწავლებისთვის გამოსაყენებლად შესაბამისი სამართლებრივი და ეთიკური გარანტიების გარეშე. “DPA”-ების მოვალეობაა, ეჭვქვეშ დააყენონ ეს ნორმა და გაამყარონ განსხვავება ხილვადობასა და ვალიდურობას შორის მონაცემთა მართვაში.

დასასრულს, საჯარო მონაცემების კანონიერი გამოყენება “AI”-ის შემუშავების პროცესში ჯერ კიდევ გადაუჭრელი საკითხია. ის მოითხოვს მყარ სამართლებრივ ინტერპრეტაციას, მკაცრ ტექნიკურ შემოწმებასა და პროაქტიულ მარეგულირებელ პოზიციას, რათა უზრუნველყოფილ იქნას, რომ ინდივიდუალური უფლებები არ დაექვემდებაროს ტექნოლოგიური ექსპანსიის იმპერატივებს.

4. დამუშავების სამართლებრივი საფუძვლები “AI” მოდელების სწავლებისას: თანხმობა, ლეგიტიმური ინტერესები და გამჭვირვალობის სირთულე

“AI” მოდელების, განსაკუთრებით კი დიდი ენობრივი მოდელების (“LLM”), სწავლებისას გამოყენებული პერსონალური მონაცემების დამუშავებისთვის ვალიდური სამართლებრივი საფუძვლის დადგენა ერთ-ერთი ყველაზე რთული და სადავო საკითხია არსებულ მარეგულირებელ გარემოში. მიუხედავად იმისა, რომ “AI” შესაძლებლობების გასავითარებლად სულ უფრო მეტად ეყრდნობიან მასიურ მონაცემთა კორპუსებს, ბევრ დეველოპერს არ განუმარტავს, თუ როგორ შეესაბამება ასეთი დამუშავება მონაცემთა დაცვის ძირითად რეგულაციას (“GDPR”), განსაკუთრებით მისი მე-6, მე-7, მე-13 და მე-14 მუხლების გათვალისწინებით.

მიუხედავად იმისა, რომ თანხმობა ხშირად "GDPR"-ით გათვალისწინებული კანონიერი დამუშავების ოქროს სტანდარტად მიიჩნევა, მისი პრაქტიკული გამოყენება "AI"-ის სწავლების კონტექსტში სირთულეებითაა სავსე. მე-4 მუხლის მე-11 პუნქტი თანხმობას განმარტავს, როგორც მონაცემთა სუბიექტის სურვილების თავისუფლად გამოხატულ, კონკრეტულ, ინფორმირებულ და ცალსახა მითითებას. თუმცა, ეს სტანდარტი იშვიათად სრულდება, როდესაც თანხმობის მიღება ხდება ზოგადი მომსახურების პირობებით, გაუმჭვირვალე კონფიდენციალურობის პოლიტიკით ან პლატფორმის დონის შეტყობინებებით. როდესაც პერსონალური მონაცემები შეგროვებულია საჯარო ვებსაიტებიდან ან მომხმარებლის მიერ გენერირებული კონტენტის პლატფორმებიდან, მონაცემთა სუბიექტებს, როგორც წესი, არ აქვთ რეალური შესაძლებლობა, მისცენ თანხმობა ან თქვან მასზე უარი, რომ აღარაფერი ითქვას იმის გაგებაზე, თუ როგორ იქნება მათი მონაცემები ხელახლა გამოყენებული "AI" სისტემებში. შესაბამისად, ამ კონტექსტში თანხმობაზე დაყრდნობა ხშირად იურიდიულად არასაკმარისი და ეთიკურად საეჭვოა.

პრაქტიკაში ბევრი დეველოპერი, როგორც უფრო მოქნილ ალტერნატივას, მე-6 მუხლის პირველი პუნქტის „f" ქვეპუნქტით გათვალისწინებულ ლეგიტიმური ინტერესის სამართლებრივ საფუძველს იყენებს[7]. თუმცა ამ საფუძვლის გამოყენების ზღვარი მკაცრია. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა ჩაატაროს ყოვლისმომცველი სამნაწილიანი დაბალანსების ტესტი: (1) განსაზღვროს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ან მესამე მხარის მიერ დაცული ლეგიტიმური ინტერესი, (2) დაასაბუთოს, რომ დამუშავება აუცილებელია ამ ინტერესის მისაღწევად, და (3) დაამტკიცოს, რომ ეს ინტერესი არ აღემატება მონაცემთა სუბიექტის უფლებებს და თავისუფლებებს. "EDPB"-ის 2024 წლის სახელმძღვანელო მითითებების თანახმად, რომელიც "AI"-სა და მონაცემთა დამუშავებას ეხება, ეს შეფასება უნდა იყოს ობიექტური და მტკიცებულებებზე დაფუძნებული და გამყარებული უნდა იყოს დოკუმენტირებული უსაფრთხოების გარანტიებით, ანგარიშვალდებულების ზომებითა და მონაცემთა სუბიექტის რისკების შემარბილებელი სტრატეგიებით.

ამ მიდგომის მთავარი სირთულე ის არის, რომ აუცილებლობა და პროპორციულობა იშვიათად არის თავისთავად ცხადი "LLM"-ების შემუშავების კონტექსტში. მონაცემების სკრაპინგის მასშტაბისა და გაუმჭვირვალობის, ასევე, მრავალფეროვანი სასწავლო მონაცემებიდან მიღებული სარგებლის სპეკულაციური ბუნების გათვალისწინებით, ხშირად გაუგებარია, არის თუ არა დამუშავება მკაცრად აუცილებელი დეკლარირებული მიზნისთვის, თუ უბრალოდ მოსახერხებელია მოდელის ეფექტიანობის მაქსიმალურად გასაზრდელად. მტკიცების ტვირთი ეკისრება მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, რომელმაც უნდა ახსნას, თუ რატომ ვერ მოხერხდა

[7] *Sangaraju V. V.,* AI and Data Privacy in Healthcare: Compliance with HIPAA, GDPR, and Emerging Regulations, International Journal of Emerging Trends in Computer Science and Information Technology, 2025, 67–74.

მსგავსი შედეგების მიღწევა ალტერნატიული, ნაკლებად ინვაზიური მეთოდებით.

ამ გამოწვევებს კიდევ უფრო ართულებს გამჭვირვალობის უზრუნველყოფის ვალდებულება, რომელიც "GDPR"-ის მე-13 და მე-14 მუხლებით არის გათვალისწინებული. ეს დებულებები ავალდებულებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს, აცნობონ მონაცემთა სუბიექტებს მათი პერსონალური მონაცემების შეგროვებისა და გამოყენების შესახებ, მიუხედავად იმისა, ეს მონაცემები მიღებულია პირდაპირ თუ ირიბად. მრავალი პლატფორმიდან ფართომასშტაბიანი სკრაპინგის საფუძველზე "AI"-ის სწავლების კონტექსტში ამ ვალდებულების შესრულება თითქმის შეუძლებელი ხდება. დეველოპერებს იშვიათად აქვთ წვდომა იმ პირთა ვინაობაზე ან საკონტაქტო ინფორმაციაზე, რომელთა მონაცემებიც სასწავლო ბაზებში მოხვდა, ხოლო რეტროაქტიული შეტყობინება ოპერაციულად შეუძლებელია.

მიუხედავად ამისა, "GDPR"-ი არ ითვალისწინებს გამონაკლისს გამჭვირვალობის ვალდებულებებთან დაკავშირებით მასშტაბის ან ტექნიკური არაპრაქტიკულობის საფუძველზე. გამჭვირვალობის ეფექტიანი მექანიზმების არარსებობის პირობებში საფუძვლად მდებარე მონაცემთა დამუშავების კანონიერება ეჭვქვეშ დგება. ამას მნიშვნელოვანი შედეგები მოაქვს იმ დეველოპერებისთვის, რომლებიც ცდილობენ დაეყრდნონ ლეგიტიმურ ინტერესს: თუ არ მოხდება მონაცემთა სუბიექტების ინფორმირება, იზღუდება მათი შესაძლებლობა, განახორციელონ თავიანთი უფლებები, როგორიცაა, მაგალითად, 21-ე მუხლით გათვალისწინებული შეწინააღმდეგების უფლება, რაც, თავის მხრივ, კიდევ უფრო ასუსტებს მონაცემთა დამუშავების ლეგიტიმურობას.

უფრო მეტიც, გამჭვირვალობა არა მხოლოდ სამართლებრივი მოთხოვნაა, არამედ უმნიშვნელოვანესი ეთიკური და საზოგადოებრივი იმპერატივი. ნდობა "AI" სისტემებისა და მათი მმართველი ინსტიტუტების მიმართ დამოკიდებულია ინდივიდების უნარზე, გაიგონ, როგორ გამოიყენება მათი მონაცემები და შეინარჩუნონ გარკვეული კონტროლი ამ გამოყენებაზე. ბევრი "LLM"-ის გაუმჭვირვალობა როგორც მათი სასწავლო მონაცემების, ისე ფუნქციონირების თვალსაზრისით, კიდევ უფრო აფართოებს ანგარიშვალდებულების ნაკლოვანებას, რაც აფერხებს დემოკრატიულ ზედამხედველობასა და საზოგადოებრივ ნდობას.

დასასრულს, AI-ის სწავლებისთვის ყველაზე ხშირად გამოყენებული სამართლებრივი საფუძვლები — თანხმობა და ლეგიტიმური ინტერესი — პრაქტიკაში უაღრესად პრობლემურია[8]. დეველოპერები უნდა გასცდნენ ზედაპირულ შესაბამისობას და გაითავისონ მონაცემთა დაცვის კანონის სულისკვეთება გამჭვირვალობის, ანგარიშვალდებულებისა და

[8] *Hoofnagle C. J., van der Sloot B., Zuiderveen Borgesius F.,* The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 2019, 65–98.

აუცილებლობის პრინციპების ჩაშენებით "AI" სისტემების დიზაინსა და დანერგვაში. ამგვარი ძალისხმევის გარეშე აღნიშნულ სამართლებრივ საფუძვლებზე დაყრდნობამ შესაძლოა, არა მხოლოდ ვერ გაუძლოს მარეგულირებლის შემოწმებას, არამედ შეარყიოს ხელოვნური ინტელექტის განვითარების ლეგიტიმურობა როგორც საზოგადოების, ისე პოლიტიკის შემქმნელების თვალში.

5. აღსრულების ტრაექტორიები და სტრატეგიული მარეგულირებელი რეაგირება "AI"-ის მიერ მონაცემთა გამოყენების პრაქტიკაზე

"GDPR"-ის დებულებების აღსრულება "AI"-ის განვითარების სფეროში თანამედროვე მონაცემთა დაცვის ერთ-ერთი ყველაზე რთული მიმართულებაა. "AI" სისტემების, განსაკუთრებით კი დიდი ენობრივი მოდელების ("LLM") სირთულე მარეგულირებლებს მრავალმხრივი გამოწვევების წინაშე აყენებს, მათ შორის, ტექნიკური გაუმჭვირვალობის, მონაცემთა გლობალიზებული ნაკადებისა და იურისდიქციათაშორისი ანგარიშვალდებულების ხარვეზების სახით. ამ ბარიერების მიუხედავად, შეინიშნება შესამჩნევი ევოლუცია ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოების ("DPA") პოზიციაში, რომლებიც სულ უფრო მეტად გადადიან რეაქციული აღსრულებიდან კოორდინირებულ და პროაქტიულ ზედამხედველობაზე.

აღსრულების ერთ-ერთი უმნიშვნელოვანესი ეტაპი 2023 წელს დადგა, როდესაც იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ ("Garante per la protezione dei dati personali") "ChatGPT"-ზე დროებითი აკრძალვა დააწესა. გადაწყვეტილება რამდენიმე საფუძველს ეყრდნობოდა, მათ შორის, მონაცემთა დამუშავების კანონიერი საფუძვლის არარსებობას, არასაკმარის გამჭვირვალობასა და იმ მექანიზმების არარსებობას, რომლებიც მონაცემთა სუბიექტებს თავიანთი უფლებებით სარგებლობის საშუალებას მისცემდა. ეს იყო ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოს ("DPA") მიერ საბაზისო მოდელის წინააღმდეგ განხორციელებული პირველი გახმაურებული ჩარევა, რაც იმის ნიშანია, რომ ხელოვნური ინტელექტის მასშტაბური სისტემებიც კი არ არის დაცული "GDPR"-ის აღსრულებისგან[9].

სხვა "DPA"-ებიც მიჰყვნენ ამ მაგალითს როგორც აღსრულების, ისე სახელმძღვანელო მითითებების შემუშავების კუთხით. საფრანგეთის მონაცემთა დაცვის ორგანომ ("CNIL") გამოსცა ყოვლისმომცველი რეკომენდაციები ვებ-სკრაპინგთან დაკავშირებით და ხაზი გაუსვა, რომ

[9] Garante per la protezione dei dati personali, Decision on OpenAI (ChatGPT), 2023, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9870832> [23.07.2025].

საჯარო ხელმისაწვდომობა არ უტოლდება იურიდიულ დასაშვებობას[10]. გაერთიანებული სამეფოს ინფორმაციის კომისრის ოფისმა ("ICO") ანალოგიურად გამოაქვეყნა სახელმძღვანელო მითითებები, რომლებშიც განმარტებულია პირობები, რომელთა დაცვითაც "AI"-ის დეველოპერებს შეუძლიათ კანონიერად გამოიყენონ საჯარო წყაროებიდან მოპოვებული მონაცემები სასწავლო მიზნებისთვის[11]. ამასობაში საბერძნეთის მონაცემთა დაცვის ორგანომ "Clearview AI" 20 მილიონი ევროთი დააჯარიმა, რითაც "GDPR"-ის დებულებების შესაბამისად, ბიომეტრიული მონაცემების სკრაპინგისთვის პასუხისმგებლობის დაკისრების პრეცედენტი შექმნა[12]. ეს ქმედებები ცხადყოფს მონაცემთა დაცვის საზედამხედველო ორგანოების ("DPA") მზარდ მზაობას, დაუპირისპირდნენ ხელოვნური ინტელექტის სფეროს გავლენიან მოთამაშეებს.

ევროპულ დონეზე მთავარი სიახლე ერთობლივი აღსრულების მექანიზმების გაჩენაა. მონაცემთა დაცვის ევროპულმა საბჭომ ("EDPB") შექმნა სპეციალური სამუშაო ჯგუფები. განსაკუთრებით აღსანიშნავია "ChatGPT"-ისა და "DeepSeek"-ის[13] შესახებ შექმნილი ჯგუფები, რომლებიც წევრ სახელმწიფოებში კოორდინირებული გამოძიებებისა და ჰარმონიზებული ინტერპრეტაციების საშუალებას იძლევა. სავარაუდოდ, ეს ძალისხმევა ინსტიტუციონალიზებული იქნება ხელოვნური ინტელექტის აქტის ფარგლებში, რომელიც ევროკავშირის მასშტაბით "AI"-ის მართვის ჩარჩოს ნერგავს და მოიცავს ხელოვნური ინტელექტის ევროპულ ოფისსა და გაძლიერებულ ტრანსსასაზღვრო საზედამხედველო სტრუქტურებს. ეს ახალი მექანიზმები იმეორებს "GDPR"-ის „ერთი ფანჯრის პრინციპის" მოდელს, თუმცა უფრო ძლიერი აქცენტით სისტემური რისკების შეფასებასა და სექტორულ ზედამხედველობაზე.

პარალელურად, "DPA"-ები იწყებენ სამომავლოდ ორიენტირებული მარეგულირებელი სტრატეგიების შემუშავებას. ეს მოიცავს პროაქტიული სახელმძღვანელო მითითებების გამოცემას, ალგორითმული ზეგავლენის შეფასებების მოთხოვნასა და ტექნიკური აუდიტის პროცედურების შესწავლას მოდელის ახსნადობისა და სასწავლო მონაცემების წარმომავლობის დასადგენად. ტრაექტორია ნათელია: აღსრულება აღარ შემოიფარგლება მხოლოდ წარსულში ჩადენილი დარღვევების დასჯით, არამედ ახლა მოიცავს

[10] CNIL, First Recommendations on the Development of AI Systems, Commission Nationale de l'Informatique et des Libertés, 2024, <https://www.cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems> [23.07.2025].

[11] ICO, The Lawful Basis for Web Scraping to Train Generative AI Models, Information Commissioner's Office (UK), 2024, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/the-lawful-basis-for-web-scraping-to-train-generative-ai-models/> [23.07.2025].

[12] Info on: <https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en> [23.07.2025].

[13] *Deng Z., Ma W., Han Q. L., Zhou W., Zhu X.,* Exploring DeepSeek: A Survey on Advances, Applications, Challenges and Future Directions, IEEE/CAA Journal of Automatica Sinica, 12(5), 2025, 872–893.

ex ante (წინასწარ) რეგულირებას, რომელიც მიზნად ისახავს სისტემური ზიანის თავიდან აცილებას, სანამ ის რეალობად იქცევა.

6. ეთიკური ზედამხედველობა "AI"-ის განვითარებაში: მონაცემთა დაცვის საზედამხედველო ორგანოების როლის გაფართოება

მიუხედავად იმისა, რომ სამართლებრივი ჩარჩოები, როგორიცაა "GDPR" და მომავალი ხელოვნური ინტელექტის აქტი, შესაბამისობის ფორმალურ კრიტერიუმებს ადგენს, მათ ყოველთვის არ შეუძლიათ სრულად მოიცვან "AI"-ის განვითარების ეთიკური განზომილებები. გენერაციული "AI" მოდელების სასწავლებლად პერსონალური მონაცემების გამოყენება წარმოშობს უფრო ფართო საზოგადოებრივ შეშფოთებას, რომელიც უკავშირდება ადამიანის ღირსებას, ინდივიდუალურ ავტონომიასა და კულტურულ რეპრეზენტაციას. პრაქტიკა, რომელიც კანონის ვიწრო ინტერპრეტაციით ტექნიკურად კანონიერია, შესაძლოა მაინც იწვევდეს ეთიკურ დისკომფორტს, საზოგადოებრივ უკმაყოფილებას ან სოციალურ ზიანს.

ამის თვალსაჩინო მაგალითია ექსპრესიული პერსონალური მონაცემების, - როგორებიცაა ხმოვანი ჩანაწერები, ბიომეტრიული გამოსახულებები ან შემოქმედებითი კონტენტი, გამოყენება სინთეტიკური მედიის გენერირებისთვის. მიუხედავად იმისა, რომ დეველოპერებმა შესაძლოა განაცხადონ, რომ მონაცემთა ასეთი გამოყენება კანონიერ საფუძვლებს ემყარება, თუკი ეს მონაცემები საჯაროდ ხელმისაწვდომი იყო, ეს მიდგომა უგულებელყოფს ისეთ უფრო ღრმა საკითხებს, როგორებიცაა თანხმობა, შემოქმედებითი საკუთრება და საკუთარი გამოსახულების უფლება. ექსპლუატაციდან გამომდინარე, შემოქმედებით და ჟურნალისტურ სექტორებში საარქივო მასალის უნებართვო გამოყენება "AI"-ის მიერ გენერირებული ხმების ან ავატარების სასწავლებლად ფართოდაა დაგმობილი. ასეთი პრაქტიკა არღვევს პროფესიულ კეთილსინდისიერებას და ამცირებს ინდივიდების უნარს, გააკონტროლონ, თუ როგორ ხდება მათი იდენტობის ციფრული რეპროდუქცია.

ეს შეშფოთების საგანი სცდება ინდივიდუალურ ზიანს და მოიცავს სისტემურ რისკებს, მათ შორის, „დიპფეიკებს", დეზინფორმაციას, პოლიტიკურ მანიპულაციასა და კულტურულ ჰომოგენიზაციას. დიდი ენობრივი მოდელების („LLM") ან მულტიმოდალური ხელოვნური ინტელექტის სისტემების მიერ გენერირებული სინთეტიკური კონტენტი შესაძლოა გამოყენებულ იქნას რეალური პირების იმიტირების, საზოგადოებრივი დისკურსის დამახინჯების ან დემოკრატიული პროცესებისთვის ძირის გამოთხრის მიზნით. ასეთი გამოყენების ეთიკური შედეგები ღრმაა და მათი წინასწარ განჭვრეტა ყოველთვის არ არის შესაძლებელი მონაცემთა შეგროვების ან მოდელის სწავლების ეტაპზე.

ამ რისკების გათვალისწინებით, "EDPB"-მ მოუწოდა "DPA"-ებს, იკისრონ უფრო ფართო ეთიკური მანდატი. ფორმალური შესაბამისობის უზრუნველყოფის მიღმა, "DPA"-ებისგან სულ უფრო მეტად მოელიან, რომ გამოავლინონ ძალაუფლების ასიმეტრია ინდივიდებსა და დეველოპერებს შორის, შეაფასონ ფართომასშტაბიანი მონაცემთა ექსპლუატაციის საზოგადოებრივი გავლენა და ხელი შეუწყონ პასუხისმგებლიან ინოვაციას. შესაბამისად, ეთიკური შეფასება უნდა განიხილებოდეს, როგორც მონაცემთა დაცვის მმართველობის დამატებითი განზომილება, რომელიც ინტეგრირებულია რისკზე დაფუძნებულ რეგულირებასა და გამჭვირვალობის ვალდებულებებში.

ამ როლის ეფექტიანად შესასრულებლად DPA-ებმა უნდა განავითარონ ინტერდისციპლინური შესაძლებლობები, რომლებიც მოიცავს იურიდიულ, ტექნიკურ, სოციოლოგიურ და ფილოსოფიურ ექსპერტიზას, და წარმართონ დიალოგი დაზარალებულ თემებთან, სამოქალაქო საზოგადოების ორგანიზაციებთან და აკადემიურ მკვლევარებთან. ეთიკური ზედამხედველობა უნდა იყოს ჩაშენებული ალგორითმულ დიზაინში ისეთი მექანიზმების საშუალებით, როგორებიცაა: სამართლიანობის აუდიტი, მოდელის შეფასებაში მონაწილეობა და საზოგადოებრივი ინტერესების ზეგავლენის შეფასების დოკუმენტები.

შეჯამების სახით, ეთიკური მეურვეობა ყალიბდება, როგორც მარეგულირებელი ფუნქციის კრიტიკული გაფართოება. ის ხელახლა აყალიბებს "DPA"-ების როლს არა მხოლოდ როგორც კანონიერების მცველების, არამედ როგორც სამართლიანობის არბიტრების სწრაფად განვითარებად ტექნოლოგიურ ლანდშაფტში. მხოლოდ სამართლებრივი შესაბამისობის ეთიკურ ლეგიტიმურობასთან შეთავსებით შეძლებს "AI" სისტემების მმართველობა შეინარჩუნოს საზოგადოებრივი ნდობა და ფუნდამენტური უფლებები ციფრულ ეპოქაში.

7. სამომავლო მიმართულებები: ხელოვნური ინტელექტის აქტის ინტეგრაცია და ინსტიტუციური გამოწვევების გადაჭრა

ჩვენ მიერ უკვე ნახსენები ევროკავშირის ხელოვნური ინტელექტის აქტი ("AI Act") წარმოადგენს უმნიშვნელოვანეს მარეგულირებელ ინიციატივას, რომელიც "AI" სისტემების მართვისთვის ყოვლისმომცველ, რისკზე დაფუძნებულ ჩარჩოს ამკვირდებს. "GDPR"-ის მიერ ჩაყრილ საფუძვლებზე დაყრდნობით, "AI Act" აწესებს მკაცრ ვალდებულებებს ე. წ. მაღალი რისკის "AI" აპლიკაციებისთვის. ეს, სხვა საკითხებთან ერთად, მოიცავს შესაბამისობის სავალდებულო შეფასებებს, სტრუქტურირებულ ტექნიკურ დოკუმენტაციას, მონაცემთა მართვის მყარ ჩარჩოებსა და ბაზარზე განთავსების შემდგომი მონიტორინგის მოთხოვნებს.

“AI Act”-ის ერთ-ერთი ყველაზე მნიშვნელოვანი წვლილი არის მონაცემთა ხარისხისა და მონაცემთა მინიმიზაციის პრინციპების ფუქნციონირება “AI”-ის სასიცოცხლო ციკლის ფარგლებში. “AI Act”-ის მე-10 მუხლის მე-3 პუნქტი ადგენს, რომ სწავლების, ვალიდაციისა და ტესტირებისთვის გამოყენებული მონაცემთა ბაზები უნდა იყოს „რელევანტური, უშეცდომო და მაქსიმალურად სრულყოფილი“. ამასთან, ხაზს უსვამს, რომ მათი მასშტაბი უნდა იყოს მინიმიზებული პერსონალური მონაცემების არასაჭირო გამჟღავნების თავიდან ასაცილებლად. ამ თვალსაზრისით, აქტი აძლიერებს “GDPR”-ის მიერ დაწყებულ ნორმატიულ ტრაექტორიას მონაცემთა დაცვის სტანდარტების პირდაპირ “AI” სისტემის დიზაინსა და შეფასებაში ჩაშენებით.

მონაცემთა დაცვის საზედამხედველო ორგანოებისთვის (“DPA”) “AI Act”-ის იმპლემენტაცია ნიშნავს როგორც პასუხისმგებლობების გაფართოებას, ისე ინსტიტუციური იდენტობის ტრანსფორმაციას. “DPA”-ები აღარ იმოქმედებენ მხოლოდ, როგორც მონაცემთა კონფიდენციალურობის ეროვნული აღმსრულებლები, არამედ უნდა ჩამოყალიბდნენ “AI”-ის მართვის პანევროპული ქსელის საკვანძო რგოლებად. ეს მოიცავს თანამშრომლობას ახლად დაარსებულ ხელოვნური ინტელექტის ევროპულ ოფისთან, მონაწილეობას ტრანსსასაზღვრო გამოძიებებში, წვლილის შეტანას ჰარმონიზებული სახელმძღვანელო მითითებების შემუშავებასა და მაღალი რისკის “AI” სისტემების ზედამხედველობაში, რომლებიც გამოიყენება მრავალ სექტორში, მათ შორის, ჯანდაცვაში, განათლებაში, დასაქმებასა და სამართალდაცვაში.

თუმცა აღნიშნული გარდამავალი პერიოდი გამოწვევებითაა სავსე. ბევრი “DPA” ამჟამად რესურსების მნიშვნელოვანი შეზღუდვების წინაშე დგას, მათ შორის, კადრების ნაკლებობის, შეზღუდული ტექნიკური ინფრასტრუქტურისა და მანქანურ სწავლებაში, ალგორითმულ აუდიტსა და სისტემურ ინჟინერიაში არასაკმარისი შიდა ექსპერტიზის სახით. “AI Act”-ით განსაზღვრული ახალი პასუხისმგებლობები, როგორებიცაა: სასწავლო მონაცემების წარმომავლობის შეფასების, ალგორითმული ზეგავლენის შეფასებისა და დიზაინის გამჭვირვალობასთან შესაბამისობის უზრუნველყოფის შესაძლებლობა, მოითხოვს მნიშვნელოვან ინვესტიციას ორგანიზაციულ შესაძლებლობებში, უნარების განვითარებასა და ინსტიტუციურ კოორდინაციაში.

სირთულის კიდევ ერთი წყაროა “GDPR”-სა და ხელოვნური ინტელექტის აქტს შორის არსებული დოქტრინული და ოპერაციული კვეთიდან გამომდინარეობს. დეველოპერებმა უნდა იხელმძღვანელონ ერთმანეთის თანმხვედრი და ზოგჯერ პოტენციურად ურთიერთსაწინააღმდეგო ვალდებულებებით, რომლებიც ეხება მონაცემთა მინიმიზაციას, დამუშავების კანონიერ საფუძველს, სამართლიანობას, ანგარიშვალდებულებასა და მონაცემთა სუბიექტის უფლებებს. ეს თანხვედრები მოითხოვს განმარტებით მითითებებს EDPB-სა და ხელოვნური ინტელექტის ევროპული ოფისისგან, რათა უზრუნველყოფილ იქნას თანმიმდევრული აღსრულება. შესაბამისობის ერთობლივი ჩარჩოებისა და სამოდელო შაბლონების შემუშავება ხელს

შეუწყობს მარეგულირებელი ხარვეზების აღმოფხვრასა და სამართლებრივი გარკვეულობის გაზრდას იმ დეველოპერებისთვის, რომლებიც ევროკავშირის მრავალ იურისდიქციაში ოპერირებენ.

დაბოლოს, "AI"-ის განვითარების გლობალური ბუნება გამოწვევებს უქმნის ევროპული რეგულაციების აღსრულების მასშტაბს. ბევრი საბაზისო მოდელი ევროკავშირის ფარგლებს გარეთ მუშავდება და მათი ინტეგრაცია ადგილობრივ პროდუქტებსა თუ სერვისებში ხშირად ბუნდოვანს ხდის იურისდიქციულ საზღვრებს. "AI Act"-ის წარმატება დამოკიდებული იქნება ევროპელი მარეგულირებლების უნარზე, დაამკვიდრონ ექსტრატერიტორიული გავლენა თანამშრომლობის მექანიზმების, ადეკვატურობის ჩარჩოებისა და საჯარო შესყიდვების წამახალისებელი მექანიზმების მეშვეობით, რომლებიც უპირატესობას ანიჭებენ შესაბამისობაში მყოფ სისტემებს.

შეჯამების სახით აღსანიშნავია, "AI Act"-ი გვთავაზობს უპრეცედენტო შესაძლებლობას, შეუთავსოს ტექნოლოგიური ინოვაცია დემოკრატიულ ღირებულებებსა და ფუნდამენტურ უფლებებს. თუმცა მისი იმპლემენტაცია მოითხოვს ძლიერ ინსტიტუტებს, სექტორთაშორის თანამშრომლობასა და მტკიცე პოლიტიკურ ნებას, რათა პასუხისმგებლიანი "AI" არა მხოლოდ მარეგულირებელ მისწრაფებად, არამედ ოპერაციულ რეალობად იქცეს.

8. დასკვნა: სამართლებრივი შესაბამისობიდან ეთიკურ და სტრატეგიულ მეურვეობამდე

მონაცემთა მინიმიზაციის პრინციპი, რომელიც ოდესღაც ტექნიკურ შეზღუდვად ან ბიუროკრატიულ ფორმალობად განიხილებოდა, ციფრულ ეპოქაში სათვალთვალო კაპიტალიზმის, ალგორითმული ექსპლუატაციისა და ძალაუფლების ასიმეტრიის წინააღმდეგ ნორმატიულ ბურჯად იქცა. ეპოქაში, რომელსაც სულ უფრო მეტად განსაზღვრავს მოდელის მაქსიმიზაცია და მონაცემთა მოდიფიკაცია, იგი ერთდროულად სამართლებრივ მოთხოვნასა და მორალურ იმპერატივს წარმოადგენს.

თუმცა ამ პრინციპის გამოყენება უნდა განვითარდეს იმ უნიკალური სირთულეების საპასუხოდ, რომლებსაც თანამედროვე "AI" სისტემები ქმნის. დიდი ენობრივი მოდელები და სხვა საბაზისო მოდელები ეჭვქვეშ აყენებს ტრადიციულ სამართლებრივ კატეგორიებსა და საპროცესო გარანტიებს, რაც მარეგულირებელი აღსრულებისადმი უფრო დინამიკურ და ჰოლისტიკურ მიდგომას მოითხოვს. შესაბამისად, მონაცემთა დაცვის საზედამხედველო ორგანოებმა ("DPA") უნდა გაიაზრონ თავიანთი მანდატი — არა მხოლოდ აღასრულონ შესაბამისობა, არამედ ხელი შეუწყონ სისტემურ ანგარიშვალდებულებას, ეთიკურ რეფლექსიასა და საზოგადოებრივ ნდობას.

ეს გაფართოებული როლი გულისხმობს მონაცემთა გაუმართლებელი ან არაპროპორციული გამოყენების პრაქტიკისთვის წინააღმდეგობის გაწევას,

გამჭვირვალე და განმარტებადი “AI”-ის ხელშეწყობასა და იმ ინდივიდების უფლებებისა და თავისუფლებების დაცვას, რომელთა მონაცემებიც ციფრული ინოვაციის საფუძველს წარმოადგენს. ასევე, ის მოითხოვს ინსტიტუციური შესაძლებლობების განვითარებას რისკზე დაფუძნებული აუდიტის ჩასატარებლად, სამოქალაქო საზოგადოებასთან თანამშრომლობისა და “AI” ტექნოლოგიების ეთიკურ მმართველობაში წვლილის შესატანად.

საბოლოო ჯამში, ხელოვნური ინტელექტის პასუხისმგებლიანი განვითარება და დანერგვა არ დაიყვანება სამართლებრივი ვალდებულებების ჩამონათვალზე. ეს არის კოლექტიური საზოგადოებრივი ვალდებულება, რომლის მიზანია ტექნოლოგიური პროგრესის ბირთვში ადამიანის ღირსების, სამართლიანობისა და სამართლის პრინციპების დანერგვა. ამ ძალისხმევაში მონაცემთა დაცვის საზედამხედველო ორგანოები (“DPA”) არ არიან მხოლოდ მარეგულირებლები, ისინი ციფრული საზოგადოებრივი ინტერესის მეურვეები არიან.

ბიბლიოგრაფია:

1. CNIL, First Recommendations on the Development of AI Systems, Commission Nationale de l’Informatique et des Libertés, 2024, <https://www.cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems> [23.07.2025].
2. *Deng Z., Ma W., Han Q. L., Zhou W., Zhu X.,* Exploring DeepSeek: A Survey on Advances, Applications, Challenges and Future Directions, IEEE/CAA Journal of Automatica Sinica, 12(5), 2025, 872–893.
3. European Data Protection Board, Statement 3/2024 on the role of DPAs under the AI Act, 2024, <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> [23.07.2025].
4. European Data Protection Board, Opinion 28/2024 on Training Data for LLMs, 2024 <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en> [23.07.2025].
5. Garante per la protezione dei dati personali, Decision on OpenAI (ChatGPT), 2023, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9870832> [23.07.2025].
6. *Hoofnagle C. J., van der Sloot B., Zuiderveen Borgesius F.,* The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 2019, 65–98.
7. ICO, The Lawful Basis for Web Scraping to Train Generative AI Models, Information Commissioner's Office (UK), 2024, <https://ico.org.uk/about-the-

ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/the-lawful-basis-for-web-scraping-to-train-generative-ai-models/> [23.07.2025].

8. *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press, 2020.
9. *Sangaraju V. V.,* AI and Data Privacy in Healthcare: Compliance with HIPAA, GDPR, and Emerging Regulations, International Journal of Emerging Trends in Computer Science and Information Technology, 2025, 67–74.
10. *Vaezi A.,* Legal Challenges in the Deployment of Large Language Models: A Comparative Analysis under the GDPR and EU AI Act, 2025.

კობა გრიალაშვილი*

პერსონალური მონაცემების დაცვა სამართალდამცავი ორგანოების საქმიანობაში

პერსონალური მონაცემების დამუშავების მიმართულებით გლობალიზაციამ ახალი გამოწვევები გააჩინა. მნიშვნელოვნად გაიზარდა მათი დამუშავების მასშტაბები. ამ მხრივ, აღსანიშნავია სამართლდამცავი ორგანოების მხრიდან პერსონალურ მონაცემთა დამუშავების მოცულობა, რამდენადაც, კანონმდებლობით დაკისრებული უფლებამოსილების განხორციელების მიზნით, მათ აქვთ როგორც ღია, ასევე ფარული წყაროებიდან მონაცემთა მოპოვებისა და სხვაგვარი დამუშავების შესაძლებლობა, ხოლო ტექნოლოგია საშუალებას აძლევს სამართალდამცავ ორგანოებს, პერსონალური მონაცემები უპრეცედენტო მასშტაბით დაამუშაონ.

სტატიაში ყურადღება გამახვილდება მონაცემთა დამუშავების სტანდარტებზე სამართალდამცავი ორგანოების საქმიანობის სპეციფიკურობის გათვალისწინებით, რაც გულისხმობს სათანადო ბალანსის დაცვას საზოგადოებრივი უსაფრთხოების დაცვის ინტერესის მიზნებსა და მონაცემთა სუბიექტის უფლების პატივისცემას შორის.

ნაშრომში განხილული იქნება ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU)2016/680 კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი მიმოცვლის შესახებ[1] *(შემდგომში - საპოლიციო დირექტივა) და მის*

* აღმოსავლეთ ევროპის უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, საქართველოს პარლამენტის ადამიანის უფლებათა დაცვისა და სამოქალაქო ინტეგრაციის კომიტეტის აპარატის უფროსი.

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (შემდგომში — „საპოლიციო დირექტივა“).

რამდენიმე ძირითად კომპონენტებზე გვექნება საუბარი, კერძოდ, განხილული იქნება საპოლიციო დირექტივის მნიშვნელობა და მისი მიღების ძირითადი მიზანი, საპოლიციო დირექტივით გათვალისწინებული მონაცემთა დამუშავების პრინციპები. ძირითადი მსჯელობა დაეთმობა მონაცემთა სუბიექტის უფლებებს, რომლებიც არის პერსონალურ მონაცემთა დაცვის კანონმდებლობის ერთ-ერთი მთავარი ხერხემალი და რომლის დაცვისა და განმტკიცების მიზნით არის მიღებული არაერთი საერთაშორისო აქტი.

საკვანძო სიტყვები: *საპოლიციო დირექტივა (LED), მონაცემთა სუბიექტის უფლებები, დანაშაულის პრევენცია, გამოძიება, დევნა ან სასჯელის აღსრულება, საზოგადოებრივი უსაფრთხოების დაცვა.*

1. შესავალი

პერსონალურ მონაცემთა დაცვის თვალსაზრისით, ევროკავშირი სამაგალითოდ მიიჩნევა მსოფლიოს მასშტაბით. ევროკავშირის მონაცემთა დაცვის სტანდარტები ემყარება გამოცდილებასა და კულტურას, რომელიც ათწლეულების განმავლობაში ყალიბდებოდა ევროპის ქვეყნებში. ევროკავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვა დამოუკიდებელ ფუნდამენტურ უფლებად არის აღიარებული - 2009 წელს ლისაბონის ხელშეკრულების საფუძველზე ძირითად უფლებათა ქარტიას[2] სამართლებრივად სავალდებულო ძალა მიენიჭა და იგი ევროკავშირის პირველადი კანონმდებლობის ნაწილი გახდა. აღნიშნულმა მონაცემთა დაცვის სამართლებრივი განვითარება ახალ საფეხურზე აიყვანა და ევროკავშირის დონეზე, კანონმდებლობით განამტკიცა პერსონალურ მონაცემთა დაცვის ძირითადი უფლება.

ძირითად უფლებათა ქარტიის მოქმედება ვრცელდება ყველა სფეროზე, მათ შორის, სამართალდამცავი ორგანოების საქმიანობაზე. სწორედ ეს გახდა საპოლიციო დირექტივის მიღების საფუძველი.

2. საპოლიციო დირექტივის მნიშვნელობა

როგორც აღინიშნა, ევროკავშირში სამართალდამცავი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავების პროცესი დამოუკიდებელი სამართლებრივი აქტით არის მოწესრიგებული. განსხვავებით ევროკავშირის

[2] Charter of Fundamental Rights of the European Union. Official Journal of the European Union C 326, 26.10.2012.

მონაცემთა დაცვის ძირითადი რეგულაციისა (GDPR), რომელსაც ფორმალურად პირდაპირ მოქმედი ძალა გააჩნია ევროკავშირის ყველა წევრ სახელმწიფოში, საპოლიციო დირექტივა ამგვარი ბუნებით არ გამოირჩევა, ვინაიდან მისი იმპლემენტაცია მოითხოვს ევროკავშირის თითოეულ წევრ სახელმწიფოში შესაბამისი, შიდა ეროვნული კანონმდებლობის მიღებას.

აღსანიშნავია, რომ საპოლიციო დირექტივით გათვალისწინებულია სამართალდამცავი ორგანოების თავისებურებები, რაც გულისხმობს მეტად ფართო ინსტრუმენტების არსებობას, რათა შესაბამისმა ორგანოებმა ეფექტიანად განახორციელონ მათზე კანონმდებლობით დაკისრებული ფუნქცია-მოვალეობები. ზოგადად შეიძლება ითქვას, რომ, სამართალდამცავი ორგანოების საქმიანობის სპეციფიკურობის გათვალისწინებით, დირექტივა ევროკავშირის ფარგლებში ადგენს ყოვლისმომცველ ჩარჩოს მონაცემთა დაცვის მაღალი სტანდარტის უზრუნველსაყოფად; მისი მოქმედება ვრცელდება პერსონალურ მონაცემთა მთლიანად ან ნაწილობრივ ავტომატური საშუალებებით დამუშავებაზე. ამასთან, ხაზგასასმელია ის გარემოება, რომ დირექტივის მოქმედება ასევე ვრცელდება იმ პერსონალური მონაცემების არაავტომატური საშუალებებით დამუშავებაზე, რომლებიც წარმოადგენენ ფაილური სისტემის ნაწილს ან ფაილურ სისტემაში შესატანად მუშავდება.[3] პირის მონაცემების დაცვა არ უნდა იყოს დამოკიდებული ტექნოლოგიების გამოყენების საკითხზე, რათა თავიდან არ იქნას აცილებული დირექტივის მოქმედება. შესაბამისად, დირექტივა ვრცელდება როგორც ავტომატური საშუალებით დამუშავებულ, ისე არაავტომატური საშუალებით დამუშავებულ მონაცემებზე, რომელთა მიზანიც არის შემდგომში ფაილურ სისტემაში შენახვა. რაც შეეხება დირექტივის მოქმედების ფარგლებს, იგი ადგენს ევროკავშირის წევრი ქვეყნებისთვის მინიმალურ სტანდარტს, რაც არ გამორიცხავს იმას, რომ წევრმა სახელმწიფოებმა უფრო მაღალი სტანდარტები დაადგინონ. შესაბამისად, საპოლიციო დირექტივის მოქმედება ვრცელდება მონაცემთა დამუშავებისას ევროკავშირის სახელმწიფოების შესაბამისი ორგანოების საქმიანობაზე, როდესაც ისინი მუშავდება დანაშაულის პრევენციის, გამოძიების, დევნის ან სასჯელის აღსრულების მიზნებისთვის, მათ შორის, საზოგადოებრივი უსაფრთხოებისთვის, საფრთხეებისგან დაცვისა და მათი პრევენციის მიზნით.

საგულისხმოა, რომ იმ შემთხვევაში, როდესაც სამართალდამცავი ორგანოები მონაცემებს ამუშავებენ ხსენებულისგან განსხვავებული მიზნებისთვის, მათზე გავრცელდება ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია. მაგალითისთვის, თუ მესაზღვრე პოლიციელი დააკავებს პირს, რომელმაც უკანონოდ გადაკვეთა ევროკავშირის წევრი სახელმწიფოს საზღვარი და აღნიშნული ამავდროულად მიიჩნევა სისხლის სამართლის დანაშაულად, პოლიციის მიერ გამოძიების დაწყების შემთხვევაზე, პირის მონაცემების დამუშავებისას, გავრცელდება საპოლიციო დირექტივით დადგენილი წესები. ხოლო იმ შემთხვევაში, თუ აღნიშნული პირი

[3] საპოლიციო დირექტივა, მუხლი 2, პ. 2.

მოითხოვს თავშესაფრის მიღებას, პოლიციის მიერ მონაცემების დამუშავება უნდა განხორციელდეს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ დადგენილი წესების შესაბამისად, ვინაიდან მოცემულ შემთხვევაში მონაცემები განსხვავებული მიზნით მუშავდება და თავშესაფრის მიღება არ უკავშირდება დანაშაულის პრევენციას ან გამოძიების წარმოებას.

3. საპოლიციო დირექტივის ძირითადი მიზანი

განზოგადებულად შეგვიძლია ვთქვათ, რომ საპოლიციო დირექტივის ძირითადი მიზანია საპოლიციო და სისხლის სამართლის სფეროში ფიზიკური პირების ფუნდამენტური უფლებების დაცვის სტანდარტის ამაღლება და ევროკავშირის წევრ სახელმწიფოებს შორის პერსონალური მონაცემების გაცვლის გაუმჯობესება. აქ იგულისხმება სახელმწიფოს პოზიტიური ვალდებულება, დაიცვას ფიზიკური პირების ფუნდამენტური უფლებები და თავისუფლებები. აღნიშნული ეხება პერსონალური მონაცემების დაცვის უფლებასა და ნეგატიურ ვალდებულებას, რათა არ შეფერხდეს პერსონალური მონაცემების მიმოცვლა ევროკავშირის ფარგლებში სამართალდამცავი ორგანოების მიერ, როდესაც ასეთი მონაცემების გადაცემა სავალდებულოა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით და პერსონალური მონაცემების დამუშავება არ არის აკრძალული ფიზიკური პირების დაცვასთან დაკავშირებული სხვა მიზეზების გამო. დირექტივის გამოყენების მიზნებისთვის აუცილებელია დაკმაყოფილდეს როგორც პირადი, ასევე მატერიალური მოქმედების სფერო. სხვა სიტყვებით, მონაცემთა დამუშავება უნდა განხორციელდეს შესაბამისი სამართალდამცავი ორგანოს მიერ (პირადი მოქმედების სფერო) დანაშაულის პრევენციის, გამოძიების, დევნის ან სასჯელის აღსრულების მიზნებისთვის, მათ შორის, საზოგადოებრივი უსაფრთხოებისთვის საფრთხეებისგან დაცვისა და მათი პრევენციის მიზნით (მატერიალური მოქმედების სფერო).[4]

ევროკავშირის წევრი ქვეყნების კანონმდებლობა შესაძლებელია განსხვავდებოდეს ქმედების სისხლის სამართლის დანაშაულად დასჯადობას მიხედვით. ერთი და იგივე ქმედება, რაც შეიძლება ერთ ქვეყანაში დანაშაულს წარმოადგენდეს, სხვა ქვეყანაში შეიძლება ადმინისტრაციულ სამართალდარღვევად ან სულაც, საფრთხის ხარისხის მცირე მნიშვნელობის გამო, არ ითვლებოდეს კანონდარღვევად. სისხლის სამართალი ძალიან ღრმად არის ფესვგადგმული ამა თუ იმ ქვეყნის შიდა პოლიტიკურ, სოციალურ და კონსტიტუციურ სისტემაში. ეს არის სფერო, რომელიც ხშირად ასოცირდება სახელმწიფოს სუვერენული ძალაუფლების მონოპოლიასთან. მაგალითად, დირექტივის შემუშავებისას კომისიის ექსპერტთა ჯგუფის ჩატარებული

[4] *Sajfert J., Quintel T.,* Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, 2017, 3.

შეხვედრების ოქმებიდან ჩანს, რომ წევრ სახელმწიფოებს შორის კონსენსუსი არ არსებობდა იმასთან დაკავშირებით, თუ როგორ უნდა განესხვავებინათ სისხლის სამართლის დანაშაული ადმინისტრაციული სამართალდარღვევის ან წვრილმანი ქმედებისგან იმ წევრ სახელმწიფოებში, რომელთა სამართლებრივი სისტემები ასეთ კლასიფიკაციას არ ადგენს. საბოლოოდ, ევროკომისიის გადაწყვეტილებით, იმპლემენტაციის პროცესში წევრ სახელმწიფოებს შეუძლიათ დაეყრდნონ სისხლის სამართლის დანაშაულის ცნებას, როგორც ეს განსაზღვრულია მათ ეროვნულ სამართლებრივ სისტემებში.[5]

ზემოთ აღნიშნული საკითხი საყურადღებოა იმდენად, რამდენადაც არსებობს დანაშაულთან ბრძოლის მოტივით საპოლიციო დირექტივის ფართოდ განმარტების რისკები მაშინ, როდესაც ტექნოლოგიური განვითარება ხელს უწყობს კომპეტენტურ ორგანოებს, პერსონალური მონაცემები გამარტივებულად შეაგროვონ თანამედროვე მეთვალყურეობის საშუალებებით და მონაცემთა ბაზების გამოყენებით, ასევე, კერძო პირების მიერ შეგროვებულ მონაცემებზე წვდომის შესაძლებლობით. ნებისმიერი ბუნდოვანება მნიშვნელოვან კითხვებს გააჩენს იმ პირთა უფლებების მდგომარეობის შესახებ, რომელთა მონაცემებიც შეიძლება დამუშავდეს ხსენებული მოტივით. აქვე, მხედველობაშია მისაღები დანაშაულის ჩადენის ან ზიანის რისკის გარდაუვალობა, რამაც შესაძლოა გაამართლოს საპოლიციო დირექტივის სტანდარტის გამოყენება.

ასევე, მონაცემთა დამუშავების ერთ-ერთ მიზანს წარმოადგენს სასჯელის აღსრულება. ამ შემთხვევაშიც ყურადღება უნდა გამახვილდეს სასჯელის არსზე, რადგან შესაძლებელია შინაარსობრივად მხოლოდ სისხლის სამართლის მნიშვნელობით სასჯელი არ იგულისხმებოდეს ამ ტერმინის ქვეშ, და ასევე მოიცავდეს ადმინისტრაციულ ან/და დისციპლინურ სახდელებს. ეს საკითხი ეროვნული კანონმდებლობით შეიძლება დაკონკრეტდეს, რადგან ზოგიერთი ადმინისტრაციული ან დისციპლინური სახდელი შეიძლება შინაარსობრივად საკმაოდ ჰგავდეს სისხლის სამართლებრივი მიზნებისთვის სასჯელის აღსრულებას. მაგალითად, როდესაც მსჯავრდებული სასჯელის მოხდის პერიოდში ჩაიდენს დისციპლინურ გადაცდომას, რთულია ამ დროს, დისციპლინური სახდელის შეფარდებისას, არ გავრცელდეს საპოლიციო დირექტივით დადგენილი რეგულაცია.

დანაშაულისგან განცალკევებულად უნდა განვიხილოთ საზოგადოებრივი უსაფრთხოების საკითხი, როდესაც არსებობს საფრთხისგან მისი დაცვის აუცილებლობა. ამ ჩანაწერმა რეალურად გააფართოვა დირექტივის მოქმედების ფარგლები და არსებობს რისკი, რომ იგი გასცდეს დანაშაულის შემადგენლობას და გავრცელდეს მონაცემთა დამუშავების ფართო სპექტრზე, ვინაიდან წევრი ქვეყნების ეროვნული კანონმდებლობის შესაბამისად, საზოგადოებრივი უსაფრთხოების მნიშვნელობაში შესაძლებელია მოიაზრებოდეს სხვა სიკეთეების დაცვა, როგორებიცაა საზოგადოებრივი

[5] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 60.

ჯანმრთელობის საკითხი და სხვა. საპოლიციო დირექტივაში ამ ჩანაწერის დამატებამ გამოწვია აზრთა სხვადასხვაობა. ამასთანავე, სამეცნიერო ლიტერატურაშიც გაკრიტიკებულია ეს საკითხი. „დირექტივის გამოყენების სფეროს გაფართოება გარდაუვლად წარმოშობს კითხვებს ინდივიდების უფლებების ღირებულებასთან, ასევე, ასეთი საკანონმდებლო გადაწყვეტის აუცილებლობასა და პროპორციულობასთან დაკავშირებით. ამის გათვალისწინებით, ზოგიერთი ავტორი გვთავაზობს დირექტივის პირველი მუხლიდან ფრაზის „მათ შორის, საზოგადოებრივი უსაფრთხოებისთვის საფრთხეებისგან დაცვისა და მათი პრევენციის“ ამოღებას“.[6]

4. მონაცემთა დამუშავებასთან დაკავშირებული პრინციპები

სამართალდამცავი ორგანოების სპეციფიკური საქმიანობის მიუხედავად, რაც გულისხმობს მონაცემთა დამუშავებისას სხვა საჯარო ორგანოებისგან განსხვავებულ მიდგომას, ისინი მაინც შეზღუდულნი არიან მონაცემთა დაცვის სახელმძღვანელო პრინციპებით. სამართალდამცავი ორგანოების მიერ შეგროვებული მონაცემები უნდა აკმაყოფილებდეს კანონიერებისა და სამართლიანობის, განსაზღვრულობის და პროპორციულობის, სიზუსტისა და უსაფრთხოების დაცვის კრიტერიუმებს.[7]

კანონიერების პრინციპი გულისხმობს, რომ პერსონალური მონაცემები უნდა დამუშავდეს იმ ორგანოს მიერ, რომელიც კანონით დადგენილი დავალების შესაბამისად მოქმედებს. გარდა იმისა, რომ სამართალდამცავი ორგანოების საქმიანობა სამართლებრივ საფუძვლებს უნდა ემყარებოდეს, აუცილებელია, რომ კანონმდებლობა ხელმისაწვდომი იყოს საზოგადებისთვის და აკმაყოფილებდეს განჭვრეტადობის კრიტერიუმებს. ეს საკითხი განსაკუთრებით საყურადღებოა სამართალდამცავი ორგანოების საქმიანობაში, როდესაც ისინი ფარული მეთოდებით მოქმედებენ. შესაბამისად, კანონმდებლობით მკაცრად უნდა იყოს განსაზღვრული ფარული მოქმედების ფარგლები, მისი განხორციელების ვადები და პროცედურები. მათ შორის, ფარული მოქმედებების განხორციელების შემდეგ შესაბამისი ორგანოს ზედამხედველობის მექანიზმები.

რაც შეეხება მონაცემთა დამუშავების პროცესში სამართალდამცავი ორგანოების მიერ სამართლიანობის პრინციპის დაცვას, მიუხედავად იმისა, რომ სამართლიანობა საკმაოდ ზოგადი ცნებაა, ამ შემთხვევაში უპირატესად იგულისხმება პროცედურული წესების სამართლიანად გამოყენება. გადაწყვეტილებებში, რომლებიც მონაცემთა სუბიექტის მიმართ მიიღება, იგი ადრეულ ეტაპზევე უნდა იყოს ჩართული, რამდენადაც ეს შესაძლებელია. მას ხელი უნდა მიუწვდებოდეს სათანადო დოკუმენტებზე და მის პოზიციას უნდა

[6] იქვე.
[7] საპოლიციო დირექტივა, მუხლი 4.

ჰქონდეს გადაწვეტილების მიღების პროცესზე გავლენის მოხდენის საშუალება, მათ შორის, სათანადო გასაჩივრების უფლების არსებობით. მხედველობაშია მისაღები სამართალდამცავი ორგანოების საქმიანობის თავისებურებებიც, რათა მათ ხელი არ შეეშალოთ დანაშაულის წინააღმდეგ ბრძოლაში. თუმცა ეს არგუმენტი არ გამოდება იმის საპირწონედ, რომ პირს არ ჰქონდეს საკუთარი უფლებების დაცვის შესაძლებლობა, მათ შორის, მისთვის დროული და სათანადო ინფორმირების გაზიარებით.

პერსონალური მონაცემები უნდა შეგროვდეს დირექტივის ფარგლებში განსაზღვრული, მკაფიო და ლეგიტიმური მიზნებისთვის და არ უნდა დამუშავდეს ისეთი მიზნებისთვის, რომლებიც შეუთავსებელია სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის ან სისხლის სამართლის სასჯელების აღსრულების მიზნებთან, მათ შორის, საზოგადოებრივი უსაფრთხოებისთვის საფრთხეებისგან დაცვისა და მათი პრევენციის მიზანთან. ეს მიზნები თავისთავად ძალიან ფართოა შესაბამისი პრინციპის დასაკმაყოფილებლად. აუცილებელია, რომ მიზანი იყოს კონკრეტულად განსაზღვრული, რათა ნათელი იყოს, თუ რატომ მუშავდება კონკრეტული მონაცემები. მხოლოდ სამართალდამცავი ორგანოების საქმიანობისთვის ზოგადი საჭიროება ვერ ჩაითვლება ლეგიტიმურ მიზნად. საქმეზე – "Inspektor v. Inspektorata kam Visshia sadeben savet" – ევროკაშირის მართლმსაჯულების სასამართლოს განმარტების თანახმად, როდესაც მონაცემები მუშავდება დანაშაულის გამოძიების მიზნებისთვის და შემდგომ გამოიყენება სისხლის სამართლის დევნის მიზნით, ეს ორი მოქმედება განსხვავებულ მიზნებს ემსახურება, თუკი შესაბამისი სისხლის სამართლის გამოძიება უშედეგოდ დასრულდა.[8]

მონაცემების მიზანმიმართულ დამუშავებასთან ასევე მჭიდროდ არის დაკავშირებული მონაცემთა მინიმიზაციის პრინციპი, რომელიც გულისხმობს, რომ დამუშავების მიზნებისთვის შეუსაბამო მონაცემები უნდა განადგურდეს. ასევე ის პრინციპი, რომლის თანახმად, არ შეიძლება იმაზე მეტი ვადით მონაცემების შენახვა, ვიდრე ეს საჭიროა იმ მიზნებისთვის, რომელთათვისაც ისინი თავდაპირველად შეგროვდა, ან სხვა ლეგიტიმური მიზნებისთვის, როგორებიცაა არქივირების ან სტატისტიკის შედგენის მიზანი. [9]

მონაცემების კანონიერად მოპოვების პარალელურად, არანაკლებ მნიშვნელოვანია მოპოვებული მონაცემების უსაფრთხოების დაცვის საკითხი, რასაც პრინციპის დონეზე ითვალისწინებს საპოლიციო დირექტივაც. ეს განსაკუთრებით მნიშვნელოვანია სამართალდამცავი ორგანოების საქმიანობის სპეციფიკის გათვალისწინებით, ვინაიდან მათ ხშირად უწევთ განსაკუთრებული კატეგორიის მონაცემების დამუშავება და მისი გამჟღავნება მნიშვნელოვანი ზიანის მომტანი შეიძლება აღმოჩნდეს მონაცემთა სუბიექტებისთვის როგორც პერსონალური მონაცემების, ასევე პირადი

[8] CJEU, C-180/21, Inspektor v. Inspektorata kam Visshia sadeben savet, (2022), 44.

[9] ძირითად უფლებათა სააგენტო (FRA), ევროსაბჭო (CoE), ადამიანის უფლებათა ევროპული სასამართლო (ECHR). მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო (თარგმ.), 2018, გვ. 143-144.

ცხოვრების უფლების დარღვევის თვალსაზრისით. ამ საფრთხეების თავიდან ასაცილებლად შესაბამის ორგანოში უნდა არსებობდეს მონაცემებზე დაშვების სპეციალური რეგულაცია და ხელმისაწვდომობა განსაზღვრული უნდა იყოს საჭიროების მიხედვით. შესაძლებელი უნდა იყოს იმის დადგენა, თუ ვის და რა მიზნით ჰქონდა წვდომა მონაცემებზე, ეფექტიანი კონტროლის მექანიზმების გამოყენებით.

ერთ-ერთ მნიშნელოვან პრინციპს, რომელიც ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციით“ არის გათვალისწინებული, წარმოადგენს გამჭვირვალობა.[10] საპოლიციო დირექტივა გამჭვირვალობას პრინციპის დონეზე არ აწესრიგებს. მიუხედავად ამისა, მისი პრეამბულის 26-ე პუნქტში აღნიშნულია, რომ პერსონალური მონაცემების ნებისმიერი დამუშავება უნდა იყოს კანონიერი, სამართლიანი და გამჭვირვალე შესაბამისი ფიზიკური პირების მიმართ და დამუშავდეს მხოლოდ კანონით დადგენილი კონკრეტული მიზნებისთვის. ეს არ უშლის ხელს სამართალდამცავ ორგანოებს, განახორციელონ ისეთი საქმიანობა, როგორიცაა ფარული გამოძიებები ან ვიდეომეთვალყურეობა.[11] გარდა ამისა, საპოლიციო დირექტივის მე-12 მუხლი ითვალისწინებს მონაცემთა სუბიექტის ინფორმირების საკითხს, რაც გულისხმობს მონაცემთა სუბიექტისთვის ინფორმაციის ლაკონიურად, გასაგები და ადვილად ხელმისაწვდომი ფორმით მიწოდებას.[12] დირექტივაში არსებული ეს ჩანაწერი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციისგან“ იმით განსხვავდება, რომ დამუშავებისთვის პასუხისმგებელი პირი ვალდებული არ არის, პროაქტიულად აცნობოს მონაცემთა სუბიექტს, არამედ მხოლოდ ხელმისაწვდომი უნდა გახადოს ასეთი ინფორმაცია. გარდა ამისა, დირექტივა შეიცავს გამონაკლისებს ინფორმაციის მიღების უფლებისა და მონაცემთა სუბიექტების მიერ წვდომის უფლებისგან, როდესაც ამ უფლებების დაცვამ შეიძლება ხელი შეუშალოს სამართალდამცავი ორგანოების სათანადო ფუნქციონირებას.[13] ამ საკითხზე უფრო სიღრმისეულად შემდეგ თავში გვექნება საუბარი.

დასკვნის სახით შეიძლება ითქვას, რომ დირექტივით გათვალისწინებული პრინციპები, მნიშვნელოვნად განსხვავდება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ ექვივალენტური დებულებებისგან. ისინი შექმნილია სპეციალურად სამართალდამცავი ორგანოების საჭიროებებისა და მათი დამუშავების საქმიანობის კონკრეტული ხასიათისთვის. აღნიშნული შეესაბამება პოლიციისა და სისხლის სამართლის ორგანოების მიერ მონაცემთა დამუშავების სპეციფიკას, რომელიც აღიარებულია ლისაბონის ხელშეკრულების თანდართულ 21-ე

[10] მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 5, პ. 1(a).
[11] საპოლიციო დირექტივის პრეამბულა, პუნქტი 26.
[12] იქვე, მუხლი 12.
[13] *Kosta E., Boehm F.*, The EU Law Enforcement Directive (LED): A Commentary. 2024, 147.

დეკლარაციაში.[14] მეორე მხრივ, განსხვავებები შეიძლება აღიქმებოდეს, როგორც ევროკავშირის კანონმდებლობით მონაცემთა სუბიექტებისთვის მინიჭებული დაცვის საერთო დონის შესუსტებად და პოლიციისა და სისხლის სამართლის ორგანოებისთვის ძალიან დიდი თავისუფლების შეთავაზებად, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ დაფარულ საჯარო სექტორის დანარჩენ ნაწილთან შედარებით.

5. მონაცემთა სუბიექტის უფლებები

ევროპაში მონაცემთა სუბიექტის უფლებები მონაცემთა დაცვის კანონმდებლობის ძირითადი კომპონენტია. საპოლიციო დირექტივის ზოგადი მიზანია მონაცემთა სუბიექტების უფლებების გაძლიერება. აღნიშული მიზნის უზრუნველსაყოფად იგი ითვალისწინებს ევროკავშირის წევრი სახელმწიფოების ვალდებულებას, შეიმუშაონ ისეთი მექანიზმები, რომლებიც უზრუნველყოფს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების ვალდებულებას, ხელი შეუწყონ მონაცემთა სუბიექტის უფლებების რეალიზებას.

5.1. ინფორმაციაზე წვდომის უფლება

მონაცემთა სუბიექტის უფლება ინფორმაციის ხელმისაწვდომობაზე გულისხმობს მისთვის გასაგები ფორმით ინფორმაციის მიღებას დამუშავებისთვის პასუხისმგებელი პირის შესახებ, მონაცემთა დამუშავების მიზნების შესახებ, რომლებისთვისაც მუშავდება მონაცემები. ასევე, უფლებას საზედამხედველო ორგანოსთვის მიმართვის შესახებ და ინფორმაცია მონაცემთა სუბიექტთან დაკავშირებულ მონაცემებთან წვდომის, მათი გასწორების, წაშლის ან დამუშავების შეზღუდვის მოთხოვნის დამუშავებისთვის პასუხისმგებელი პირისთვის წარდგენის უფლების არსებობის შესახებ. გარდა ამისა, კონკრეტულ შემთხვევებში და საკუთარი უფლებების განხორციელების მიზნით, მონაცემთა სუბიექტს უნდა ეცნობოს დამუშავების სამართლებრივი საფუძვლისა და მონაცემების შენახვის ხანგრძლივობის შესახებ იმდენად, რამდენადაც ასეთი დამატებითი ინფორმაცია აუცილებელია იმ კონკრეტული გარემოებების გათვალისწინებით, რომლებშიც მონაცემები მუშავდება, რათა უზრუნველყოფილი იყოს მონაცემთა სუბიექტის მონაცემების მიმართ სამართლიანი დამუშავება.[15] თუმცა ინფორმაციის მიღების უფლება არ არის აბსოლუტური და ექვემდებარება შეზღუდვას. ეს დაკავშირებულია

[14] Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (2007). 12007L/AFI/DCL/21.

[15] საპოლიციო დირექტივა, მუხლი 13, პ. 2.

სამართალდამცავი ორგანოების საქმიანობის სპეციფიკასთან და სახელმწიფოს აქვს უფლება, რომ სუბიექტისთვის ინფორმაციის მიწოდებასთან დაკავშირებით გაითვალისწინოს გარკვეული ხასიათის გამონაკლისები. ბუნებრივია, ამ შემთხვევაში საჭიროა ერთგვარი ბალანსის დაცვა, სუბიექტის უფლების, მასთან დაკავშირებული ინფორმაციის მიწოდების აუცილებლობასა და სამართალდამცავი ორგანოს საქმიანობისთვის საფრთხის შექმნის თავიდან აცილების გათვალისწინებით, რა დროსაც შესაძლებელია აღნიშნული ორგანო მონაცემებს ამუშავებდეს ფარული მეთოდებით. ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეზე "Roman Zakharov v. Russia" ხაზგასმით აღნიშნა გარემოება, რომ ფარული საგამოძიებო მოქმედებების შემდეგ პირისთვის შეტყობინების განხორციელება დაკავშირებულია სასამართლოში სამართლებრივი დაცვის ეფექტიანობასთან. სასამართლო აღნიშნავს, რომ რუსეთის კანონმდებლობა არ იძლევა საიდუმლო თვალთვალის ზომებისაგან ეფექტიანი სამართლებრივი დაცვის საშუალებას მაშინ, როდესაც მიყურადების ობიექტის წინააღმდეგ არ არის აღძრული სისხლის სამართლის საქმე. შედეგად, „ეროვნული სამართლებრივი დებულებანი, რომლებიც არეგულირებს კომუნიკაციების მიყურადებას, არ იძლევა ადექვატური და ეფექტიანი დაცვის გარანტიებს თვითნებობისა და უფლების დარღვევის საფრთხისაგან. ეროვნული კანონმდებლობა არ აკმაყოფილებს „კანონის ხარისხის" მოთხოვნას და ვერ ინარჩუნებს „ჩარევას" იმ მასშტაბით, რომელიც გახლავთ „აუცილებელი დემოკრატიულ საზოგადოებაში".[16]

რაც შეეხება საპოლიციო დირექტივას, იგი შესაძლებლობას აძლევს ევროკავშირის წევრ სახელმწიფოებს, სამართლებრივი საფუძვლის არსებობის შემთხვევაში, შეზღუდონ მონაცემთა სუბიექტის უფლებები ინფორმაციაზე წვდომის თვალსაზრისით, თუ არსებობს ლეგიტიმური ინტერესი, ჩარევა აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში და არსებობს სამართალდამცავი ორგანოებისთვის ხელის შეშლის საშიშროება. ანუ, თუ ეს აუცილებელია დანაშაულის პრევენციის, გამოძიების, სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების ხელის შეშლის აღკვეთის მიზნით. ასევე, თუ ეს მნიშვნელოვანია საზოგადოებრივი და ეროვნული უსაფრთხოების დასაცავად და სხვათა უფლებებისა და თავისუფლებების დასაცავად.[17]

შეჯამებისთვის შეიძლება ითქვას, რომ, ამ მხრივ, საპოლიციო დირექტივის მიზანია პირს ჰქონდეს ინფორმაცია მისი მონაცემების დამუშავების შესახებ, რათა დაცული იყოს სხვისი მხრიდან მონაცემების ბოროტად გამოყენებისგან. ამასთან, ასეთი უფლება შეიძლება დაექვემდებაროს შეზღუდვას, თუმცა იმ ფარგლებში, რამდენადაც ეს მკაცრად აუცილებელია.[18]

[16] ECtHR, Roman Zakharov v. Russia, (Application no. 47143/06), VII.
[17] საპოლიციო დირექტივა, მუხლი 13, პ. 3.
[18] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 256.

5.2. მონაცემებზე წვდომის უფლება

სუბიექტების უფლებების დასაცავად საპოლიციო დირექტივა ასევე ითვალისწინებს მონაცემებზე წვდომის შესაძლებლობას, რაც გულისხმობს სუბიექტის უფლებას, ჰქონდეს წვდომა მის შესახებ დამუშავებულ და შენახულ მონაცემებზე. აგრეთვე, იცოდეს ამ მონაცემების კატეგორიები, დამუშავების მიზნები და სამართლებრივი საფუძველი, რომლებიც ადასტურებს მის შესახებ ინფორმაციის დამუშავების კანონიერებას.[19] თუკი შესაძლებელია, სუბიექტს უნდა მიეწოდოს ინფორმაცია დამუშავების პერიოდულობისა და მონაცემების გადაცემის შესახებ, თუ ვის და სად გადაეცა ინფორმაცია და ვინ არის ამ ინფორმაციის მიმღები. სუბიექტს უფლება აქვს, ასევე იცოდეს დამუშავებისთვის პასუხისმგებელი პირის მხრიდან მონაცემების გასწორების, წაშლის ან დამუშავების შეზღუდვის შესახებ. აგრეთვე, საზედამხედველო ორგანოში საჩივრის შეტანის შესახებ.[20] საპოლიციო დირექტივის მე-14 მუხლის მიზანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ხელი შეუწყოს სუბიექტს, მისთვის გასაგები და ხელმისაწვდომი ფორმით ჰქონდეს წვდომა მის შესახებ არსებულ მონაცემებზე, იმ შემთხვევაში, თუ ასეთი მონაცემების დამუშავებას აქვს ადგილი.

ადამიანის უფლებათა ევროპული სასამართლოს მოსაზრებით, ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის მე-8 მუხლით გათვალისწინებული სახელმწიფოს პოზიტიური ვალდებულება მოითხოვს, რომ უზრუნველყოს ეფექტიანი და ხელმისაწვდომი პროცედურა, რომელიც განმცხადებლებს საშუალებას მისცემს, ჰქონდეთ წვდომა კონკრეტული მიზნებისთვის აუცილებელ ყველა შესაბამის ინფორმაციაზე.[21] თუმცა უნდა აღინიშნოს, არც ინფორმაციაზე წვდომის უფლება არ არის აბსოლუტური ხასიათისა. ამ შემთხვევაშიც საჭიროა დაბალანსებული მიდგომის არსებობა, სამართალდამცავი ორგანოების საქმიანობის საჭიროებიდან გამომდინარე, რათა ინფორმაციის გამჟღავნებამ შესაძლებელია ხელი შეუშალოს მათი საქმიანობის ძირითად მიზნებს. შესაბამისად, დირექტივა, გამონაკლისის სახით, ითვალისწინებს აღნიშნული უფლების შეზღუდვის საფუძველს და ასეთ შემთხვევაში დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას დოკუმენტაციის შედგენის თაობაზე.[22] წვდომის უფლებაზე შეზღუდვები შეიძლება დაწესდეს ინდივიდუალური შემთხვევის გარემოებიდან გამომდინარე. ამასთან, წვდომის უფლების სრული ან ნაწილობრივი შეზღუდვისას საჭიროა ოთხი პირობის კუმულატიურად დაკმაყოფილება:

პირველი, ეს არის სამართლებრივი საფუძვლის არსებობა. სახელმწიფოს შეუძლია მიიღოს საკანონმდებლო ზომები შესაბამის სამართლებრივ აქტებში ცვლილებების შეტანის გზით, წვდომის უფლების განხორციელების

[19] საპოლიციო დირექტივა, მუხლი 14.
[20] იქვე.
[21] ECtHR, Yonchev v. Bulgaria (Application no. 12504/09), 50.
[22] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 284.

შეზღუდვის მიზნით. ბუნებრივია, ეს სამართლებრივი აქტები ხელმისაწვდომი უნდა იყოს შესაბამისი პირებისთვის და აკმაყოფილებდეს განჭვრეტადობის კრიტერიუმებს.

მეორე პირობა, რომელის დაკმაყოფილებაც აუცილებელია, არის ის, რომ მონაცემებზე წვდომის შეზღუდვა არ უნდა ხდებოდეს განუსაზღვრელი ვადით. იგი გარკვეული დროით და ფარგლებით შეიძლება დაწესდეს, რაც გულისხმობს დემოკრატიულ საზოგადოებაში აუცილებლობის, პროპორციულობის ტესტის დაკმაყოფილებას.

მესამე პირობა ითვალისწინებს სხვისი უფლებების პატივისცემის და ინტერესების გათვალისწინებას, რაც, მათ შორის, გარანტირებულია ევროკავშირისა და ევროპის საბჭოს მიერ მიღებული აქტებით.

მეოთხე პირობა, რომელიც მონაცემებზე წვდომის შეზღუდვის მოთხოვნას უნდა აკმაყოფილებდეს, არის ის, რომ იგი უნდა ემსახურებოდეს სამართლებრივი მოკვლევის, გამოძიების ან პროცედურების ხელის შეშლის თავიდან აცილებას, დანაშაულის პრევენციას, გამოვლენას, გამოძიებას, სისხლისსამართლებრივი დევნის ან სასჯელის აღსრულების თავიდან აცილებას. აგრეთვე, საზოგადოებრივი და ეროვნული უსაფრთხოების დაცვის უზრუნველყოფას და სხვათა უფლებების დაცვას.[23] ადამიანის უფლებათა ევროპული სასამრთლოც დასაშვებად მიიჩნევს ინფორმაციაზე წვდომის უფლების შეზღუდვას. კერძოდ, საქმეზე – ”Segerstedt-Wiberg And Others v. Sweden” – სასამართლომ აღიარა სადაზვერვო სამსახურების ლეგიტიმურად არსებობის შესაძლებლობა, ხოლო მოქალაქეებზე ფარული თვალთვალის დასაშვებობა, ვინაიდან, კონვენციის თანახმად, აღნიშნული მკაცრად აუცილებელია დემოკრატიული ინსტიტუტების დასაცავად. ამასთან, სასამართლო მიიჩნევს, რომ სახელმწიფოს ინტერესი ეროვნული უსაფრთხოების დაცვასა და ტერორიზმთან ბრძოლაში უნდა იყოს დაბალანსებული პირადი ცხოვრების პატივისცემის უფლებაში ჩარევის ხარისხთან.[24]

მეხუთე მიზანი შეეხება სხვათა უფლებებისა და თავისუფლებების დაცვას. ამ შემთხვევაში უპირატესად იგულისხმება სამართალდამცავი ორგანოების მიერ გამოძიების პროცესში მოპოვებული მონაცემების დაცვა, რომლებიც შეიძლება შეიცავდეს პოტენციური მსხვერპლის, მოწმის ან სხვა მონაწილე სუბიექტის პერსონალურ მონაცემებს.[25] მონაცემთა სუბიექტს უფლება აქვს, იცოდეს მონაცემებზე წვდომის შეზღუდვის შესახებ, შეზღუდვის მიზეზების ახსნის მითითებით, თუ ეს ხელს არ შეუშლის ზემოთ ჩამოთვლილი მიზნების მიღწევას, რათა საჭიროების შემთხვევაში მან შეძლოს ამ გადაწყვეტილების გასაჩივრება.

[23] საპოლიციო დირექტივა, მუხლი 15.
[24] ECtHR, Segerstedt-Wiberg and Others v. Sweden (Application no. 62332/00), 88.
[25] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 290.

5.3. მონაცემთა დამუშავების გასწორება, წაშლა და შეზღუდვა

დირექტივა, მონაცემთა სუბიექტის უფლებების დაცვის მიზნით, ასევე ითვალისწინებს ისეთი მექანიზმების არსებობას, როგორებიცაა მონაცემთა დამუშავების გასწორება, წაშლა და შეზღუდვა.[26] ეს მექანიზმები ხელს უწყობს მონაცემთა სუბიექტს, მოახდინოს შესაბამისი რეაგირება, როდესაც მისი მონაცემის კანონის დარღვევით მუშავდება. იმ შემთხვევაში, თუ საგამოძიებო ორგანოებში ინახება არაზუსტი მონაცემები, აღნიშნული უფრო მეტად ზრდის სუბიექტის უფლებების დარღვევის რისკებს. მონაცემების გასწორების საჭიროება ძირითადად მაშინ წარმოიშვება, როცა სუბიექტის შესახებ ინფორმაცია არასწორია ან ფაქტობრივი შეცდომებით არის შეტანილი სამართალდამცავი ორგანოების მონაცემთა ბაზებში. მაგალითად, პირის შესახებ ბიომეტრიულ მონაცემებს შეიძლება არასწორად ინახავდეს პოლიცია, რამაც შეიძლება არსებითი გავლენა მოახდინოს მის პირად ცხოვრებაზე.

რაც შეეხება მონაცემების წაშლის საკითხის, აღნიშნული სუბიექტის უფლებასა და დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას წარმოადგენს იმ შემთხვევაში, თუ დარღვეულია მონაცემთა დამუშავების პრინციპები და საფუძვლები, განსაკუთრებული კატეგორიის მონაცემების დამუშავება მოხდა კანონის დარღვევით ან მონაცემების წაშლა გამომდინარეობს დამუშავებისთვის პასუხისმგებელი პირის სამართლებრივი ვალდებულებიდან. ასევე, მნიშვნელოვანია, მონაცემთა დროული წაშლის უზრუნველყოფაც. აღსანიშნავია, რომ ადამიანის უფლებათა ევროპული სასამართლომ მონაცემების წაშლის უფლებასთან დაკავშირებით დაადგინა პირადი ცხოვრების უფლების დარღვევა მაშინ, როდესაც პოლიციის ორგანოების მონაცემთა ბაზებში ბრალდებულების შესახებ ინფორმაცია კანონოთ დადგენილი ვადაზე მეტი ხნით ინახებოდა.[27] მონაცემების წაშლის ნაცვლად დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეზღუდოს მონაცემების დამუშავება იმ შემთხვევაში, როდესაც მონაცემების ნამდვილობა სადავოა და სიზუსტის დადგენა შეუძლებელია. ასეთ დროს დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, აცნობოს ამის შესახებ სუბიექტს დამუშავების შეზღუდვის მოხსნამდე ან მონაცემების დამუშავება აუცილებელია მტკიცებულების მიზნებისთვის.

საგულისხმოა, რომ მონაცემთა სუბიექტის ზემოხსენებული უფლებებიც არ არის აბსოლუტური ხასიათის, რათა მათი განხორციელებით ხელი არ შეეშალოს სამართალდამცავი ორგანოების კანონიერი ამოცანების შესრულებას. მონაცემთა სუბიექტის უფლებებიც შესაძლებელია, რომ იმავე მიზნების მიღწევის უზრუნველსაყოფად შეიზღუდოს, რომლებიც სუბიექტის მხრიდან მონაცემების წვდომის უფლების შეზღუდვის საკითხზე იქნა აღნიშნული.[28]

[26] საპოლიციო დირექტივა, მუხლი 16.
[27] ECtHR, S. And Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), 119, 124.
[28] საპოლიციო დირექტივა, მუხლი 16.

5.4. მონაცემებზე არაპირდაპირი წვდომის უფლება

მონაცემთა სუბიექტის უფლებების განხორციელების უზრუნველსაყოფად დირექტივა ითვალისწინებს დამატებითი გარანტიების არსებობას, როდესაც სუბიექტს შეზღუდული აქვს ინფორმაციის მიღების, მასზე წვდომის, გასწორების ან წაშლის უფლება. აღნიშნული მექანიზმის მიზანია სუბიექტის უფლებებისა და საგამოძიებო ორგანოების საქმიანობას შორის დაბალანსებული მიდგომის არსებობა. იმ შემთხვევაში, თუ მონაცემთა სუბიექტს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი არ აძლევს მონაცემებზე ინფორმაციას, მასზე წვდომის, გასწორების ან წაშლის უფლებას, მოცემულ შემთხვევაში მონაცემთა სუბიექტს ეროვნული საზედამხედველო ორგანოს საშუალებით არაპირდაპირი წვდომის შესაძლებლობა ეძლევა. აღნიშნული გულისხმობს მის უფლებას, მოსთხოვოს საზედამხედველო ორგანოს, შეამოწმოს მონაცემთა დამუშავების კანონიერება. ამ უფლების ცოდნის შესახებ ინფორმაციის მიწოდების ვალდებულება დამუშავებისთვის პასუხისმგებელი პირის პრეროგატივას განეკუთვნება, ხოლო საზედამხედველო ორგანო ვალდებულია, მონაცემთა სუბიექტს აცნობს შემოწმების შედეგები. ასევე, განუმარტოს სასამართლოში მიმართვის უფლება.[29]

5.5. მონაცემების დამუშავება ეროვნული კანონმდებლობის მიხედვით

დირექტივა ითვალისწინებს ევროკავშირის წევრი სახელმწიფოების შესაძლებლობას, სისხლის სამართლის საქმეზე გამოძიებისა და სასამართლო წარმოების ფარგლებში (იგულისხმება მოწმეთა ჩვენებები, ჩხრეკის და ფარული მიყურადების დროს მოპოვებული პერსონალური მონაცემები და სხვა) ინფორმაციაზე წვდომის, მონაცემების გასწორებისა და წაშლის უფლება, ასევე დამუშავების შეზღუდვა ეროვნული კანონმდებლობის შესაბამისად.[30] აღნიშნული ხაზს უსვამს სახელმწიფოს სუვერენიტეტის მნიშვნელობას გამოძიებისა და სასამართლოს წარმოების პროცესში. თუმცა ეს სამართლებრივი შესაძლებლობა არ აძლევს სახელმწიფოებს უფლებას, ხელი შეუშალოს ან კიდევ უფრო შეზღუდოს სუბიექტის უფლებები. პირიქით, წევრი სახელმწიფოს შესაბამისი სფეროს კანონმდებლობა სუბიექტის უფლებების დაცვის გარანტიებს უნდა ქმნიდეს, მიუხედავად მათი სამართლებრივი მოწყობისა.[31] ამ შემთხვევაში სახელმწიფოებს ექნებათ მეტი მოქნილობის შესაძლებლობა სამართლებრივი და ტექნიკური თვალსაზრისით, თუმცა არა

[29] იქვე, მუხლი 17.
[30] იქვე, მუხლი 18.
[31] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 322.

სუბიექტის უფლებების შეზღუდვის ხარჯზე, არამედ ეროვნულ კანონმდებლობაში მინიმალური მექანიზმების შემოღების გზით.

მიუხედავად იმისა, რომ მოცემული ნაშრომის მიზანი არ არის საქართველოს კანონმდებლობის შედარება საპოლიციო დირექტივასთან, ზოგადად შეიძლება მსჯელობა იმის თაობაზე, თუ რამდენად არის შესაბამისობაში მონაცემთა დაცვის ეროვნული კანონმდებლობა ხსენებული დირექტივის მიზნებთან. ის ფაქტი, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება არ ვრცელდება დანაშაულის თავიდან აცილების, გამოძიების, სისხლისსამართლებრივი დევნის, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისთვის სახელმწიფო საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ნახევრად ავტომატური საშუალებებით დამუშავებასა და არაავტომატური საშუალებებით დამუშავებაზე,[32] თავსებადი ვერ იქნება საპოლიციო დირექტივასთან.

6. დასკვნა

ნაშრომში განხილულია საპოლიციო დირექტივის მნიშვნელობა და მისი მიღების ძირითადი მიზანი. ასევე, გაანალიზებულია დირექტივით გათვალისწინებული მონაცემთა დამუშავების პრინციპები. ძირითადი მსჯელობა ეთმობა მონაცემთა სუბიექტის უფლებებს, როდესაც სამართალდამცავი ორგანოები სუბიექტის მონაცემებს ამუშავებენ დანაშაულის პრევენციის, გამოძიების, სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების, ასევე, საზოგადოებრივი და ეროვნული უსაფრთხოების დაცვის მიზნით. ნაშრომზე მუშაობისას გამოჩნდა, რომ, სისხლის სამართლის სფეროში პერსონალური მონაცემების დამუშავების სპეციფიკური ბუნებისა და მგრძნობელობის გათვალისწინებით, საჭირო იყო მონაცემთა დაცვის ზოგადი სამართლებრივი ჩარჩოსგან განსხვავებული წესების შემოღება. ამასთანავე, აუცილებელია, რომ ზემოაღნიშნული საკითხების ახლებურად მოწესრიგების პირობებში ადამიანის უფლებაში ჩარევა იყოს გამართლებული და უზრუნველყოფილ იქნას ბალანსის დაცვა, ერთი მხრივ, შესაბამისი სუბიექტის უფლებასა და, მეორე მხრივ, სამართალდამცავი ორგანოების ეფექტიანად ფუნქციონირებას შორის.

რა თქმა უნდა, საზოგადოებრივი უსაფრთხოების დაცვა და დანაშაულის პრევენცია/გამოძიება მნიშვნელოვან ამოცანას წარმოადგენს, თუმცა ეს არ უნდა მოხდეს ადამიანის უფლებების დარღვევის ხარჯზე. ამ დროს განსაკუთრებულია სახელმწიფოს პასუხიმგებლობა, რათა ორივე მიზანს მიაღწიოს დაბალანსებული ზომების მიღების საშუალებით, მათ შორის,

[32] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144- XIმს-Xმპ, 14/06/2023. მუხლი 2.

უზრუნველყოს მონაცემთა დაცვის განსხვავებული წესების შემოღება სისხლის სამართლის სფეროში. შედეგად, მიუხედავად სამართალდამცავი ორგანოებისთვის განსხვავებული ფუნქციების არსებობისა, მონაცემთა დაცვის ზოგადი სამართლებრივი წესები და მონაცემთა დაცვის სპეციალური რეჟიმი, რომლებიც შესაბამისი ორგანოებისთვის არის დამახასიათებელი, ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მოთხოვნებს თანაბრად უნდა ითვალისწინებდეს.

ბიბლიოგრაფია:

1. ძირითად უფლებათა სააგენტო (FRA), ევროსაბჭო (CoE), ადამიანის უფლებათა ევროპული სასამართლო (ECHR). მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო (თარგმ.), 2018.
2. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023.
3. Charter of Fundamental Rights of the European Union. Official Journal of the European Union C 326, 26.10.2012.
4. Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (2007). 12007L/AFI/DCL/21.
5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
6. *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary, 2024.
7. *Sajfert J., Quintel T.,* Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, 2017.
8. CJEU, C-180/21, Inspektor v. Inspektorata kam Visshia sadeben savet, (2022).
9. ECtHR, Yonchev v. Bulgaria (Application no. 12504/09), 2017.
10. ECtHR, Roman Zakharov v. Russia, (Application no. 47143/06). 2015.
11. ECtHR, S. And Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), 2008.
12. ECtHR, Segerstedt-Wiberg And Others v. Sweden *(*Application no. 62332/00).

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

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

დასაბუთებას (1958), რომელიც მოგვიანებით დაიხვეწა ლიკელის და სხვების მიერ (2001), როგორც 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.

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]

---

[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.

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

[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.

მიუხედავად, კვლევის ინდივიდუალური მონაწილის მათ ტომობრივ ჯგუფთან დაკავშირება კვლავ შესაძლებელი იყო.

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

[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.

ფარგლებში ფართოდ გამოიყენება,[18] ისევე როგორც ხელოვნურ ინტელექტთან დაკავშირებულ ახალ კვლევით სფეროებში.

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

[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.

[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].

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, 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

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

[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.

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. ”
>
> 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]

---

[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

„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 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,

---

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.

[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/>.

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.

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,

---

[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.

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 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

[34] *Nicholson W., Cohen G.,* Privacy in the Age of Medical Big Data, Nature Medicine 25, 2019, 37–43.
[35] *Muhlhoff R., Ruschemeier H.,* Predictive Analytics and the Collective Dimensions of Data Protection, 16.1 Law, Innovation and Technology, 2023.

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 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,

---

[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.

[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].

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 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,

[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].

[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].

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.

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

[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.

[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

იმიტომ, რომ ინფორმაციული ტექნოლოგიები სწრაფად ვითარდებოდა. თავიდან პროგრესი ნელი იყო, მსოფლიოს სხვადასხვა კუთხეში მცირე 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

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].

[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].

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, 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

[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).

[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.

უფლებები.[56] "GDPR"-ის ტიპის კანონები, ასევე, რთული მოსარგებია 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]

---

[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).

[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].

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 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]

---

[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.

[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

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 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

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.

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:

---

[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.

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.

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 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.

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

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

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 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,

[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].

[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].

- 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.

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

[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.

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:

- ჩართოთ “te ao Māori”-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

[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].

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

[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].

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, 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

[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].

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

[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].

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. “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.

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

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 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

[87] Id. პარაგრაფი 19.

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 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 "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

[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].

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 უფლებსა 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 დგანან? 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.

ჯუზეპე დ'აკვისტო*
ლუდოვიკა დე ბენედეტი**

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვის ჩარჩო მონაცემთა სანდო გაზიარების მიზნით**

1. მონაცემთა გაზიარების კონცეფცია

მონაცემები წარმოადგენს აუცილებელ აქტივს, რომლებიც ორგანიზაციებს ეხმარება მიაღწიონ თავიანთ დასახულ მიზნებს და შექმნან ღირებული პროდუქტი. მაგალითად, მონაცემების შეგროვება და ანალიზი შესაძლებელია მომხმარებლის გამოცდილების გაუმჯობესების, ბიზნეს ოპერაციების ოპტიმიზაციის ან ორგანიზაციის ინტერესებიდან გამომდინარე, ინოვაციების ხელშეწყობის მიზნით იყოს გამოყენებული.

თუმცა მონაცემები ხშირად სცილდება იმ ორგანიზაციების ფარგლებს, რომლებმაც თავდაპირველად შეაგროვეს და გამოიყენეს ისინი. სხვა წყაროებთან შერწყმისას მონაცემებს შეუძლიათ ახალი ინფორმაციის გენერირება, ახალი პროდუქტებისა და მომსახურების განვითარების მხარდაჭერა და როგორც სოციალური, ასევე ეკონომიკური ზრდის სტიმულირება. ამგვარად, თავდაპირველი ღირებულების მიღმა შესაძლებელია ერთი და იმავე მონაცემთა ნაკრებიდან დამატებითი ღირებულების მიღება.[1]

ამ დაკვირვების საფუძველზე, ბევრმა ორგანიზაციამ ხელი შეუწყო „მონაცემთა გაზიარების" კონცეფციას, რომელსაც შეუძლია მიიღოს მონაცემთა მართვის შიდა სტრატეგიების ფორმა ერთი კომპანიის ფარგლებში ან კანონმდებლობით განსაზღვრული სახით ეროვნულ ან საერთაშორისო დონეზე.[2] ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის

---

* Garante per la Protezione dei Dati Personali Italian Data Protection Authority.

** Institute of International Legal Studies (ISGI), Consiglio Nazionale delle Ricerche (CNR) - Italy.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. თბილისში გამართულ „ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის", რიგით 75-ე შეხვედრაზე წარდგენილი მოხსენების ტექსტს.

[1] According to the Organization for Economic Cooperation and Development (OECD), data access and sharing can help generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP when also including private-sector data (https://www.oecd.org/digital/data-governance/). The EU Commission forecasts that the value of the data economy in the EU27 area is expected to reach €829 billion by 2025, up from €301 billion in 2018 with a compound annual growth rate (CAGR) of more than 14% <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en> [01.06.2024].

[2] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [15.09.2025].

("OECD") თანახმად, მონაცემთა გაზიარება „გულისხმობს მონაცემებზე წვდომის უზრუნველყოფას სხვების მიერ გამოყენების მიზნით, შესაბამისი ტექნიკური, ფინანსური, სამართლებრივი ან ორგანიზაციული მოთხოვნების დაცვით".[3] „ის მოიცავს როგორც მონაცემების ხელახალ გამოყენებას კომერციული და არაკომერციული პირობითი მონაცემთა გაზიარების შეთანხმებების საფუძველზე, ასევე ღია მონაცემებს."[4]

უფრო ფართო და მრავალფეროვანი მონაცემთა ნაკრების შეგროვებით ორგანიზაციებს შეუძლიათ ინოვაციებისა და ზრდის ხელშეწყობა უფრო ფართო, საზოგადოებრივი ინტერესებიდან გამომდინარე. მაგალითად, როდესაც ჯანდაცვის სერვისების მიმწოდებლები მონაცემებს მკვლევრებს უზიარებენ, აღნიშნულით უმჯობესდება დიაგნოზების სიზუსტე და უფრო ეფექტიანი მკურნალობის საფუძველია. ანალოგიურად, როდესაც საჯარო ხელისუფლების მიერ მონაცემების გაზიარების პროცესში უმჯობესდება კოორდინაცია და კრიზისულ სიტუაციებში რეაგირება (პანდემიები ან სტიქიური უბედურებები), მონაცემთა გაზიარებამ შეიძლება საშუალება მისცეს ორგანიზაციებს მიიღონ ახალი ინფორმაცია, შეიმუშაონ ახალი პროდუქტები და მომსახურება საზოგადოებრივი სარგებლისთვის, რომელთა შექმნასაც ისინი სხვა შემთხვევაში ვერ შეძლებდნენ. აღნიშნულმა შეიძლება გააძლიეროს კონკურენტუნარიანობა, შესაბამისად, შეიქმნას სამუშაო ადგილები. ამიტომ მონაცემთა გაზიარებას აქვს პოტენციალი, გააუმჯობესოს გადაწყვეტილების მიღების პროცესი, შედეგი და, საბოლოოდ, სარგებელი მოუტანოს საზოგადოებას.

ამავდროულად, მონაცემთა გაზიარებას შეიძლება, მოჰყვეს გარკვეული რისკი და უარყოფითი შედეგები. ინდივიდუალური ზიანის გარდა (პირადი ცხოვრების ხელშეუხებლობის დარღვევა), ერთ-ერთი ყველაზე აქტუალური პრობლემა ჯგუფური დისკრიმინაციაა.[5] ეს ხდება მაშინ, როდესაც გაზიარებული მონაცემთა ნაკრებები გამოიყენება იმგვარად, რომ იქმნება დისკრიმინაციის ახალი ფორმები ან მძაფრდება კონკრეტული სოციალური ჯგუფების მიმართ მიკერძოება (ეთნიკური კუთვნილების სქესის, ასაკის, სოციალურ-ეკონომიკური სტატუსის და სხვა მახასიათებლებთან დაკავშირებით). მაშინაც კი, როდესაც მონაცემები ანონიმურია, ნიმუშებითა და კორელაციებით შეიძლება დაიდენტიფიცირდეს ის ჯგუფები, რომლებიც შემდეგ დიფერენცირებულ მოპყრობას ექვემდებარებიან. მაგალითად, გაზიარებულ მონაცემთა ნაკრებებზე დაფუძნებული ალგორითმული გადაწყვეტილების მიღებამ შეიძლება პირთა გარკვეული წრე არახელსაყრელ მდგომარეობაში ჩააგდოს კრედიტებზე, ჯანდაცვაზე ან დასაქმების

[3] *OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463, 2021* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463> [15.09.2025].

[4] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [15.09.2025].

[5] *Favaretto M., De Clercq E. & Elger B.S.,* Big Data and discrimination: perils, promises and solutions. A systematic review, J Big Data 2019, 6-12 <https://doi.org/10.1186/s40537-019-0177-4> [01.09.2025].

შესაძლებლობებზე წვდომის თვალსაზრისით[6]. ეს შეიძლება მოხდეს მონაცემთა „დაბინძურების“ გამო, რაც გამოწვეულია ისტორიულად დამახინჯებული მონაცემთა ნაკრებით ან მონაცემთა მაინერების მიერ შემოღებული სუბიექტური კლასობრივი ეტიკეტირებით. გარდა ამისა, შეიძლება არსებობდეს „შეგროვების მიკერძოება“, რაც გამოწვეულია კონკრეტული ჯგუფების სისტემატური არასაკმარისი ან გადაჭარბებული წარმოდგენით, რაც პოტენციურად იწვევს დისკრიმინაციულ ან არათანაბარ მოპყრობას[7].

სინამდვილეში, მონაცემთა გაზიარების შედეგად წარმოშობილი რისკები არ შემოიფარგლება მხოლოდ განზრახ ბოროტად გამოყენებით, არამედ შეიძლება, წარმოიშვას ერთი შეხედვით ნეიტრალური პრაქტიკიდანაც, როგორიცაა მონაცემთა მოდელის დიზაინი ან ტრენინგის მონაცემთა ნაკრების შერჩევა. ამიტომ სხვადასხვა ტიპის პოტენციური დისკრიმინაციის რისკის მოგვარება მოითხოვს პროაქტიული დაცვის ზომებს, მათ შორის მიკერძოების აუდიტს, სამართლიანობის შეფასებებს და ინკლუზიურ მმართველობას.

ამავდროულად, მონაცემთა გაზიარება ხშირად გულისხმობს პერსონალური მონაცემების დამუშავებას, რომლებიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. მონაცემთა გაზიარების პრაქტიკა ავტომატურად არ იწვევს მონაცემთა დაცვის უფლების დარღვევას, თუმცა, ვინაიდან გაზიარება გულისხმობს პერსონალური მონაცემების დამუშავებას, აუცილებელია მონაცემთა დაცვის პრინციპების მკაცრი დაცვა. ამ პრინციპების დაცვა უზრუნველყოფს მონაცემთა მწარმოებლებსა და მომხმარებლებს შორის ნდობის განმტკიცებას, რაც მნიშვნელოვანი ეკონომიკური ღირებულების გენერირების წინაპირობაა. გარდა ამისა, პერსონალური მონაცემების „საზოგადოებრივი სარგებლისთვის“ დამუშავებისას უმნიშვნელოვანესია იმის უზრუნველყოფა, რომ ამგვარი დამუშავება პროპორციული იყოს ძირითად საზოგადოებრივ ინტერესთან მიმართებით.

მონაცემთა დაცვის პრინციპების გათვალისწინებით, ორგანიზაციები არა მხოლოდ ამცირებენ მონაცემთა ბოროტად გამოყენების რისკებს, არამედ ქმნიან ხელსაყრელ გარემოს ინოვაციური თანამშრომლობისთვის.

მონაცემთა სათანადო დამუშავება გადამწყვეტია მონაცემთა სრული მნიშვნელობის გამოსავლენად, რადგან მას შეუძლია საზოგადოებაში ნდობის ჩამოყალიბება. მონაცემთა გაზიარების პროცესში ჩართულ პირებს სურთ ჰქონდეთ გონივრული მოლოდინი, რომ მათი მონაცემები გამოყენებული იქნება ეთიკური და ლეგიტიმური მიზნებისთვის.

---

[6] *d'Alessandro B., O'Neil C., La Gatta T.,* Conscientious Classification: a Data Scientist's Guide to Discrimination-Aware Classification, Big Data, 2017, 5(2), 120–34. *Schermer BW.*, The Limits of Privacy in Automated Profiling and Data Mining, Comput Law Secur Rev. 2011, 27(1), 45–52. *Kroll JA., Huey J., Barocas S., Felten EW., Reidenberg JR., Robinson DG., Yu HL*., Accountable algorithms, Univ Pa Law Rev. 2017, 165(3), 633–705.

[7] *Brayne S.,* Big Data surveillance: the case of policing, Am Sociol Rev. 2017, 82(5), 977–1008. *Barocas S., Selbst AD.,* Big Data's disparate impact. California Law Rev. 2016, 104(3), 671–732.

ამ მხრივ, მნიშვნელოვანი სტრატეგიაა "by-design" მიდგომა,[8] რომელიც სისტემების დიზაინში თავიდანვე მონაცემთა დაცვისა და ეთიკური მოსაზრებების ინტეგრირებას ითვალისწინებს. ამ მიდგომის გამოყენებით, ორგანიზაციებს შეუძლიათ გააძლიერონ მონაცემთა მართვის პრაქტიკა და უზრუნველყონ მონაცემთა პასუხისმგებლიანი და ეფექტიანი გაზიარება.

ამ მიდგომის მიხედვით, ტექნიკური და ორგანიზაციული ზომების ერთობლიობა (კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები, "PET"), ხელმისაწვდომია სხვადასხვა დონეზე.[9] ეს ტექნოლოგიები მიზნად ისახავს კონფიდენციალობის რისკების შემცირებას მონაცემების გაზიარებისას, მათ შორის, განსაკუთრებული კატეგორიის ან კონფიდენციალური ინფორმაციის, რითაც ხელი ეწყობა ინოვაციებს.

წინამდებარე სტატია მიმოიხილავს სამართლებრივ ინსტრუმენტებს, რომლებიც ხელს უწყობს მონაცემთა გაზიარებას, დაკავშირებულ რისკებს და მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ დამცავ ზომებს. განსაკუთრებული ყურადღება ეთმობა კონფიდენციალობის გამაძლიერებელ ტექნოლოგიებს როგორც სანდო მონაცემთა გაზიარების სამართლებრივ, ასევე ტექნიკურ ინსტრუმენტებსა და რეკომენდაციებს.

2. მონაცემთა გაზიარების ხელშემწყობი სამართლებრივი ინსტრუმენტები

მსოფლიოში კანონმდებლებს შორის მზარდი ინტერესი არსებობს მონაცემთა გაზიარების რეგულირების მიმართ, რაც აისახება როგორც ეროვნულ, ასევე საერთაშორისო დონეზე. ეს ტენდენცია ინოვაციის, ეკონომიკური კონკურენტუნარიანობისა და საზოგადოებრივი კეთილდღეობის ძირითადი ხელშემწყობი ფაქტორებია, მაგრამ მათი გაზიარება მნიშვნელოვან სამართლებრივ, ეთიკურ და სოციალურ გამოწვევებს წარმოშობს. ჯერ კიდევ 2019 წელს ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ ("OECD") 30-ზე მეტ ქვეყანაში 200-ზე მეტი მთავრობის ხელმძღვანელობით გამოავლინა ინიციატივა, რომელიც მიზნად ისახავდა მონაცემთა გაზიარების ხელშეწყობას. ამ ინიციატივების უმეტესობა (თითქმის 65%) საჯარო სექტორის მიერ შენახული მონაცემების გაზიარებაზეა ორიენტირებული, მაგრამ მნიშვნელოვანი ნაწილი (დაახლოებით 15%) კერძო სექტორში მონაცემთა გაზიარების ხელშეწყობის მიზანს ისახავს. აღსანიშნავია, რომ ამ ინიციატივების თითქმის ნახევარი პერსონალური მონაცემების გაზიარებას გულისხმობდა, რაც მონაცემთა დაცვისა და პირადი ცხოვრების

[8] Art. 25, 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 or GDPR).

[9] The United Nations guide on Privacy-Enhancing Technologies for official statistics. United nations Big Data 2023 <https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf> [25.09.2025].

ხელშეუხებლობის ჩარჩოსთან შესაბამისობის თვალსაზრისით პრობლემას ქმნიდა[10].

ქვემოთ წარმოგიდგენთ ბოლოდროინდელი ინიციატივების მაგალითს, რომლებიც მიზნად ისახავს (ეროვნული) მონაცემთა ნაკრებების შეგროვების, დამუშავებისა და გადაცემის რეგულირებას:

- ევროკავშირის მიერ ცოტა ხნის წინ განხორციელდა ორი საკანონმდებლო ინიციატივა, „მონაცემთა მმართველობის შესახებ ევროპული აქტი“[11] და „მონაცემთა შესახებ ევროკავშირის აქტი“[12], რომლებიც მიზნად ისახავს მონაცემთა გაზიარების ხელშეწყობას საჯარო და კერძო სექტორებში. „მონაცემთა მმართველობის შესახებ ევროპული აქტი“ ხელს უწყობს მონაცემთა გაზიარებას ზომების ერთობლიობის დადგენით, ასევე, საჯარო სექტორსა და ხელახლა მომხმარებელს შორის ახალ სახელშეკრულებო შეთანხმებებს. ანალოგიურად, „მონაცემთა შესახებ ევროკავშირის აქტი“ ადგენს მონაცემთა გაცვლის წესებს, ხსნის სახელშეკრულებო დისბალანსს და განსაზღვრავს იმ გარემოებებს, რომელთა არსებობის შემთხვევაშიც საჯარო სექტორის ორგანოებს შეუძლიათ წვდომა და მათზე კერძო კომპანიების მიერ შენახული მონაცემების გამოყენება ზოგადი მიზნებისთვის;
- „მონაცემთა ხელმისაწვდომობისა და გამჭვირვალობის შესახებ 2022 წლის კანონი“ (ავსტრალია)[13] ადგენს მონაცემთა გაზიარების სქემას, რომლის მიხედვითაც ორგანოები უფლებამოსილნი არიან, გაუზიარონ საჯარო სექტორის მონაცემები აკრედიტებულ მომხმარებლებს, ხოლო აკრედიტებულ მომხმარებლებს უფლებამოსილება აქვთ, შეაგროვონ და გამოიყენონ მონაცემები კონტროლირებადი გზით;[14]

---

[10] *The World Economic Forum*, *Good Data: Sharing Data and Fostering Public Trust and Willingness*, p. 6, 2021 <www.weforum.org/whitepapers/good-data-sharing-data-and-fostering-public-trust-and-willingness/> [10.09.2025] and *Organization for Economic Co-operation and Development, Economic and social benefits of data access and sharing* - in *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Chapter 3, OECD Publishing, 2019 <www.oecd-ilibrary.org//sites/276aaca8-en/1/2/3/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book> [15.09.2025].

[11] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44. <https://eur-lex.europa.eu/eli/reg/2022/868/oj> [15.09.2025].

[12] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023, p. 1-71. <https://eur-lex.europa.eu/eli/reg/2023/2854> [15.09.2025].

[13] Australian Data Availability and Transparency Act 2022 <www.datacommissioner.gov.au/law/dat-act> - Legal-Text available at: <www.legislation.gov.au/C2022A00011/latest/text> [01.06.2025].

[14] Sections 8 – 13 of the complementary “Data Availability and Transparency Act 2022” list “circumstances in which (data) sharing is barred”

- „მონაცემთა გაზიარების მმართველობის ჩარჩო“ (2022, დიდი ბრიტანეთი)[15] ადგენს დიდი ბრიტანეთის საჯარო სექტორის ორგანოებს შორის მონაცემთა გაზიარების სახელმძღვანელო პრინციპებს, ამასთან, ითვალისწინებს ასეთი გაზიარების ტექნიკურ (თანამედროვე სისტემებთან თავსებადობა, მონაცემთა განსხვავებული ფორმატები) და ორგანიზაციულ ბარიერებს;
- „კონფიდენციალობის დაცვისა და მონაცემთა გაზიარებისა და ანალიტიკის ხელშეწყობის ეროვნული სტრატეგია“ (2023, აშშ) მიზნად ისახავს აშშ-ის ფედერალური მთავრობის საჯარო სექტორის ორგანოებს შორის მონაცემთა გაზიარებისა და ანალიტიკის მნიშვნელოვან განვითარებას;[16]
- ამის საპირისპიროდ, ჩინეთის მიერ ცოტა ხნის წინ იქნა მიღებული რიგი ზომები, რომლებიც ორიენტირებულია ტრანსასაზღვრო მონაცემთა ნაკადების რეგულირებაზე. ესენია: პერსონალური ინფორმაციის გადაცემის ხელშეკრულების სტანდარტული პირობები (ძალაშია 2023 წლის 1 ივნისიდან)[17], ტრანსასაზღვრო მონაცემთა გადაცემის ხელშეწყობისა და რეგულირების შესახებ რეგულაციები (ძალაშია 2024 წლის 22 მარტიდან)[18] და ქსელურ მონაცემთა უსაფრთხოების მართვის რეგულაცია (ქსელური მონაცემების რეგულაცია) (ძალაშია 2025 წლის 1 იანვრიდან)[19]. აღნიშნული ინსტრუმენტების ერთობლიობა ასახავს შემზღუდველ და სუვერენიტეტზე ორიენტირებულ მიდგომას, რომელიც ცდილობს მონაცემებზე სახელმწიფო კონტროლის დამყარებას;
- საუდის არაბეთის მონაცემთა გაზიარების პოლიტიკა (مشاركة سياسة البيانات)[20] 2024 წელს დამტკიცდა და გამოიცა საუდის არაბეთის მონაცემებისა და ხელოვნური ინტელექტის ორგანოს ("SDAIA") მიერ. იგი მონაცემთა უსაფრთხო გაზიარების ყოვლისმომცველ ჩარჩოს ადგენს და

[15] Uk, Data Sharing Governance Framework, 2022 <www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework> [01.06.2025].

[16] Table 1 on Page 15 of this National Strategy lists technologies suitable for Privacy Preserving Data Sharing and Analytics.

[17] China, Measures for the Standard Contract for the Outbound Transfer of Personal Information, Cyberspace Administration of China, Decree No. 13 (effective 1 June 2023). Text available at the following link: <https://appinchina.co/government-documents/measures-for-the-standard-contract-for-outbound-transfer-of-personal-information/?utm_source=chatgpt.com> [20.09.2025].

[18] China, Provisions on Facilitating and Regulating Cross-Border Data Flow (effective 22 March 2024). Text and commentary available at: <www.chinalawupdate.cn/2024/04/articles/data-privacy/china-issues-regulations-on-facilitating-and-regulating-cross-border-data-flow/?utm_source=chatgpt.com> and <www.loc.gov/item/global-legal-monitor/2024-05-13/china-new-rules-on-cross-border-data-transfers-released/?utm_source=chatgpt.com> [20.09.2025].

[19] Regulation on Network Data Security Management (effective 1 January 2025), State Council Decree No. 790. Text available at the following link: <https://appinchina.co/government-documents/regulation-on-network-data-security-management/?utm_source=chatgpt.com> [20.09.2025]; official translation in English <https://english.www.gov.cn/policies/latestreleases/202409/30/content_WS66fab6c8c6d0868f4e8eb720.html?utm_source=chatgpt.com> [20.09.2025].

[20] SDAIA, Data Sharing Policy, 2024 <https://sdaia.gov.sa/en/SDAIA/about/Documents/DataSharingPolicyEN.pdf> [22.09.2025].

განსაზღვრავს მთავრობის მიერ მონაცემთა გაცვლის მკაფიო წესებს "Government Service Bus"-ისა და "Data Marketplace"-ის მეშვეობით, აწესებს მკაცრი ავტორიზაციისა და კლასიფიკაციის მოთხოვნებს და აფასებს კანონიერების, უსაფრთხოების, გამჭვირვალობისა და ეთიკური გამოყენების გარანტიებს. ასევე, პოლიტიკა აწესებს მოთხოვნის დამუშავებისთვის სავალდებულო ვადებს, ავალდებულებს ჩანაწერების წარმოებას და პირადი მონაცემების დაცვის კანონის დაცვის უზრუნველყოფას და "SDAIA"-ს ანიჭებს იმპლემენტაციისა და აღსრულების ზედამხედველობის უფლებამოსილებას.

აღნიშნული ინიციატივების ერთობლიობა მონაცემთა გაზიარების გლობალური მიდგომების განსხვავებულ მხარეებს ასახავს. მიუხედავად იმისა, რომ ევროკავშირი და ავსტრალია ფოკუსირებულია ნდობის განმტკიცებასა და მონაცემთა ხელახალი გამოყენების რეგულირებადი მექანიზმების შექმნაზე, დიდი ბრიტანეთი ხაზს უსვამს მმართველობასა და მოქნილობას, აშშ - კონფიდენციალობის დაცვის გაზიარების ტექნოლოგიურ გადაწყვეტილებებს, ჩინეთი იღებს სუვერენიტეტზე დაფუძნებულ მოდელს, რომელიც პრიორიტეტს ანიჭებს სახელმწიფო ზედამხედველობას, ხოლო საუდის არაბეთი ხაზს უსვამს წესებზე დაფუძნებულ, პრინციპებზე ორიენტირებულ სისტემას, რომელიც ორიენტირებულია უსაფრთხოებაზე, ეთიკურ გამოყენებასა და "SDAIA"-ს მეშვეობით სამთავრობათაშორისო კოორდინაციაზე. ამ განსხვავებების მიუხედავად, საერთო მნიშვნელია იმის აღიარება, რომ მონაცემთა გაზიარება აქტიურად უნდა იყოს რეგულირებული არა მხოლოდ ინოვაციისა და ზრდის პოტენციალის თვალსაზრისით, არამედ კონფიდენციალობის, სამართლიანობისა და ეროვნული უსაფრთხოების რისკების მოსაგვარებლად.

მიუხედავად ამისა, ქვეყნებს შორის ჰარმონიზებული მიდგომების ნაკლებობა, განსაკუთრებით პერსონალურ და კონფიდენციალურ მონაცემებთან დაკავშირებით, კვლავ ზღუდავს ტრანსასაზღვრო წვდომას. ეს ხარვეზი კვლავ გრძელდება საერთაშორისო მოწოდებების მიუხედავად, როგორებიცაა ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის რეკომენდაცია საჯარო სექტორის ინფორმაციაზე გაძლიერებული წვდომისა და უფრო ეფექტური გამოყენების შესახებ (2008)[21], ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის კანკუნის დეკლარაცია ციფრული ეკონომიკის შესახებ (2016)[22] და G20 ციფრული ეკონომიკის მინისტრთა დეკლარაცია (2024)[23], რომლებიც ხაზს უსვამს საერთაშორისო შეთანხმებებისა და თავსებადი კონფიდენციალობის

[21] *OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD, Paris, 2008* <https://legalinstruments.oecd.org/public/doc/122/122.en.pdf> [22.09.2025].
[22] *OECD, Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration), OECD, Paris, 2016* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0426> [22.09.2025].
[23] G20 Digital Economy Ministerial Conference, 2024 <https://www.g20.utoronto.ca/2024/240913-digital-ministerial-declaration.html> [15.09.2025].

ჩარჩოების შემუშავების მნიშვნელობას, რათა ხელი შეუწყოს იურისდიქციებს შორის მონაცემთა უსაფრთხო და სანდო ნაკადებს.

3. მონაცემთა გაზიარების სამართლებრივი არქიტექტურა

პერსონალური მონაცემების დამუშავების ფარგლებში მონაცემთა გაზიარება არ წარმოადგენს დაურეგულირებელ პროცესს. პირიქით, ის ინტეგრირებულია საერთაშორისო და რეგიონული სამართლებრივი ნორმების ქსელში, რომელიც მოითხოვს, რომ მონაცემთა გაზიარების ნებისმიერი პრაქტიკა უზრუნველყოფდეს მონაცემთა დაცვის ძირითადი პრინციპებისა და პირთა უფლებების დაცვას. აღნიშნული ვალდებულებები შეიძლება გამომდინარეობდეს რამდენიმე საერთაშორისო ინსტრუმენტიდან, განსაკუთრებით ევროპის საბჭოს კონვენციიდან პერსონალური მონაცემების ავტომატური დამუშავების დროს ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია), ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპებიდან პერსონალური მონაცემების კონფიდენციალობისა და ტრანსსასაზღვრო ნაკადების დაცვის შესახებ (1980, გადაიხედა 2013 წელს) და, ზოგადად, კონფიდენციალობის უფლებიდან, რომელიც გათვალისწინებულია სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტის ("ICCPR") მე-17 მუხლითა და ადამიანის უფლებათა ევროპული კონვენციის ("ECHR") მე-8 მუხლით.

გლობალურ დონეზე ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის ("OECD") სახელმძღვანელო პრინციპები კონფიდენციალობის დაცვისა და პერსონალური მონაცემების ტრანსსასაზღვრო ნაკადების შესახებ (პირველად მიღებული 1980 წელს და განახლებული 2013 წელს) კვლავ ერთ-ერთ პირველ და ყველაზე გავლენიან მცდელობად რჩება ტრანსსასაზღვრო მონაცემთა ნაკადების თანმიმდევრული ჩარჩოს უზრუნველყოფის მიმართულებით. ეს სახელმძღვანელო პრინციპები ადგენს ისეთ ძირითად პრინციპებს, როგორებიცაა მიზნის განსაზღვრა, მონაცემთა მინიმიზაცია და ანგარიშვალდებულება და კვლავაც წარმოადგენს როგორც ეროვნული კანონმდებლობის, ასევე საერთაშორისო მოლაპარაკებების ინფორმირების საშუალებას[24].

ანალოგიურად, გაერთიანებული ერების ორგანიზაციის ფარგლებში, სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტის ("ICCPR") მე-17 მუხლით გათვალისწინებული პირადი ცხოვრების ხელშეუხებლობის უფლება სულ უფრო ხშირად განიმარტება, როგორც ციფრული გარემოს იმგვარი გავრცობა, რომლითაც იზღუდება პერსონალური მონაცემების გაზიარების ან გადაცემის გზები იურისდიქციებს შორის.[25] ასევე,

[24] *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013 Revision. OECD, Explanatory memoranda of the OECD Privacy Guidelines, 2022, PP 11-12.*

[25] International Covenant on Civil and Political Rights (Adopted by General Assembly resolution 2200 (XXI) of 16 December 1966) (ICCPR), Art. 17: Right to privacy.

გაეროს გენერალურმა ასამბლეამ მიიღო მრავალი რეზოლუცია, რომლებიც აღიარებს პირადი ცხოვრების ხელშეუხებლობის დაცვის მნიშვნელობას ციფრული კომუნიკაციებისა და ტრანსასაზღვრო მეთვალყურეობის კონტექსტში, რაც ირიბად აყალიბებს მონაცემთა მმართველობის შესახებ გლობალურ სტანდარტებს.[26]

რეგიონულ დონეზე ევროპა მარეგულირებელი ცვლილებების სათავეში იდგა. ევროპის საბჭოს 108-ე კონვენცია (1981 წელი, გადაიხედა 2018 წელს) მონაცემთა დაცვის შესახებ ერთადერთი სავალდებულო საერთაშორისო ხელშეკრულებაა და ცალსახად მოიცავს მონაცემთა ტრანსსასაზღვრო ნაკადებს, ამავდროულად მოითხოვს მხარეებისგან, უზრუნველყონ შესაბამისი დაცვის სტანდარტები ტრანსასაზღვრო გადაცემების შემთხვევაში[27]. ევროკავშირის ფარგლებში „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”, რეგულაცია (EU) 2016/679) უზრუნველყოფს მონაცემთა დამუშავების ყოვლისმომცველ ჩარჩოს და ადგენს მკაცრ პირობებს მონაცემთა საერთაშორისო გადაცემისთვის. აღსანიშნავია, რომ, ევროპის მიღმა, სხვა რეგიონულ ორგანიზაციებსაც აქვთ განვითარებული მარეგულირებელი ჩარჩოები.[28]

წინამდებარე ინსტრუმენტები ცხადყოფს, რომ მონაცემთა გაზიარება აღარ რეგულირდება მხოლოდ ეროვნულ დონეზე, არამედ სულ უფრო მეტად ინტეგრირდება საერთაშორისო, რეგიონული და საერთაშორისო ჩარჩოების რთულ ქსელში. ეს ნორმატიული არქიტექტურა არა მხოლოდ აყალიბებს ეროვნულ კანონმდებლობას, არამედ უზრუნველყოფს ძირითად პრინციპებს (კანონიერება, სამართლიანობა, ანგარიშვალდებულება, უსაფრთხოება და პროპორციულობა), რომლებიც სახელმწიფოებმა უნდა გაითვალისწინონ საკუთარი პოლიტიკის შემუშავებისას.

წინამდებარე საერთაშორისო სტანდარტები მოიცავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის მოთხოვნების სერიას. უპირველესად, მათ მოეთხოვებათ შექმნან მონაცემთა მართვის თანმიმდევრული და ძლიერი ჩარჩოები, რათა უზრუნველყონ პერსონალური

[26] UN General Assembly Resolutions on the right to privacy in the digital age, e.g., A/RES/68/167 (2013).

[27] Council of Europe, Convention 108, 1981; modernized as Convention 108+, 2018, Arts. 5–7.

[28] აფრიკის კავშირის კიბერუსაფრთხოებისა და პერსონალური მონაცემების დაცვის შესახებ კონვენცია (მალაბოს კონვენცია, 2014) ადგენს წევრი სახელმწიფოების ვალდებულებებს მონაცემთა გაზიარებისა და გადაცემის შესახებ, ხოლო აზია-წყნარი ოკეანის რეგიონში APEC-ის ტრანსასაზღვრო კონფიდენციალობის წესების (CBPR) სისტემა ადგენს ნებაყოფლობით, აღსრულებად მექანიზმს მონაწილე ეკონომიკებს შორის სანდო მონაცემთა ნაკადის ხელშეწყობის მიზნით. ორმხრივ და პლურილტერალურ დონეზე რამდენიმე სავაჭრო შეთანხმება, როგორებიცაა ტრანს-წყნარი ოკეანის პარტნიორობის ყოვლისმომცველი და პროგრესული შეთანხმება (CPTPP) და USMCA (ამერიკის შეერთებული შტატები-მექსიკა-კანადის შეთანხმება), მოიცავს დებულებებს ტრანსასაზღვრო მონაცემთა ნაკადების შესახებ, რომლებიც ირიბად არეგულირებენ მონაცემთა გაზიარებას გაუმართლებელი შეზღუდვების აკრძალვით და ამავდროულად პერსონალური ინფორმაციის დაცვის მოთხოვნით.

მონაცემების მართვა პასუხისმგებლიანი და ეთიკური მიდგომით.[29] ასეთ ჩარჩოებს თან უნდა ახლდეს ყოვლისმომცველი რისკების შეფასებები, რომლებიც მიზნად ისახავს მონაცემთა გაზიარებასთან დაკავშირებული პოტენციური რისკების იდენტიფიცირებას. ეს მოიცავს კონფიდენციალობისა და მონაცემთა დაცვაზე ზეგავლენის შეფასებებს (PIAs/DPIAs), რაც ხელს უწყობს კონფიდენციალობასთან დაკავშირებული პოტენციური რისკების შეფასებას და შესაბამისი შემარბილებელი ზომების იდენტიფიცირებას.[30]

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ასევე ვალდებულნი არიან, მიიღონ მონაცემთა შენახვისა და განადგურების მკაფიო პოლიტიკა და პროცედურები, რათა უზრუნველყონ, რომ პერსონალური მონაცემები არ შეინახოს საჭიროზე მეტხანს და უსაფრთხოდ განადგურდეს. ანგარიშვალდებულების უზრუნველსაყოფად მათ უნდა ჩაატარონ მონაცემთა გაზიარების პროცესის რეგულარული შემოწმება და მიმოხილვა, რათა დაადასტურონ სამართლებრივ და მარეგულირებელ მოთხოვნებთან შესაბამისობა.

კიდევ ერთი მნიშვნელოვანი ელემენტია გამჭვირვალობა ფიზიკური პირების მიმართ, რაც გულისხმობს მონაცემთა სუბიექტების ინფორმირებას მათი პერსონალური მონაცემების გაზიარების შესახებ და მათთვის ინფორმაციის მიწოდებას უფლებების შესახებ, მათ შორის მონაცემებზე წვდომისა და მათი შესწორების უფლების შესახებ. ამავდროულად, მონაცემთა სიზუსტე და ხარისხი უნდა გაუმჯობესდეს ისეთი მექანიზმების მეშვეობით, როგორებიცაა მონაცემთა ვალიდაცია ან, საჭიროების შემთხვევაში, ასაკის დადასტურება.

გარდა ამისა, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა ჩაატარონ აუცილებლობისა და პროპორციულობის ტესტები, რათა მინიმუმამდე დაიყვანონ სხვა ორგანიზაციებისთვის გადაცემული პერსონალური მონაცემების მოცულობა, რითაც შემცირდება დარღვევებისა და კონფიდენციალობის დარღვევის რისკი. ასევე, მათ უნდა დაადგინონ პროცედურები მონაცემთა უსაფრთხოების დარღვევების პრევენციისა და მათზე რეაგირების მიზნით დაზარალებული პირების დასაცავად, შემამსუბუქებელი ზომების გატარების პარალელურად.

არანაკლებ მნიშვნელოვანია მონაცემთა გაზიარების შესახებ მრავალმხრივი შეთანხმებების მიღება, რომლებიც მკაფიოდ განსაზღვრავს გაზიარების მიზანს, ფარგლებს და პირობებს, მათ შორის, გაზიარებული მონაცემების გამოყენების შეზღუდვებს, კონფიდენციალობის ვალდებულებებსა და არაავტორიზებული ხელახალი იდენტიფიცირების

[29] Convention 108+ (Art. 10) explicitly requires controllers to adopt appropriate safeguards, while the GDPR (Art. 24) imposes the principle of accountability, obliging controllers to demonstrate compliance.

[30] როგორც 108-ე კონვენცია (მუხლი 10(3)), ასევე GDPR (მუხლი 35) ავალდებულებს მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) გამოყენებას იმ შემთხვევებში, როდესაც დამუშავება, სავარაუდოდ, დარღვევის მაღალ რისკებს შეუქმნის ინდივიდების უფლებებსა და თავისუფლებებს. ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპები ანალოგიურად ხაზს უსვამს პერსონალური მონაცემების ნაკადების მიმართ რისკზე დაფუძნებულ მიდგომებს.

შესახებ აკრძალვებს. ეს შეთანხმებები უნდა იყოს მხარდაჭერილი სასწავლო პროგრამებით, რომლებიც ხელს შეუწყობს მონაცემთა გაზიარებასთან დაკავშირებული რისკების შესახებ ცნობიერების ამაღლებას და საჭირო ცოდნისა და უნარების განვითარებას.

დაბოლოს, დამუშავებისთვის პასუხისმგებელი პირებისგან მოსალოდნელია მონაცემთა პორტირების მექანიზმების დანერგვა, რომლებიც მონაცემთა სუბიექტებს საშუალებას მისცემს, მიიღონ თავიანთი პერსონალური მონაცემები სტრუქტურირებული ფორმით, ან პირდაპირ გადასცენ ეს მონაცემები დამუშავებისთვის პასუხისმგებელ სხვა პირს.

4. მონაცემთა დაცვის რისკები მონაცემთა გაზიარებისას

თანამშრომლობის პოტენციური მნიშვნელობა ყოველთვის ყურადღებით უნდა შეფასდეს კონფიდენციალობის, მონაცემთა უსაფრთხოებისა და განსაკუთრებული კატეგორიის მონაცემების კონტროლის კუთხით. მონაცემთა გაზიარების კონცეფციასთან დაკავშირებულია რამდენიმე რისკი, რომელთა გათვალისწინებაც აუცილებელია პერსონალური მონაცემების დაცვის კონტექსტში არა მხოლოდ ინდივიდების უფლებების დასაცავად, არამედ ორგანიზაციებს შორის მდგრადი თანამშრომლობისთვის აუცილებელი ნდობის უზრუნველსაყოფად.[31]

ერთ-ერთი მთავარი გამოწვევა მონაცემთა სუბიექტებისა და საზოგადოების მხრიდან არასაკმარისი ცნობიერებაა იმის შესახებ, თუ რა ხდება მონაცემთა დამუშავებისას, რა არის მიზანი, სამართლებრივი საფუძველი, ბიზნეს მოდელი (რომელი გამოყენების შემთხვევებია გათვალისწინებული „მონაცემთა სივრცის“/„მონაცემთა გაზიარებისთვის“, მათ შორის, საზოგადოებაზე ეკონომიკური ინკლუზიურობისა და ურთიერთგაზიარების ხელშეწყობის თვალსაზრისით[32]).

ცნობიერების ნაკლებობა, რომელიც ძირითადად გამჭვირვალობის პრობლემატიკით არის გამოწვეული, ეწინააღმდეგება სამართლიანობისა და კანონიერების პრინციპებს საერთაშორისო და რეგიონულ დონეზე[33], რომლებიც მოითხოვს, რომ მონაცემთა სუბიექტები მკაფიოდ იყვნენ ინფორმირებულნი მათთან დაკავშირებული დამუშავების პროცესის შესახებ. ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპები კონფიდენციალობის დაცვისა და პერსონალური მონაცემების ტრანსსასაზღვრო ნაკადების შესახებ ასევე

[31] *OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019* <https://doi.org/10.1787/276aaca8-en> [20.09.2025].

[32] იხ.: for instance *Assessment of current and future impact of Big Data on Financial Services*, 2016, available at <https://finance.ec.europa.eu/system/files/2016-12/1606-big-data-on-financial-services_en_0.pdf> [06.09.2025].

[33] მაგალითად: 108-ე კონვენციის 5(4)(a) მუხლი და, რეგიონულ დონეზე, მონაცემთა დაცვის ზოგადი რეგულაციის 2016/679 (GDPR) 5(1)(a) მუხლი.

ითვალისწინებს გამჭვირვალობას, როგორც მონაცემთა ტრანსსასაზღვრო ნაკადების ძირითად პრინციპებს[34].

კიდევ ერთი გამოწვევა მონაცემთა დამუშავების პროცესში სამართლიანობის ნაკლებობაა, რაც ხშირად არასაკმარისი ტექნოლოგიური ან ორგანიზაციული დაცვის შედეგია. შესაბამისი მექანიზმების გარეშე პირები შეიძლება დაექვემდებაროონ არაგამჭვირვალე მონაცემთა დამუშავების პრაქტიკას, რაც ხელს უშლის მათ კონტროლის განხორციელებაში. ამასთან მჭიდრო კავშირშია მიზნის შეზღუდვის არარსებობა. მონაცემთა გაზიარების კონტექსტში დამუშავების ფარგლები ბუნდოვნად არის განსაზღვრული, აქტივობები განპირობებულია შემთხვევითი აღმოჩენით და არა სტრუქტურირებული, ჰიპოთეზებზე დაფუძნებული ან სამეცნიერო მიდგომით. ეს პრაქტიკა ეწინააღმდეგება მიზნის შეზღუდვის პრინციპს, რომლისთვისაც მონაცემები შეიძლება დამუშავდეს მხოლოდ განსაზღვრული, მკაფიო და ლეგიტიმური მიზნებისთვის და არ უნდა დამუშავდეს შემდგომში ისე, რომ არ შეესაბამებოდეს ამ მიზნებს[35].

მაშინაც კი, როდესაც ფიზიკური პირები და ორგანიზაციები ცალსახად თანხმდებიან მონაცემთა გაზიარებისა და ხელახალი გამოყენების კონკრეტულ პირობებზე, მათ შორის იმ მიზნებზე, რომელთათვისაც ლეგიტიმურად შეიძლება მონაცემების ხელახალი გამოყენება, კვლავ არსებობს მნიშვნელოვანი რისკი, რომ მესამე მხარეებმა, შეგნებულად ან უნებლიეთ, შეთანხმებული ჩარჩოდან გადახვევის გზით, მონაცემები ხელახლა გამოიყენონ. ფართოდ განხილული "Cambridge Analytica"-ს საქმე ამ რისკის ნათელი მაგალითია: "Facebook"-ის მომხმარებლების პერსონალური მონაცემები, რომლებიც თავდაპირველად შეგროვდა კვლევისთვის მიზნებისთვის, ხოლო შემდგომში გამოყენებული იქნა პოლიტიკური კამპანიისთვის. აღნიშნული განხორციელდა "Facebook"-ის მიერ მონაცემების „ნებისმიერი სარეკლამო ქსელისთვის, მონაცემთა ბროკერისთვის ან სხვა სარეკლამო ან მონეტიზაციასთან დაკავშირებული სერვისისთვის", გაყიდვის ან გადაცემის ცალსახა აკრძალვის მიუხედავად.[36]

"Cambridge Analytica"-ს ინციდენტი მხოლოდ ერთ-ერთია იმ მრავალ შემთხვევას შორის, როდესაც მონაცემების ხელახლა იქნა გამოყენებული. მნიშვნელოვანია, რომ ასეთი დარღვევები ყოველთვის არ არის ბოროტი განზრახვის შედეგი. მონაცემთა გაზიარება გულისხმობს მონაცემების ამოღებას ერთი კონტექსტიდან და მათ მეორეში გადატანას. როგორც ეს

[34] *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, Part Two: Basic Principles of National Application.*

[35] ეს პრინციპი, მაგალითად, გათვალისწინებულია ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპებში, 108-ე კონვენციის 5(4)(a) მუხლსა და GDPR-ის 5(1)(b) მუხლში.

[36] *Granville K.,* Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, The New York Times, 2018; *Isaak J. and Hanna M.*, User data privacy: Facebook, Cambridge Analytica, and Privacy Protection, Computer, Vol. 51/8, pp. 56-59, 2018.

შეიძლება გავიგოთ ნისენბაუმის კონფიდენციალობის თეორიის[37], როგორც კონტექსტური მთლიანობის მითითებით. კონტექსტში ნებისმიერი ცვლილება ართულებს არსებული უფლებებისა და ვალდებულებების შენარჩუნების უზრუნველყოფას. მაგალითად, მონაცემთა თავდაპირველი გამოყენებისას ნაგულისხმევი კონფიდენციალობის მოლოდინები შესაძლოა, აღარ გავრცელდეს შემდგომ ხელახალ გამოყენებაზე. მონაცემთა ხელახალ გამოყენებასთან დაკავშირებული რისკები დამოკიდებულია იმ კონტექსტზე, რომელშიც შეგროვდა მონაცემები და იმ ახალ კონტექსტზე, რომელშიც ისინი იქნება გამოყენებული. ამიტომ მონაცემთა გაზიარება და მისი გამოყენება დამატებითი მიზნებისთვის უნდა იყოს ინტეგრირებული გამჭვირვალობის, ანგარიშვალდებულებისა და დაცვის მყარ ჩარჩოში.

ასევე, რისკები ვრცელდება მონაცემთა დუბლირებასა და გავრცელებაზე კანონიერი ან ლეგიტიმური მიზნების მიღმა, რამაც შეიძლება დაარღვიოს როგორც შენახვის შეზღუდვის, ასევე მიზნის შეზღუდვის პრინციპები. გარდა ამისა, ხშირად ხდება მონაცემების არაეფექტიანი ან არასაჭირო გამოყენება. ეს ფენომენი, რომელიც შეიძლება შეფასდეს, როგორც „მონაცემთა ფლანგვა“, არა მხოლოდ იწვევს რესურსების არაეფექტურ განაწილებას, არამედ არღვევს მონაცემთა მინიმიზაციის პრინციპს[38] და მჭიდროდ უკავშირდება მონაცემთა უსაფრთხოების გაზრდილ რისკებს.

ფაქტობრივად, უსაფრთხოება კიდევ ერთი საზრუნავია. მასშტაბური მონაცემთა გაზიარება ხშირად გულისხმობს მონაცემების გადაცემას მრავალ ქსელსა და სისტემას შორის, რომელთაგან თითოეულს სხვადასხვა ორგანიზაცია მართავს განსხვავებული პოლიტიკით. აღნიშნული ზრდის უსაფრთხოების ინციდენტებისა და მონაცემთა დარღვევის ალბათობას, რაც პოტენციურად საფრთხეს უქმნის კონფიდენციალობას, მთლიანობას და ხელმისაწვდომობას.[39] გარდა ამისა, უკანონო წვდომა ან გამჟღავნება გაზრდილ რისკს წარმოადგენს, რადგან მონაცემები იცვლება მრავალ ორგანიზაციასა და სისტემას შორის და ამ შემთხვევებში, იურისდიქციებსა თუ სექტორებს შორის თანმიმდევრული მმართველობითი ჩარჩოების შექმნის სირთულემ შეიძლება კიდევ უფრო შელახოს დამუშავების კანონიერება.[40]

მონაცემთა ხარისხის შემცირება (“reduction in data quality”) არანაკლებ პრობლემურია, რადგან შეიძლება გამოიწვიოს არასწორი გადაწყვეტილებები და დისკრიმინაციული შედეგები. მონაცემთა წყაროების ჰეტეროგენულობამ, თუ სათანადოდ არ იქნება მოგვარებული, შეიძლება გამოიწვიოს შეუსაბამობები და შეცდომები, რომლებითაც დაირღვევა მონაცემთა სიზუსტის პრინციპი.[41] ამ უზუსტობამ ასევე შეიძლება გავლენა იქონიოს

[37] *Nissenbaum H*., Privacy as Contextual Integrity, Washington Law Review, Vol. June, 2004.

[38] Convention 108, Art. 5(4)(c) and GDPR, Art. 5(1)(c).

[39] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019.

[40] Convention 108+, Art. 5(4)(a); GDPR, Art. 5(1)(a).

[41] Article 5(4)(d) Convention 108 ; Article 5(1)(d) GDPR.

სამართლიანობაზე, განსაკუთრებით მაშინ, როდესაც საქმე ეხება ავტომატიზებული გადაწყვეტილების მიღებას, რაც პოტენციურად გაამძაფრებს მიკერძოებას და დისკრიმინაციას.

ანგარიშვალდებულების პრინციპი, რომელიც მოითხოვს პროაქტიულ ქცევას და პერსონალური მონაცემების დაცვის უზრუნველსაყოფად კონკრეტული ზომების დემონსტრირებას, ასევე უფრო რთული ხდება მონაცემთა გაზიარების კონტექსტში განსახორციელებლად. როდესაც დამუშავების რთულ ოპერაციებში მრავალი ორგანიზაცია მონაწილეობს, ხშირად გაურკვეველია, თუ როგორ ნაწილდება პასუხისმგებლობა მონაცემთა დამუშავებისთვის პასუხისმგებელ და უფლებამოსილ პირებს შორის.[42] აღნიშნული გაურკვევლობა ართულებს რეგულაციების აღსრულებას და ასუსტებს ანგარიშვალდებულების მარეგულირებელი ჩარჩოების ეფექტიანობას.[43]

საბოლოოდ, მონაცემთა გაზიარება მოიაზრებს მონაცემთა დაცვის ყველა პრინციპს. თუ აღნიშნული სწორად განხორციელდება და არა მხოლოდ ფორმალურად, მონაცემთა დაცვის პრინციპები დაბრკოლებას კი არ წარმოადგენს, არამედ პასუხისმგებლიანი გაზიარების ხელშემწყობ ფაქტორს. აუცილებლობისა და პროპორციულობის პრინციპი უზრუნველყოფს სამართლებრივ საფუძველს ინოვაციისა და ფუნდამენტური უფლებების შეთავსებისთვის. აღნიშნული მოითხოვს, ერთი მხრივ, მონაცემთა გაზიარების ეფექტიანობის დაბალანსებას დასახული მიზნის მისაღწევად, ხოლო, მეორე მხრივ, ჩარევას კონფიდენციალობასა და მონაცემთა დაცვაში.[44]

კონკრეტული რისკის შემცირების ზომა, როგორიცაა კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვა, მიზნის მკაცრი შეზღუდვა ან მყარი სახელშეკრულებო ჩარჩოები, ამ ბალანსის ნაწილია. საერთაშორისო და რეგიონულ მონაცემთა დაცვის სტანდარტებთან შესაბამისობის უზრუნველყოფით, მონაცემთა გაზიარებას შეუძლია ხელი შეუწყოს ინოვაციის დანერგვას და ამავდროულად დაამყაროს ნდობა, რაც აუცილებელია თანამშრომლობისთვის, ღირებულების შექმნისა და საზოგადოებრივი სარგებლისთვის. ამ თვალსაზრისით, მონაცემთა დაცვის კანონმდებლობა მოქმედებს არა როგორც დაბრკოლება, არამედ როგორც მონაცემთა გაზიარების ხელშემწყობი ფაქტორი, რომელიც გვთავაზობს პრინციპულ და პროგნოზირებად ჩარჩოს ტექნოლოგიური პროგრესის პირთა ძირითად უფლებებთან შეთავსებისთვის.

[42] *European Data Protection Board (EDPB), Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0, 7 July 2021.*

[43] Convention 108+, Art. 10; GDPR, Arts. 24–28.

[44] ეს პრინციპი ნათლად არის ასახული ადამიანის უფლებათა ევროპულ კონვენციაში, რომი, 1950 წლის 4 აპრილი, მე-8(2) მუხლი (ECHR) და სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო კონვენციის მე-17 მუხლში და შემდგომში განხორციელდა ევროკავშირის სამართალში GDPR-ის დებულებების მეშვეობით.

5. კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები, როგორც სამართლებრივი და ტექნიკური ინსტრუმენტები

კონსოლიდირებულ ტექნოლოგიებს, ე.წ. კონფიდენციალობის გამაძლიერებელ ტექნოლოგიებს ("PETs"), გააჩნია პოტენციალი, ფუნდამენტურად შეცვალოს მონაცემთა გაზიარების დინამიკა რისკების აღმოფხვრისა თუ შემცირების საშუალებით. აღნიშნული რისკები დაკავშირებულია მონაცემთა გაზიარებასთან. დღევანდელ რეალობაში უკვე შესაძლებელია ტექნოლოგიებთან მიმართებით არსებულ კითხვებზე პასუხის გაცემა.[45]

მონაცემთა გაზიარების პროცესში მხარეთა შორის თანამშრომლობის სტანდარტული ფორმა, როგორც წესი, მოიაზრებს მონაცემთა გაერთიანებას ერთ ნაკრებად, რომელიც შემდეგ ყველასთვის ხელმისაწვდომი ხდება. თუმცა თანამედროვე ტექნოლოგიები მონაცემთა გაზიარების გამარტივებულ ფორმაზე გადასვლის საშუალებას იძლევა. თანამედროვე მიდგომების მეშვეობით, წინასწარი გამოთვლის და ლოგიკური ოპერაციების განხორციელების გზით, შესაძლებელია გასაზიარებელი მონაცემების მინიმიზაცია. ამავდროულად, წინასწარი მოქმედებების განხორციელების შედეგად შესაძლებელია მონაცემთა სათანადო დაცვის უზრუნველყოფა. ამდენად, კონფიდენციალობის გამაძლიერებელი ტექნოლოგიებით მონაცემთა დაცვა შესაძლებელია როგორც ტექნოლოგიებით სარგებლობის, ასევე ტექნოლოგიების გამოყენების შემდგომ ეტაპებზე.

კონფიდენციალობის შიდა სისტემური უზრუნველყოფისთვის კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები უკვე ხელმისაწვდომია. მათში მოიაზრება: კერძო ნაკრების მოდელი,[46] ჰომომორფული დაშიფვრა,[47] მრავალმხრივი გამოთვლა დაცული საშუალებებით[48] და მტკიცებულებები ცოდნის გარეშე.[49] აღნიშნულის სანაცვლოდ, სისტემის მიღმა გამჟღავნებული მონაცემების დაცვა

[45] PETs-ის საკითხებთან დაკავშირებით იხ. *OECD-ის სახელმძღვანელო, სახელწოდებით: Emerging privacy-enhancing technologies: Current regulatory and policy approaches, OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023* <https://doi.org/10.1787/bf121be4-en> [01.10.2025] and *Asrow K. and Samonas S.,* Privacy Enhancing Technologies: Categories, Use Cases and Considerations, Federal Reserve Bank of San Francisco, CA, 2021.

[46] კერძო ნაკრების მოდელი ("PSI"): დაცული მრავალმხრივი კომპიუტერული კრიპტოტექნიკა, რომელიც ნებას რთავს ორ მხარეს, შეადარონ დაშიფრული ვერსიები აღნიშნული კერძო ნაკრების გამოყენებით. ამ პროცესში, კერძო ნაკრების გარდა, მხარეები ერთმანეთს სხვა ინფორმაციას არ უზიარებენ.

[47] ჰომომორფული დაშიფვრა ("HE"): საშუალებას იძლევა, რომ გამოთვლები განხორციელდეს უშუალოდ დაშიფრულ მონაცემებზე, რომლის შედეგად მონაცემები დაშიფრული სახით გენერირდება და მათი გაშიფვრა შესაძლებელია მოგვიანებით, ძირითადი, თავდაპირველი მონაცემების გამჟღავნების გარეშე.

[48] მრავალმხრივი გამოთვლა დაცული მეთოდებით ("SMPC") საშუალებას აძლევს სხვადასხვა მხარეს, რომ ერთობლივად გამოთვალონ მონაცემები კონფიდენციალური სახით.

[49] მტკიცებულებები ცოდნის გარეშე (ZKPs) წარმოადგენს პროტოკოლს, რომლის შესაბამისად ერთ მხარეს შეუძლია მეორე მხარეს დაუსაბუთოს, რომ კონკრეტული მტკიცება არის სწორი (მაგალითად, ისინი აკმაყოფილებს განსაზღვრულ პირობებს), სხვა დამატებითი ინფორმაციის გაზიარების გარეშე.

შესაძლებელია კონფიდენციალობის გამაძლიერებელი ორი დამატებითი ზომით: რანდომიზაცია[50] და განზოგადება[51].

კონფიდენციალობის გამაძლიერებელმა ტექნოლოგიებმა შეიძლება მნიშვნელოვნად შეამციროს იმ პირთა რაოდენობა, რომლებსაც წვდომა აქვთ პერსონალურ ინფორმაციაზე. კონკრეტულად, მხარეს, რომელიც პერსონალურ მონაცემებთან მიმართებით ახორციელებს რიცხობრივ თუ ლოგიკურ მოქმედებებს, არ შეუძლია: ღია, დაუშიფრავი სახით მონაცემების დანახვა; მონაცემთა დამუშავების პროცესში წვდომა ჰქონდეს შუალედურ მნიშვნელობებზე ან სტატისტიკურ შედეგებზე (გარდა იმ შემთხვევისა, თუ მონაცემი სპეციალურად არის განკუთვნილი გასაზიარებლად); გამოიყენოს ისეთი ტექნიკა, როგორიცაა შეტევა სხვა საშუალებებით ("side-channel attacks"), რათა დამუშავების პროცესში გამოვლენილი ცვლილებების, მაგალითად, მოთხოვნის შესრულების დროის ან ენერგომოხმარებისას, ანალიზით მოიპოვოს მონაცემები.

ქსელური კონფიდენციალობის ტექნიკა, როგორც წესი, გულისხმობს მონაცემთა ტრანსფორმაციას და გამოთვლებს დაშიფვრის მექანიზმის მეშვეობით. მაგალითად, დაცული მრავალმხრივი გამოთვლის ("SMPC") ტექნიკის გამოყენებისას მონაცემები იყოფა მრავალ კომპონენტად, რომლებიც შემდეგ ეტაპზე გამოთვლების შესასრულებლად ერთიანდება.[52]

კონფიდენციალობის დაცვის თვალსაზრისით ერთ-ერთ მაგალითად შეიძლება იქნეს მოყვანილი სავაჭრო მონაცემების დამუშავება ტრანსსასაზღვრო კონტექსტში. დაცული მრავალმხრივი გამოთვლის ტექნიკის გამოყენებით შესაძლებელი ხდება იმპორტის მონაცემების შედარება ექსპორტის მონაცემებთან. ამ გზით ორივე მხარეს შეუძლია შესაბამისობის თუ ხარვეზების გამოვლენა სავაჭრო მონაცემების გამჟღავნების გარეშე. აღნიშნული საშუალებით მხარეთა შორის ხორციელდება მნიშვნელოვანი მონაცემების მიმოცვლა განსაკუთრებული კატეგორიის მონაცემების გამჟღავნების გარეშე. სისტემური კონფიდენციალობის ტექნიკა, როგორიცაა დაცული მრავალმხრივი გამოთვლა, ფსევდონიმიზაციის საუკეთესო ფორმად შეიძლება იქნეს მიჩნეული, როდესაც ტექნოლოგიაში ასახული მონაცემები პირადი ხასიათისაა.[53]

კონფიდენციალობის სხვა ტექნიკა შეიძლება გულისხმობდეს იმგვარ სანდო გარემოს შექმნას, როდესაც გამოთვლები უსაფრთხო ტექნოლოგიურ

[50] რანდომიზაციის საშუალებით შესაძლებელია ინდივიდუალური ჩანაწერების დაფარვა, თუმცა, ამავდროულად, მონაცემთა ანალიზი.

[51] მონაცემთა განზოგადება წარმოადგენს მონაცემების შემცირების ან შეჯამების პროცესს, რომლის საშუალებითაც არსებული მონაცემები დაცულია, თუმცა ზოგადი დასკვნების გამოტანა შესაძლებელია.

[52] დაცული მრავალმხრივი გამოთვლის მიმართულებით საინტერესოა JOCONDE-ის (Joint On-demand COmputation with No Data Exchange) ინიციატივა, რომელიც ევროსტატმა 2024 წლის აპრილში წამოიწყო PET-ების ევროპულ სტატისტიკურ სისტემაში დანერგვის ხელშეწყობის მიზნით, <https://cros.ec.europa.eu/joconde> [05.09.2025].

[53] *ENISA Data Pseudonymisation: Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021.*

სისტემაში ხორციელდება. აღნიშნული ამცირებს მონაცემთა დამუშავების ოპერაციების შეცვლის რისკებს.

ტექნოლოგიებით სარგებლობის შემდგომ ეტაპზე არსებული კონფიდენციალობის ტექნიკების გამოყენებით, რომლებიც მოიცავს ხმის დამატებას ან მონაცემების კატეგორიებად დაჯგუფებას, შესაძლებელია პერსონალური მონაცემების სათანადო დაცვა. აღსანიშნავია, რომ ხმის დონის ან ინტერვალების ამპლიტუდის განსაზღვრით, მონაცემები შეიძლება დარჩეს ზუსტი. აღნიშნულის საპირისპიროდ, ხელახალი იდენტიფიკაციის მცდელობები შეიძლება იყოს არაგონივრული, მაგალითად, "GDPR"-ის პრეამბულის 26-ე პუნქტით[54] გათვალისწინებული იდენტიფიცირებადობის კრიტერიუმის შესაბამისად. სამართლებრივი თვალსაზრისით, ტექნოლოგიით სარგებლობის დასრულების შემდგომ ეტაპზე გამოყენებული კონფიდენციალობის ტექნიკა შეიძლება მიჩნეულ იქნეს ანონიმიზაციად.

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები ამცირებს რისკს, რომ ფიზიკურმა პირებმა მონაცემების დამუშავებისას შეძლონ პერსონალური ინფორმაციის მოპოვება. აღნიშნული შედეგი დგება იმის მიუხედავად, აკმაყოფილებს თუ არა განხორციელებული გამოთვლები ან ლოგიკური ოპერაციები სისტემური კონფიდენციალობის პირობებს. "PET"-ის გამოყენება, რომელიც უზრუნველყოფს შედეგების კონფიდენციალობას, სასარგებლოა როგორც ანონიმური სტატისტიკის საჯაროდ ხელმისაწვდომობისთვის, ასევე ანალიზის შედეგების გასაზიარებლად.

ასევე, კონფიდენციალობის გამაძლიერებელი ამგვარი ტექნოლოგიები მნიშვნელოვან როლს ასრულებს შენახვის ვადის შეზღუდვისა და მონაცემთა მინიმიზაციის პრინციპების დაცვის თვალსაზრისით.[55]

კონფიდენციალობის დაცვის კონტექსტში საინტერესოა სტატისტიკის ეროვნული სამსახურის მიდგომა, რომელიც მონაცემებს მათ გამოქვეყნებამდე ამატებს კალიბრირებულ ხმას. აღნიშნული ტექნიკის გამოყენება ნათლად წარმოაჩენს ანონიმიზაციის ეფექტიანობას.[56]

ტექნოლოგიების როგორც გამოყენების, ასევე გამოყენების შემდგომ ეტაპებზე დასახელებული სტანდარტების გათვალისწინება მნიშვნელოვნად უზრუნველყოფს გაზიარებული პერსონალური მონაცემების

[54] "GDPR"-ის პრეამბულის 26-ე პუნქტი: „იმისათვის, რომ განისაზღვროს, შესაძლებელია თუ არა ფიზიკური პირის იდენტიფიცირება, მხედველობაში უნდა იქნეს მიღებული ყველა გონივრული შესაძლო საშუალება, მაგალითად, ფიზიკური პირის ამოცნობა, რაც შესაძლოა გამოყენებულ იქნეს დამუშავებისთვის პასუხისმგებელი პირის ან სხვა პირის მიერ პირის პირდაპირ ან არაპირდაპირ იდენტიფიცირების მიზნით. იმის დასადგენად, მოხდება თუ არა გონივრული საშუალებების გამოყენება ფიზიკური პირების იდენტიფიცირების მიზნით, მხედველობაში უნდა იქნეს მიღებული ყველა ობიექტური გარემოება, როგორებიცაა იდენტიფიცირებისათვის საჭირო ხარჯები და დრო, მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიები და ტექნოლოგიის განვითარება.

[55] Information Commissioner's Office, Privacy-enhancing technologies (PETs), June 2023, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf> [05.09.2025].

[56] იხ., Harvard University (n.d.), Differential Privacy, Harvard University Privacy Tools Project, <https://privacytools.seas.harvard.edu/differential-privacy> [02.10.2025].

კონფიდენციალობას. დადგენილი ტექნიკების შემუშავებით ორგანიზაციებს შეუძლიათ მონაცემები სხვადასხვა სახით დაამუშაონ, რა პროცესშიც სათანადოდ იქნება დაცული პირადი ინფორმაცია. აგრეთვე, უზრუნველყოფილი იქნება მონაცემების სანდო, სამართლებრივი და ეკონომიკური პერსპექტივიდან მომგებიანი გაზიარება, მათ შორის, საერთაშორისო გადაცემის კონტექსტში, რაც სხვა შემთხვევაში შეუძლებელი იქნებოდა.

გარდა აღნიშნულისა, არსებობს კონფიდენციალობის გამაძლიერებელი სხვა ტექნოლოგიები, რომლებიც განსხვავდება განხილული ტექნოლოგიებისგან. ისინი გულისხმობს მონაცემების უსაფრთხო დამუშავებას და ამცირებს პერსონალური მონაცემების რაოდენობას, რომლებზეც წვდომა აქვთ სხვა მხარეებს. აღნიშნული უზრუნველყოფს მონაცემთა დამუშავების პრინციპების დაცვას, მაგალითად, როგორებიცაა დეცენტრალიზებული (ფედერაციული) სწავლება[57] და სინთეზური მონაცემების გამოყენება.[58]

6. რეკომენდაციები

სტატიის წინა თავებში ხაზი გაესვა მონაცემთა გაზიარებასთან დაკავშირებულ პოტენციალსა და რისკებს: როდესაც ორი ან მეტი ორგანიზაცია ერთობლივად მონაწილეობენ მონაცემთა გაზიარებაში, ისინი კოლექტიურად ქმნიან უფრო ფართო და მონაცემთა მრავალფეროვან ეკოსისტემას, რომელსაც პოტენციურად დიდი სარგებელი მოაქვს საზოგადოებისთვის. აღნიშნული წარმოშობს რისკებს კონფიდენციალობის დაცვის თვალსაზრისით. ამგვარ გარემოში გამოყენებული მიდგომების საშუალებით შეიძლება გამოიკვეთოს ახალი ტენდენციები. თუმცა ტრადიციული მიდგომების გამოყენება, როგორებიცაა ნედლი მონაცემთა ნაკრებების ორმხრივი გაცვლა ან საერთო საცავში განთავსება, რომელიც ხელმისაწვდომია ყველა მხარისთვის, არ არის მიზანშეწონილი განსაკუთრებით იმ კონტექსტში, როდესაც მონაწილეები დეცენტრალიზებულნი არიან და ხორციელდება მონაცემთა ფართომასშტაბიანი მიმოცვლა.[59]

აღნიშნულის ნაცვლად, მრავალმხრივი მიდგომა, რომელიც ეფუძნება კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვას, შეიძლება იყოს უფრო ხელსაყრელი ვარიანტი გრძელვადიან პერსპექტივაში. "PeTs"-ის გამოყენებით, დაინტერესებულ მხარეებს შეუძლიათ, შექმნან სანდო გარემო, რომელიც ორიენტირებული იქნება მონაცემთა დაცვაზე და,

[57] *Konečnỳ J., McMahan B., Ramage D..* Federated optimization: Distributed optimization beyond the datacentre, arXiv preprint arXiv:1511.03575, 2015.
[58] *El Emam K., Mosquera L., Hoptroff R.,* Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data, O'Reilly Media, 2020.
[59] *Tene O.and Polonetsky J.,* Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 2013.

ამავდროულად, უზრუნველყოფს მონაცემთა დაცვის დადგენილ პრინციპებთან შესაბამისობას.[60]

მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებზე დაკისრებული ორგანიზაციული ვალდებულებების, მონაცემთა გაზიარებისთვის დამახასიათებელი რისკებისა და კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დადებითი მხარეების გათვალისწინებით, მოცემული თავი ორიენტირებულია ტექნოლოგიების მართვის პრაქტიკულ ასპექტებზე. კერძოდ, ასახულია რეკომენდაციები, რომელთა მიზანია დაინტერესებული მხარეებისთვის სათანადო ინფორმაციის მიწოდება კონფიდენციალობის დაცვის უზრუნველსაყოფად.

6.1. რეკომენდაციები დამუშავებისთვის პასუხისმგებელი პირებისთვის

დამუშავებისთვის პასუხისმგებელმა პირებმა აუცილებელია, შეაფასონ მონაცემთა გაზიარების მიზანშეწონილობა, რომლის ფარგლებშიც უნდა დააიდენტიფიცირონ მხარეები, რომლებთანაც ხორციელდება მონაცემების გაზიარება. აღნიშნულის შესახებ სათანადოდ უნდა იყვნენ ინფორმირებულნი მონაცემთა სუბიექტები. მნიშვნელოვანია, რომ მონაცემთა სუბიექტებმა მონაცემთა დამუშავებამდე, მათ შორის, მონაცემთა შეგროვებასა და გაზიარებამდე, მარტივი და გასაგები ფორმით მიიღონ სრულყოფილი ინფორმაცია მათი პერსონალური მონაცემების დამუშავების შესახებ.[61] ამგვარი ინფორმაცია არ უნდა იყოს მიწოდებული რთული ფორმით, კერძოდ, უნდა იყოს მარტივი ენით და, ასევე, მონაცემთა სუბიექტს უნდა ჰქონდეს დამატებითი განმარტებების მიღების შესაძლებლობა. რაც მთავარია, ფიზიკურ პირებს ასევე უნდა მიეცეთ საშუალება, უარი თქვან მათი პერსონალური მონაცემების გაზიარებაზე.

პერსონალური მონაცემების გაზიარებასთან დაკავშირებული ნებისმიერი მოქმედება წარმოადგენს პერსონალური მონაცემების დამუშავებას და, შესაბამისად, წარმოშობს იურიდიულ ვალდებულებებს ორგანიზაციებისთვის. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა მიიღონ ყველა საჭირო ზომა მონაცემთა დამუშავების პროცესების კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად ყველა იურისდიქციაში, რომლებსაც გადაეცემა მონაცემები. ამისათვის აუცილებელია მონაცემთა გაზიარებისთვის სათანადო სამართლებრივი საფუძვლის განსაზღვრა.[62]

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები მნიშვნელოვან როლს ასრულებს მონაცემთა გაზიარების თანხმლები რისკების შემცირებაში,

[60] European Union Agency for Cybersecurity (ENISA), Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, December 2015. European Union Agency for Cybersecurity (ENISA), ENISA's PETs Maturity Assessment Repository, November 2018.

[61] *OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.*

[62] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller, WP 217, 9 April 2014.

მათ შორის, განსაკუთრებული კატეგორიის მონაცემების დამუშავების კუთხით. იურისდიქციის სპეციფიკის გათვალისწინებით, "PETs" შესაძლოა დამხმარე საშუალება იყოს მონაცემთა გაზიარების კონტექსტში, რაც სხვა შემთხვევაში შეუძლებელი იქნებოდა. ასევე, "PETs" წარმოადგენს ბიზნესის წარმართვის ხელშემწყობ საშუალებას, რაც ორგანიზაციებს ეხმარება, ისარგებლონ მონაცემთა დამუშავების უპირატესობებით ისე, რომ შემცირებული იყოს კონფიდენციალობასთან დაკავშირებული რისკები.[63] სწორედ აღნიშნულის გათვალისწინებით, ტექნოლოგიები უნდა დაინერგოს განსაკუთრებული სიფრთხილით.

6.2. რეკომენდაციები კანონმდებლებისა და მთავრობებისათვის

კანონმდებლებმა და მთავრობებმა უნდა შეიმუშაონ მონაცემთა გაზიარების შესახებ სამართლებრივი სისტემა, რომელიც გასცდება ორგანიზაციებს შორის მონაცემთა მარტივი გადაცემის ფარგლებს და, ამავდროულად, შეიზღუდება მონაცემთა გადამეტებული ცენტრალიზაცია.[64] ამგვარი მიდგომით, მხედველობაში უნდა იქნეს მიღებული მონაცემთა გაზიარების სოციალური და ეკონომიკური ფაქტორები, ისევე როგორც კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების პოტენციალი წარმოქმნილი რისკების შესამცირებლად.[65] "PETs"-მა, ბაზარზე შესვლის ბარიერების შემცირებითა და ახალი აქტორებისთვის ციფრული ბაზრების გახსნით შეიძლება ხელი შეუწყოს კონკურენციას.[66]

ამდენად, საკანონმდებლო ინიციატივები მიზნად უნდა ისახავდეს სამართლებრივი ჩარჩოების ჩამოყალიბებას, რომლებიც ხელს შეუწყობს "PETs"-ის დანერგვას და ორგანიზაციების წახალისებას კონფიდენციალობის დამცავი ტექნოლოგიების გამოყენების თვალსაზრისით. ამავდროულად, ინსტიტუტებმა მნიშვნელოვანი ინვესტიცია უნდა ჩადონ კვლევასა და განვითარებაში, რათა გაუმჯობესდეს "PETs"-ის გამოყენებადობა, მასშტაბურობა და ეფექტიანობა.[67] დამატებით, მთავრობებს შეუძლიათ მიზნობრივი სუბსიდიებით და სათანადო ნაბიჯების გადადგმით დააჩქარონ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვა.[68]

---

[63] *McCarthy N., Fourniol F.,* The role of technology in governance: The example of Privacy Enhancing Technologies, Data & Policy, 2020.

[64] *Organisation for Economic Co-operation and Development (OECD), Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.*

[65] *Organisation for Economic Co-operation and Development (OECD), Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.*

[66] *Organisation for Economic Co-operation and Development (OECD), Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.*

[67] *OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2021.*

[68] European Commission, Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM(2022) 68 final.

სტრატეგიულ დონეზე, სამთავრობო მონაცემთა პოლიტიკის შესაბამისად, პრიორიტეტული უნდა იყოს მონაცემთა დაცვის რეგულაციებთან შესაბამისობის უზრუნველყოფა და, ასევე, გამოთვლითი ინფრასტრუქტურის შექმნა აღსრულების სათანადო გარანტიებით. ამ თვალსაზრისით, კერძო და საჯარო სექტორების თანამშრომლობა და მარეგულირებელი "sandboxes"-ის შექმნა მნიშვნელოვან როლს ასრულებს დაინტერესებულ მხარეთა შორის ნდობის ჩამოყალიბებაში, ინოვაციების წახალისებისა და მონაცემთა დაცვის მაღალი სტანდარტების შენარჩუნებაში.[69]

გარდა აღნიშნულისა, აუცილებელია მონაცემთა გაზიარების შესახებ ჰარმონიზებული საერთაშორისო მარეგულირებელი ჩარჩოს შემუშავება. ტრანსსასაზღვრო დონეზე, შემუშავებული ჩარჩოს საშუალებით, მონაცემთა გაცვლა გახდება მეტად მარტივი და განჭვრეტადი. აგრეთვე, შეიქმნება ძლიერი და ეფექტიანი გარანტიები ინდივიდთა უფლებების დასაცავად.

6.3. რეკომენდაციები ტექნოლოგიების გამოყენების შესახებ გადაწყვეტილების მიმღებ პირთათვის

ტექნოლოგიების გამოყენების შესახებ გადაწყვეტილების მიმღებმა პირებმა, გამჭვირვალობის უზრუნველსაყოფად, ხელი უნდა შეუწყონ დანერგილი ტექნოლოგიის ფუნქციონირების შესახებ ინფორმაციის გასაჯაროებას, რომლის საშუალებითაც მონაცემთა სუბიექტები მათი პერსონალური მონაცემების დამუშავების შესახებ სრულ ინფორმაციას მიიღებენ.[70] ამასთან, საზოგადოებას უნდა ჰქონდეს მათ შესახებ ალგორითმების შემოწმების შესაძლებლობა ხელმისაწვდომობის უზრუნველყოფით. აღნიშნული ხელს შეუწყობს ნდობის გაზრდასა და სამართლიანობის დაცვას.

ამასთან, უნდა შეიქმნას მხარეთა თანამშრომლობის ფორმატი, რომლის საშუალებითაც მონაცემების გაზიარება მოხდება მკაფიოდ განსაზღვრული წესების საფუძველზე, რა პროცესშიც მონაცემთა დაცვას მიენიჭება უპირატესობა.

თავის მხრივ, უპირატესობა უნდა მიენიჭოს სტანდარტიზებულ გადაწყვეტილებებს, რათა თავიდან იქნეს აცილებული სხვადასხვა იურისდიქციით გათვალისწინებული შეუსაბამობები მონაცემთა უკანონო დამუშავების პრევენციისთვის. გარდა სამართლებრივი ვალდებულებებისა,

[69] *Truby J. et al.*, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", European Journal of Risk Regulation, 2021 <www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandboxapproach-to-regulating-highrisk-artificial-intelligenceapplications/C350EADFB379465E7F4A95B973A4977D> [05.09.2025]

[70] *United Nations, Roadmap for Digital Cooperation, 2020*, available at: <www.un.org/en/content/digital-cooperation-roadmap> [20.09.2025].

სექტორულ დონეზე უნდა შემუშავდეს ქცევის წესები მონაცემთა კონფიდენციალობის უზრუნველსაყოფად.[71]

6.4. რეკომენდაციები სამეცნიერო საზოგადოებისთვის

მკვლევრებმა და აკადემიურმა წრეებმა მიზანშეწონილია, ყურადღება გაამახვილონ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებასთან დაკავშირებულ საკითხებზე. აღნიშნული ხელს შეუწყობს "PETs"-ის პრაქტიკულ გამოყენებას და მათი პოტენციური უპირატესობების დემონსტრირებას სხვადასხვა სფეროში.[72]

გარდა აღნიშნულისა, სახელმძღვანელო რეკომენდაციების საშუალებით, დამუშავებისთვის პასუხისმგებელ პირებს უფრო მეტი ინფორმაცია უნდა მიეწოდოთ იმისათვის, რომ მაქსიმალურად შემცირდეს ტექნოლოგიების გამოყენებასთან დაკავშირებული რისკები.[73]

მკვლევრები და აკადემიური წრეების წარმომადგენლები აქტიურად უნდა ჩაერთონ ინდუსტრიის მიერ წარმოდგენილი გადაწყვეტილებების კრიტიკული შეფასების პროცესში. აღნიშნულის მიზანია მონაცემთა დაცვა დადგენილი სტანდარტების შესაბამისად.[74]

6.5. რეკომენდაციები მონაცემთა დაცვის საზედამხედველო ორგანოებისთვის

მონაცემთა დაცვის საზედამხედველო ორგანოებმა ხელი უნდა შეუწყონ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიებით სარგებლობას და უზრუნველყონ მათი გამოყენება პრაქტიკაში.

ამასთან, საზედამხედველო ორგანოებმა უნდა დაიცვან კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენების კონტექსტში ტაქსონომიისა და საზღვრების ბალანსი იმისათვის, რომ უკეთ იქნეს გააზრებული მონაცემთა გაზიარების და ამ პროცესში თანამშრომლობის მნიშვნელობები. აგრეთვე, უნდა მიიღონ ზომები ცნობიერების ამაღლების უზრუნველსაყოფად.[75]

---

[71] აგრეთვე, მისასალმებელი იქნება სახელმძღვანელო რეკომენდაციების შემუშავება, რომლებიც განკუთვნილი იქნება პროდუქტის მწარმოებლებისთვის, რა პროცესშიც ხორციელდება სენსიტიური ინფორმაციის გაზიარება, მაგალითად: *CDEI (n.d.), PETs Adoption Guide,* <https://cdeiuk.github.io/pets-adoption-guide/adoption-guide> [02.10.2025].

[72] *Wang Y. & Kobsa A.,* Privacy-Enhancing Technologies: Classification and Applications, in The Handbook of Privacy and Privacy-Enhancing Technologies, 2018.

[73] *Danezis G. et al.,* Privacy and Data Protection by Design – From Policy to Engineering, Computer Law & Security Review, Vol. 34, Issue 2, 2018.

[74] *van Blarkom J.J., van Eck B.M.A. & Verhaar P.,* Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, College bescherming persoonsgegevens, 2003.

[75] *Jurcys P., Corrales Compagnucci M., Fenwick M.,* The Future of International Data Transfers: Managing Legal Risk with a User-Held Data Model, Computer Law & Security Review, Volume 46, September 2022, 105691.

მონაცემთა დაცვის საზედამხედველო ორგანოებმა უნდა წაახალისონ ორგანიზაციები, რომ ტექნოლოგიების გამოყენებისას დანერგონ მონაცემთა დაცვის სტანდარტები, რა პროცესშიც არსებითად მნიშვნელოვანია მონაცემთა დაცვის ექპერტებსა და ტექნოლოგიების სფეროში მომუშავე პირებს შორის თანამშრომლობა. აღნიშნული საშუალებით პასუხები გაეცემა კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებასთან დაკავშირებულ კითხვებს.[76]

7. დასკვნა

მონაცემთა გაზიარებით შესაძლებელია მნიშვნელოვანი ეკონომიკური ღირებულების შექმნა საზოგადოებისთვის ინოვაციების დანერგვის ხელშეწყობით და თანამშრომლობის წახალისებით; თუმცა აღნიშნული მოიცავს რისკებს, როგორებიცაა: მონაცემებზე არასანქცირებული წვდომა; მონაცემთა დამუშავების პროცესში გამჭვირვალობის არარსებობა; მონაცემთა სუბიექტების უფლებების განხორციელების თვალსაზრისით ბარიერების შექმნა (მონაცემთა სუბიექტმა შეიძლება არ იცოდეს, ვინ აკონტროლებს მის პერსონალურ ინფორმაციას); მონაცემთა დამუშავების მიზნის ცვლილება (“Purpose creep”). თითოეული ეს გამოწვევა უნდა მოგვარდეს ეფექტიანი რეაგირებით. ნებისმიერ შემთხვევაში პერსონალური მონაცემების, განსაკუთრებით სავალდებულო მონაცემების, შეგროვება და გამოყენება უნდა შეესაბამებოდეს აუცილებლობისა და პროპორციულობის პრინციპებს. კერძო სუბიექტების მიერ მონაცემთა დამუშავების შემთხვევაში სათანადო ყურადღება უნდა მიექცეს ყველა პოტენციურ რისკს, რომლებიც უკავშირდება ძირითადი უფლებებისა და თავისუფლებების დაცვას და დაინტერესებულ პირთა ინტერესებს. აღნიშნულ პროცესში მხედველობაში უნდა იქნეს მიღებული, მათ შორის, დისკრიმინაციის არარსებობა, პროფაილინგთან დაკავშირებული რისკები და მანიპულაციის რისკები.[77]

ზემოაღნიშნული გამოწვევები მოითხოვს როგორც ტექნიკური, ასევე სამართლებრივი ზომების მიღებას იმისათვის, რომ სათანადოდ შეფასდეს და შემცირდეს კონფიდენციალობასთან დაკავშირებული რისკები. თუკი ორგანიზაციები ამ ზომებს არ მიიღებენ, ისინი არა მხოლოდ დაარღვევენ მონაცემთა დაცვის შესახებ მოქმედ კანონმდებლობასა და პრინციპებს, არამედ საზოგადოებაში მათ მიმართ გაჩნდება უნდობლობის განცდა. უნდობლობამ შეიძლება მნიშვნელოვანი გავლენა იქონიოს ეკონომიკის ეფექტიანობაზე და, საბოლოოდ, ხელი შეუშალოს მონაცემთა მიმოცვლას.

[76] *Gregory Voss W.,* “Cross-Border Data Flows, the GDPR, and Data Governance,” Washington International Law Journal, Vol. 29, No. 3, 2020.

[77] *Citron D.K. and Solove D.J.,* Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793, 2022, <https://ssrn.com/abstract=3782222> [18.09.2025].

გაზიარებული და დამუშავებული მონაცემების მოცულობის გათვალისწინებით, ორგანიზაციებმა ახალი პროდუქტის შექმნის ეტაპზევე პროაქტიულად უნდა დანერგონ მონაცემთა დაცვის სტანდარტები ("privacy by design"). თუკი ამგვარი სტანდარტები საწყის ეტაპზე არ დაინერგა, შემდგომი ზომების მიღება დამატებით ხარჯებთან შეიძლება იყოს დაკავშირებული. ასევე, წარმოიშობა უფრო მაღალი, არაპირდაპირი ხარჯები და ბუნდოვანებები მოქალაქეებისა და კომპანიებისთვის მონაცემთა გაზიარების კონტექსტში.

მონაცემთა დამუშავების ყველა პრინციპის დაცვით მონაცემთა გაზიარებამ შეიძლება დადებითი გავლენა იქონიოს არა მხოლოდ ბიზნეს სექტორზე, არამედ მთლიანად საზოგადოებაზე. აღნიშნული პრინციპები უნდა დაინერგოს ეფექტიანი, ტექნოლოგიებზე ორიენტირებული მიდგომებით, რათა მონაცემთა გაზიარებისას დაცულ იქნეს მონაცემთა დაცვის პრინციპები და მოთხოვნები. მონაცემთა გაზიარების ტრადიციული მეთოდები, კერძოდ, მონაცემთა ნაკრებების გაერთიანება შეუზღუდავი ფორმით, რომელზე წვდომაც ექნება ყველა ორგანიზაციას, ვერ უზრუნველყოფს აღნიშნული მოთხოვნების დაცულობას. თანამედროვე რეალობაში კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები მნიშვნელოვნად აუმჯობესებს მონაცემთა გაზიარების პროცესს რისკების აღმოფხვრისა თუ შემცირების გზით. ტექნოლოგიური მიღწევებით, თანამშრომლობის პროცესში, ადრე არსებული გამოწვევები აღმოფხვრილია და უკვე შესაძლებელია მონაცემთა გაზიარების ყველა ეტაპზე პერსონალური მონაცემების დაცვა.

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები შეიძლება მიჩნეულ იქნეს პარტნიორობისა და თანამშრომლობის ხელშემწყობ ფაქტორად, რადგან აწესრიგებს მონაცემთა გაზიარებასთან დაკავშირებულ საკითხებს, რაც ადრე გამოწვევას წარმოადგენდა. უპირველესად, ორგანიზაციებმა უნდა უპასუხონ შემდეგ კითხვებს: რატომ აზიარებენ მონაცემებს; ვინ არის მონაცემთა მიმღები; მონაცემთა გაზიარების შესახებ არიან თუ არა ინფორმირებულები მონაცემთა სუბიექტები; მონაცემთა სუბიექტებს შეუძლიათ თუ არა თავიანთი უფლებებით სარგებლობა. შემდგომ ეტაპზე, კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებით, ორგანიზაციებს შეუძლიათ კიდევ უფრო გააძლიერონ მონაცემთა დაცვის სტანდარტები, რომელთა საშუალებითაც მინიმუმამდე იქნება შემცირებული მონაცემთა გაზიარებასთან დაკავშირებული რისკები. საერთო ჯამში, კონფიდენციალობის გამაძლიერებელ ტექნოლოგიებს შეუძლია გადამწყვეტი როლი შეასრულოს ერთობლივი გადაწყვეტილების მიღების საფუძვლის შექმნაში, რაც საზოგადოებას სარგებელს მოუტანს და მიჩნეული იქნება „პარტნიორობის ხელშემწყობ ტექნოლოგიად".[78]

მონაცემთა გაზიარების პროცესში, ჰარმონიზებულ და საერთაშორისო დონეზე კოორდინირებულ მარეგულირებელ ჩარჩოში ზემოაღნიშნული

[78] *The Royal Society, From privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023* <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf> [24.09.2025].

ტექნოლოგიების ინტეგრაციით, შესაძლებელი იქნება ეკონომიკური და სოციალური სარგებლის მიღება და ადამიანის უფლებების დაცვა გლობალურ დონეზე.

ბიბლიოგრაფია:

1. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014).
2. *Asrow K. and Samonas S.,* Privacy Enhancing Technologies: Categories, Use Cases and Considerations, Federal Reserve Bank of San Francisco, CA, 2021.
3. Australian Data Availability and Transparency Act 2022.
4. *CDEI (n.d.), PETs Adoption Guide*, <https://cdeiuk.github.io/pets-adoption-guide/adoption-guide> [02.10.2025].
5. China, Measures for the Standard Contract for the Outbound Transfer of Personal Information, Cyberspace Administration of China, Decree No. 13.
6. China, Provisions on Facilitating and Regulating Cross-Border Data Flow (effective 22 March 2024).
7. China Regulation on Network Data Security Management (effective 1 January 2025), State Council Decree No. 790.
8. *Citron D.K., Solove D.J.,* Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793, 2022.
9. Council of Europe, Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, June 2018.
10. Councile of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28.I.1981.
11. *d'Alessandro B., O'Neil C., La Gatta T.,* Conscientious Classification: a Data Scientist's Guide to Discrimination-Aware Classification, Big Data, 2017, 5(2), 120–34.
12. *Danezis G. et al.,* Privacy and Data Protection by Design – From Policy to Engineering, Computer Law & Security Review, Vol. 34, Issue 2, 2018.
13. *El Emam K., Mosquera L., Hoptroff R.,* Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data, O'Reilly Media, 2020.
14. *ENISA, Readiness Analysis for the Adoption and Evolution of Privacy-Enhancing Technologies (PETs), 2022.*
15. *ENISA Data Pseudonymisation: Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021.*
16. *ENISA's PETs Maturity Assessment Repository, November 2018.*
17. *ENISA, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, December 2015.*

18. *European Data Protection Board (EDPB), Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0, 7 July 2021*.
19. European Commission, Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM(2022) 68 final.
20. European Commission, A European Strategy for Data, COM(2020) 66 final, 19 February 2020.
21. European Convention on Human Rights, Rome, 4.XI.1950.
22. European Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023, p. 1-71.
23. European Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44.
24. European 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.
25. *Favaretto M., De Clercq E. & Elger B.S.,* Big Data and discrimination: perils, promises and solutions. A systematic review, J Big Data 2019, 6-12.
26. *Financial Services User Group (FSUG), Assessment of current and future impact of Big Data on Financial Services, 2016.*
27. *Granville K.,* Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, the New York Times, 2018.
28. *Gregory Voss W.,* "Cross-Border Data Flows, the GDPR, and Data Governance," Washington International Law Journal, Vol. 29, No. 3, 2020.
29. Harvard University (n.d.), Differential Privacy, Harvard University Privacy Tools Project, <https://privacytools.seas.harvard.edu/differential-privacy> [02.10.2025].
30. International Covenant on Civil and Political Rights (Adopted by General Assembly resolution 2200 (XXI) of 16 December 1966).
31. *Isaak J. and Hanna M.*, User data privacy: Facebook, Cambridge Analytica, and Privacy Protection, Computer, Vol. 51/8, pp. 56-59, 2018.
32. *Jurcys P., Corrales Compagnucci M., Fenwick M.,* The Future of International Data Transfers: Managing Legal Risk with a User-Held Data Model, Computer Law & Security Review, Volume 46, September 2022, 105691.
33. *Konečnỳ J., McMahan B., Ramage D.*. Federated optimization: Distributed optimization beyond the datacentre, arXiv preprint arXiv:1511.03575, 2015.
34. *Kroll J.A., Huey J., Barocas S., Felten EW., Reidenberg JR., Robinson DG., Yu HL*., Accountable algorithms, Univ Pa Law Rev. 2017, 165(3), 633–705.
35. *McCarthy N., Fourniol F.,* The role of technology in governance: The example of Privacy Enhancing Technologies, Data & Policy, 2020.

36. *OECD, "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023.*
37. *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013 Revision. OECD, Explanatory memoranda of the OECD Privacy Guidelines, 2022, PP 11-12.*
38. *OECD*, *Recommendation of the Council on, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, OECD/LEGAL/0463, 2021.*
39. *OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019*.
40. *OECD, Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration), OECD, Paris, 2016*
41. *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013.*
42. *OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD, Paris, 2008.*
43. *Nissenbaum H*., Privacy as Contextual Integrity, Washington Law Review, Vol. June, 2004.
44. *Royal Society, From privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023.*
45. *Schermer BW.*, The Limits of Privacy in Automated Profiling and Data Mining, Comput Law Secur Rev. 2011, 27(1), 45–52.
46. SDAIA, Data Sharing Policy, 2024
47. *Tene O.and Polonetsky J.,* Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 2013.
48. *Truby J. et al.*, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", European Journal of Risk Regulation, 2021.
49. UK, Data Sharing Governance Framework, 2022.
50. UK Information Commissioner's Office, Privacy-enhancing technologies (PETs), June 2023.
51. UN General Assembly Resolutions on the right to privacy in the digital age, e.g., A/RES/68/167 (2013).
52. *United Nations guide on Privacy-Enhancing Technologies for official statistics. United nations Big Data 2023.*
53. *United Nations, Roadmap for Digital Cooperation, 2020.*
54. US National Strategy lists technologies suitable for Privacy Preserving Data Sharing and Analytics.
55. *van Blarkom J.J., van Eck B.M.A. & Verhaar P.,* Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, College bescherming persoonsgegevens, 2003.

56. *Wang Y. & Kobsa A.,* Privacy-Enhancing Technologies: Classification and Applications, in The Handbook of Privacy and Privacy-Enhancing Technologies, 2018.
57. *World Economic Forum*, *Good Data: Sharing Data and Fostering Public Trust and Willingness*, p. 6, 2021.

დევიდ ვაინკაუფი*

სამუშაო დოკუმენტი დიდი ენობრივი მოდელების (“LLMs”) შესახებ**

დიდი ენობრივი მოდელები (“LLMs”) წარმოადგენს განსაკუთრებით მასშტაბურ და კომპლექსურ მანქანური სწავლების სისტემებს, რომლებსაც შეუძლია მომხმარებლის შეკითხვებზე პასუხად შექმნან მკაფიო და დამაჯერებლად ჟღერადი — თუმცა არა აუცილებლად ჭეშმარიტი — ტექსტი. წინამდებარე ნაშრომი გთავაზობთ “LLM”-ების სიღრმისეულ და კომპლექსურ ანალიზს, რომლის მიზანია მონაცემთა დაცვის საზედამხედველო ორგანოებს დაეხმაროს ამ ახალი ტექნოლოგიით გამოწვეული სირთულეების რეგულირებასა და მათზე ეფექტიან რეაგირებაში. ნაშრომში “LLM” გაანალიზდა სამი პერსპექტივიდან: (1) ტექნოლოგიური პერსპექტივა — ის, თუ როგორ ფუნქციონირებს და როგორ ვითარდება “LLM”; (2) “LLM”-ის განვითარებასთან დაკავშირებული რისკები მონაცემთა დაცვის სფეროში; და (3) აღნიშნული რისკების შესამცირებლად ან აღმოსაფხვრელად ჩამოყალიბებული საუკეთესო პრაქტიკის მაგალითები.

***საკვანძო სიტყვები**: დიდი ენობრივი მოდელები, ხელოვნური ინტელექტი, ტექნიკური ანალიზი, პირადი ცხოვრების ხელშეუხებლობა, პერსონალურ მონაცემთა დაცვა, რისკები, საუკეთესო პრაქტიკა, შემამსუბუქებელი ღონისძიებები.*

---

* დოქტორი, ტექნოლოგიური პოლიტიკის უფროსი მრჩეველი, კანადის კონფიდენციალობის კომისრის ოფისი.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. თბილისში გამართულ „ტექნოლოგიის მიმართულებით მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის“, რიგით 75-ე შეხვედრაზე წარდგენილი მოხსენების ტექსტს. თავდაპირველი ვერსია გამოქვეყნდა 2024 წლის 27 დეკემბერს და ხელმისაწვდომია შემდეგ ბმულზე:
<https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.pdf?__blob=publicationFile&v=2> [25.11.2025].

1. შესავალი

დიდი ენობრივი მოდელები (“LLM”) წარმოადგენს მათემატიკურ მოდელებს, რომლებიც შემუშავებულია ხელოვნური ინტელექტისა (“AI”) და მანქანური სწავლების (“ML”) ტექნიკების გამოყენებით, ბუნებრივ ენასთან დაკავშირებული ამოცანების შესასრულებლად. ბოლო წლებში ამ სფეროში მიღწეული ტექნოლოგიური პროგრესი არსებითად დაჩქარდა, რის შედეგადაც ზოგიერთმა “LLM”-მა გარკვეული ამოცანების ფარგლებში ადამიანური და მეტიც — ექსპერტული დონის შესაძლებლობებიც კი გამოავლინა. სფეროში მიღწული პროგრესი უმთავრესად განპირობებულია მოდელების არქიტექტურისა და ტრენინგის ტექნიკების გაუმჯობესებით; აგრეთვე მოდელების ზომის, სასწავლო მონაცემთა კორპუსების მოცულობისა და გამოთვლითი რესურსების ხელმისაწვდომობის სწრაფი ზრდით.

მიუხედავად მათი შესაძლებლობებისა, დიდი ენობრივი მოდელები არ წარმოადგენს ტექნოლოგიურ პანაცეას. “LLM”-ის ხელოვნურ ინტელექტზე დაფუძნებული მიდგომა, რომელიც ენობრივი ამოცანების ავტომატიზაციას ემსახურება, წარმოშობს რიგ რისკებს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის მიმართულებით. ზოგიერთი რისკი უკავშირდება საბაზისო ტექნოლოგიის დიზაინს, ზოგი კი — პერსონალური მონაცემების დამუშავების პრაქტიკას. ამასთანავე, მნიშვნელოვანი რისკები უკავშირდება ენის აღქმისა და ენობრივი ამოცანების შესრულების ხელოვნურ ინტელექტზე დაფუძნებული მათემატიკური მიდგომების სტრუქტურულ შეზღუდვებს.

წინამდებარე ნაშრომის მიზანია დიდი ენობრივი მოდელების სიღრმისეული ანალიზი პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის პერსპექტივიდან. ვინაიდან “LLM”-ები წარმოადგენს კომპლექსურ ტექნოლოგიებს, რომლებიც პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის კუთხით მრავალფეროვან რისკებს წარმოშობს, მათი ანალიზიც მოითხოვს მრავალმხრივ შეფასებას. ამდენად, აუცილებელია “LLM”-ების გაანალიზება არა მხოლოდ ტექნოლოგიურ ჭრილში, ე.ი. იმის მიხედვით, თუ როგორ ფუნქციონირებენ ისინი ტექნიკურად, არამედ პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის რისკების, ისევე როგორც იმ საუკეთესო პრაქტიკების გათვალისწინებით, რომლებიც მიზნად ისახავს აღნიშნული რისკების შემცირებას ან აღმოფხვრას. მხოლოდ აღნიშნული სამი პერსპექტივის — ტექნოლოგიის, მონაცემთა დაცვის რისკებისა და საუკეთესო პრაქტიკის — ერთობლივი გააზრებით შეუძლიათ მონაცემთა დაცვის საზედამხედველო ორგანოებს ამ ახალი გამოწვევის ეფექტიანი რეგულირება და მათზე ადეკვატური რეაგირება.

ნაშრომი შედგება სამი ნაწილისგან. პირველ ნაწილში წარმოდგენილია დიდი ენობრივი მოდელების ტექნიკური ანალიზი, შესაბამისი აქცენტით “LLM”-ების განვითარების თითოეულ ეტაპზე გამოყენებული სხვადასხვა კომპონენტის როლზე. მეორე ნაწილში განხილულია დიდი ენობრივი

მოდელების მიერ წარმოშობილი სხვადასხვა რისკი მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კუთხით. მესამე ნაწილში კი განხილულია საუკეთესო პრაქტიკა, რომელიც მიზნად ისახავს "LLM"-ებთან დაკავშირებული გარკვეული რისკების პრევენციას ან შემსუბუქებას, აქცენტით იმ ძირითად საკითხებზე, რომლებიც საჭიროებს გააზრებას როგორც ტექნოლოგიების თავდაპირველი შემუშავების, ისე მათი გამოყენების დროს.

დათქმა

წინამდებარე ნაშრომში არ არის მოცემული სამართლებრივი რჩევები. ამასთან, ნაშრომში გამოთქმული შეხედულებები აუცილებლად არ ასახავს „ტექნოლოგიების სფეროში მონაცემთა დაცვის საერთაშორისო სამუშაო ჯგუფის" ("IWGDPT") ცალკეული წევრების ოფიციალურ პოლიტიკას ან პოზიციას.

2. რა არის დიდი ენობრივი მოდელები ("LLMs")?

დიდი ენობრივი მოდელები წარმოადგენს განსაკუთრებით მასშტაბურ და კომპლექსურ მანქანური სწავლების სისტემებს, რომლებსაც შეუძლიათ მომხმარებლის შეკითხვებზე პასუხად შექმნან მკაფიო და დამაჯერებლად ჟღერადი — თუმცა არა აუცილებლად ჭეშმარიტი — ტექსტი. "LLM"-ები შედგება ასობით მილიარდი, ხოლო ზოგ შემთხვევაში — ტრილიონობით პარამეტრისგან, რომელიც განაწილებულია სხვადასხვა სტრუქტურულ კომპონენტზე. თითოეული ასეთი კომპონენტი ასრულებს კონკრეტულ ფუნქციას და სისტემას ახალ შესაძლებლობებს მატებს. აღნიშნული კომპონენტების მაგალითებია ლექსიკონი, სიტყვების რიცხვით ვექტორებად გარდაქმნა ("embeddings"), მოდელის შინაარსი, ანუ ე.წ. კონტექსტის ფანჯარა, მრავალთავიანი თვითყურადღების მექანიზმი და წინ მიმართული ნერვული ქსელები.

ეს კომპონენტები ერთობლივად ქმნის ე.წ. „ტრანსფორმერის" აგებულებას (არქიტექტურას). ხელოვნური ინტელექტის ("AI") მოდელებს, მათ შორის დიდ ენობრივ მოდელებს, რომელთა სტრუქტურა ეფუძნება აღნიშნულ აგებულებას, ჩვეულებრივ „ტრანსფორმერულ" მოდელებად მოიხსენიებენ. „ტრანსფორმერის" მოდელის დეტალური ტექნიკური ანალიზი გთხოვთ იხილოთ წინამდებარე სტატიის ორიგინალ ვერსიაში.[1]

დიდი ენობრივი მოდელების გაწვრთნის (ტრენინგის) ციკლი მნიშვნელოვნად განსხვავდება მანქანური სწავლების სხვა პროგრამების

[1] იხ.: *IWGDPT*, *სამუშაო დოკუმენტი დიდი ენობრივი მოდელების შესახებ (LLMs),* დეკემბერი 27, 2024, <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.pdf?__blob=publicationFile&v=2> [25.11.2025].

გაწვრთნის პროცესისგან. კერძოდ, ერთსაფეხურიანი გაწვრთნის მოდელის ნაცვლად, "LLM"-ების შემთხვევაში, როგორც წესი, იყენებენ ორ ეტაპიან პროცესს, რომელიც სწავლის რამდენიმე სხვადასხვა მეთოდს აერთიანებს. გაწვრთნის პირველ ეტაპს ეწოდება „წინასწარი წვრთნა" ("pre-training"), ხოლო მეორეს — „დაზუსტება / შესაბამისობაში მოყვანა" ("fine-tuning / alignment").

ნაშრომის შემდგომ ნაწილებში განხილულია დიდი ენობრივი მოდელების განვითარების და გაწვრთნის პროცედურა თითოეული ეტაპის ცალკეული ანალიზის გზით, მათ შორის გამოყენებული სასწავლო მეთოდების აღწერით და სისტემის საერთო ფუნქციონირებაში თითოეული ფაზის წვლილის წარმოჩენით.

მნიშვნელოვანია აღინიშნოს, რომ ნაშრომში განხილული ეტაპები სრულად არ ფარავს "LLM"-ების განვითარების ყველა ფაზას. მაგალითად, ბევრი "LLM" გამოყენებამდე გადის ე.წ. "red-teaming"-ის ეტაპს, რომლის ფარგლებშიც უსაფრთხოების სპეციალისტებისა და სხვა დარგობრივი ექსპერტებისგან შემდგარი ჯგუფი ცდილობს, გამოავლინოს სისტემის სუსტი მხარეები და მისი ბოროტად გამოყენების შესაძლო სცენარები. მიუხედავად ამისა, "LLM"-ების განვითარების ციკლის აღნიშნული ეტაპები იძლევა საშუალებას, განვიხილოთ მათი მრავალი უნიკალური მახასიათებელი, რაც ხელს უწყობს სისტემის საერთო ფუნქციონირების უკეთ გააზრებას.

2.1. 1-ელი ეტაპი: წინასწარი წვრთნა

დიდი ენობრივი მოდელების გაწვრთნის პირველი ეტაპის მიზანია, შეიქმნას ზოგადი დანიშნულების მოდელი, რომელსაც ექნება პირველადი, ჯერ კიდევ დაუმუშავებელი უნარი — კონკრეტული თემის ფარგლებში ტექსტის მიმდევრობაში უწყვეტად იწინასწარმეტყველოს მომდევნო სიტყვა ან სიტყვითი ერთეული ("token"). ამ მიზნის მისაღწევად მოდელი იწვრთნება განსაკუთრებით დიდი მოცულობის ბუნებრივი ენის მონაცემების გამოყენებით, რომლებიც, როგორც წესი, მოიცავს ინტერნეტში ხელმისაწვდომი ვებგვერდებიდან შეგროვებულ ტექსტებს და/ან ელექტრონულ წიგნებს.

წინასწარი წვრთნა ეფუძნება ე.წ. თვითსწავლებაზე ("self-supervised learning") დაფუძნებულ მიდგომას. ეს მეთოდი ჰგავს ზედამხედველობითი სწავლების მეთოდს ("supervised learning"), თუმცა იმ მნიშვნელოვანი განსხვავებით, რომ სწორი პროგნოზის დასადგენად საჭირო „მითითებები" არ ეფუძნება ცალკე, ადამიანის მიერ მომზადებულ „ეტიკეტირებულ" მონაცემებს. ამის ნაცვლად, სწორი პროგნოზისათვის საჭირო ინფორმაცია — ე.წ. "ground truth" — უშუალოდ სასწავლო მონაცემებშია უკვე მოცემული. რადგან ბუნებრივი ენა თავისთავად შეიცავს იმის მაგალითებს, თუ რომელი სიტყვა მოჰყვება წინამორბედს, მოდელს შეუძლია ისწავლოს მომდევნო სიტყვის წინასწარმეტყველება დამატებითი, ადამიანის მიერ შექმნილი ეტიკეტების გარეშე.

წინასწარი წვრთნა მოიცავს ნაბიჯების თანმიმდევრობას, რომლებიც განმეორებით სრულდება იმდენ ხანს, რამდენიც გათვალისწინებულია სასწავლო პროცესისთვის. სასწავლო ალგორითმი ასრულებს შემდეგ მოქმედებებს:

1. სასწავლო მონაცემებიდან არჩევს ტექსტის ერთ მონაკვეთს;
2. არჩეული ტექსტი (ბოლო სიტყვის გარეშე) შეჰყავს მოდელში, რათა მიიღოს მომდევნო, ე.ი. იმ ბოლო სიტყვის პროგნოზი, რომელიც არ შეიყვანა;
3. გამოთვლის პროგნოზის შეცდომას პროგნოზირებული შედეგისა და რეალურად არსებული ბოლო სიტყვის შედარების საფუძველზე; და
4. შეცდომის შემცირების მიზნით ასწორებს მოდელში არსებული თითოეული პარამეტრის მნიშვნელობას ე.წ. „უკუდიფერენცირების“ (“backpropagation”) მეთოდის გამოყენებით.

წინასწარი წვრთნის დასრულების შედეგად მიღებული მოდელის აღსაწერად გამოიყენება ტერმინი „ფუძემდებლური მოდელი“ (“foundation model”).[2] თუმცა აღნიშნული ტერმინი გარკვეულწილად საკამათოა. ტერმინის შემქმნელებმა განმარტეს, რომ იგი შეირჩა იმ მიზნით, რომ „ასახოს ამ მოდელების დაუსრულებელი, თუმცა მნიშვნელოვანი ნაწილი, ვინაიდან ისინი „წარმოადგენს საერთო საძირკველს, რომლის საფუძველზეც ადაპტაციის გზით შეიქმნება მრავალი განსხვავებული, ამოცანაზე ორიენტირებული მოდელი“.[3] ამ ხედვის საპირისპიროდ, კრიტიკოსები მიიჩნევენ, რომ აღნიშნული ტერმინი არაზუსტად ასახავს ამ მოდელების კავშირს ბუნებრივ ენასთან. ხელოვნური ინტელექტის ერთ-ერთმა მკვლევარმა აღნიშნულთან დაკავშირებით განაცხადა: „ეს მოდელები სინამდვილეში ჰაერში აშენებული სასახლეებია — მათ არავითარი საფუძველი არ აქვთ.“[4]

აკადემიური კვლევის მიღმა შესაძლებელია წინასწარი წვრთნის შედეგის უფრო პრაქტიკული და უბრალო ენით აღწერაც. ერთ-ერთი პრაქტიკოსის შეფასებით, წინასწარი წვრთნის შედეგად მიღებული მოდელი ფუნქციონირებს როგორც სისტემა, რომელიც ინტერნეტში არსებულ ტექსტურ მასალებზე დაყრდნობით ახდენს ტექსტის ავტომატურ გენერირებას, სიღრმისეული ანალიზის გარეშე.[5]

---

[2] იხ.: *Bommasani R., Hudson D., Adeli E. et al.*, On the Opportunities and Risks of Foundation Models, August 2021, <https://doi.org/10.48550/arXiv.2108.07258> [25.11.2025].

[3] იქვე, გვ. 3 (n. 2) და გვ. 7.

[4] იხ. ავტორის ციტატა: *Malik J.* in: *Knight W.*, A Stanford Proposal Over AI's 'Foundations' Ignites Debate, *Wired*, September 2021, <https://www.wired.com/story/stanford-proposal-ai-foundations-ignites-debate/> [25.11.2025]. აღნიშნული მოსაზრების ვიდეოჩანაწერი ხელმისაწვდომია შემდეგ ბმულზე: <https://www.reddit.com/r/MachineLearning/comments/pd4jle/d_jitendra_maliks_take_on_foundation_models_at/> [25.11.2025].

[5] იხ.: *Karpathy A.*, Let’s build GPT: from scratch, in code, spelled out, January 2023, <https://www.youtube.com/watch?v=kCc8FmEb1nY> [25.11.2025], at 1:51:45.

2.2. მე-2 ეტაპი: შესაბამისობაში მოყვანა

ზოგადი დანიშნულების „ფუძემდებლური მოდელის" შექმნის შემდეგ წვრთნის მომდევნო ეტაპი უკავშირდება მოდელის ქცევის დახვეწას, რათა მისი პასუხები უკეთ შეესაბამებოდეს ადამიანის ღირებულებებს. სასურველი ქცევა, როგორც წესი, გამოიხატება სამი ძირითადი კომპონენტით, რომლებიც ცნობილია „სამი H"-ის სახელწოდებით: "LLM"-მა უნდა იმოქმედოს ისე, რომ მისი პასუხები იყოს სასარგებლო ("helpful"), გულწრფელი ("honest") და უსაფრთხო ("harmless").[6]

აღნიშნული ამოცანა მნიშვნელოვან გამოწვევებს უკავშირდება. წინასწარი წვრთნის შემდეგ მოდელს შეუძლია მხოლოდ ტექსტის მიმდევრობაში მომდევნო სიტყვის პროგნოზირება. მიუხედავად იმისა, რომ ეს უნარი გარკვეულწილად უკავშირდება წვრთნის მეორე ეტაპზე ფორმირებულ შესაძლებლობებს, იგი არსებითად განსხვავდება მათგან. კერძოდ, მომდევნო სიტყვის პროგნოზირება არ უტოლდება ადამიანის მიერ გაცემული მითითებების შესრულებას, ცრუ ინფორმაციის თავიდან აცილებას ან მომხმარებლისთვის ტოქსიკური და მავნე შინაარსის მიწოდებისგან შეზღუდვის უნარებს, რომლებიც "LLM"-მა უნდა განივითაროს წვრთნის მეორე ეტაპზე. მაგალითად, როდესაც მომხმარებლის მიერ გაცემულ მითითებას დავალების სახით ვთავაზობთ "OpenAI"-ის მესამე თაობის გენერაციულ მოდელს — "GPT-3"-ს, რომელსაც გავლილი აქვს მხოლოდ წვრთნის პირველი ეტაპი (წინასწარი წვრთნა), იგი, როგორც წესი, უბრალოდ აგრძელებს მსგავსი მითითებების ჩამონათვალს. იმავე მოდელის "fine-tuned" ვერსია — "InstructGPT" — ანუ მოდელი, რომელსაც გავლილი აქვს წვრთნის მეორე ეტაპი და რომელიც წარმოადგენს "OpenAI"-ის პოპულარული "ChatGPT"-ის წინამორბედს, იმავე დავალების პასუხად უკვე იძლევა პირდაპირ და შინაარსობრივად გამართულ პასუხს.

საილუსტრაციოდ იხილეთ ცხრილი 1.

მითითება:	**გთხოვთ, აუხსენით მთვარეზე დაჯდომის (პილოტირებული მისია მთვარისაკენ) ფაქტი 6 წლის ბავშვს რამდენიმე წინადადებით.**
პასუხები:	"GPT-3"-ის პასუხი: „აუხსენით მიზიდულობის თეორია 6 წლის ბავშვს.

[6] იხ.: *Askell A., Bai Y., Chen A. et al.*, A General Language Assistant as a Laboratory for Alignment, 2021, <https://doi.org/10.48550/arXiv.2112.00861> [25.11.2025].

	აუხსენით თანაფარდობის თეორია 6 წლის ბავშვს რამდენიმე წინადადებით. აუხსენით დიდი აფეთქების თეორია 6 წლის ბავშვს. აუხსენით ევოლუცია 6 წლის ბავშვს.“
	“InstructGPT”-ის პასუხი: „ადამიანები გაფრინდნენ მთვარეზე, გადაიღეს ფოტოები იმისა, რაც იქ ნახეს, და ეს ფოტოები დედამიწაზე გამოგზავნეს, რათა ჩვენ ყველას შეგვეძლოს მათი ნახვა.“

ცხრილი 1: *ერთი და იმავე მითითებაზე “GPT-3”-ისა და “InstructGPT”-ის მიერ გაცემული განსხვავებული პასუხების მაგალითი. წყარო: OpenAI, Aligning language models to follow instructions, <https://openai.com/research/instruction-following> [25.11.2025].*

ზოგადად, “fine-tuning”-ის ეტაპზე წვრთნის პროცესი იყოფა ორ საფეხურად (ქვეეტაპად). პირველი ეფუძნება ზედამხედველობით სწავლას (“supervised learning”), ხოლო მეორე — განმტკიცებაზე / წახალისებაზე დაფუძნებულ სწავლებას (“reinforcement learning”).

2.2.1. ზედამხედველობითი სწავლება

დიდი ენობრივი მოდელების გაწვრთნის ქვემოთ განხილული ეტაპი გარკვეულწილად ჰგავს წინასწარი წვრთნის ეტაპს, თუმცა იმ არსებითი განსხვავებით, რომ ის მაგალითები, რომელთა საფუძველზეც მოდელი იწვრთნება, ადამიანის მიერ წინასწარ არის შერჩეული და დამუშავებული. აღნიშნული მაგალითები მოიცავს როგორც იმ ტიპის მითითებებს — ანუ დავალებებს — რომელთა მიღებაც “LLM”-ს ევალება, ისე იმ პასუხებს, რომლებიც მან ასეთ შემთხვევებში უნდა გადასცეს მომხმარებელს. სწორედ ამიტომ ეწოდება აღნიშნულ ეტაპს „ზედამხედველობითი“ სწავლება. სასწავლო მასალა მოიცავს “LLM”-სა და მომხმარებელს შორის ამოცანაზე ორიენტირებული ურთიერთქმედების სრულ მაგალითებს, მათ შორის როგორც მომხმარებლის მიერ გაცემულ მითითებას, ისე შესაბამის, „სწორ“ პასუხს, რომელიც მოდელმა უნდა გასცეს.

როგორც წესი, ამ ეტაპზე გამოყენებული სასწავლო მონაცემების მოცულობა მნიშვნელოვნად ნაკლებია იმ მონაცემებთან შედარებით, რომლებიც გამოიყენება წინასწარი წვრთნის ეტაპზე. ეს განპირობებულია როგორც პრაქტიკული, ისე სამეცნიერო მიზეზებით. პრაქტიკული კუთხით, ზედამხედველობითი სწავლებისთვის სპეციალურად მორგებული სასწავლო მონაცემთა ბაზების შექმნა მნიშვნელოვნად მეტ დროსა და რესურსს

მოითხოვს, ვიდრე თვითსწავლებაზე დაფუძნებული სწავლებისთვის ინტერნეტში ხელმისაწვდომი ტექსტების ან ელექტრონული წიგნების მასობრივი გამოყენება, განსაკუთრებით თანამედროვე ციფრული მასალის დიდი მოცულობის გათვალისწინებით. ამასთან, მანქანური სწავლების თვალსაზრისით, ამ ეტაპზე ნაკლები, თუმცა მაღალი ხარისხის მონაცემები რეალურად უფრო ეფექტიანია. კვლევებმა აჩვენა, რომ ზედამხედველობითი სწავლების ეტაპი ხასიათდება ე.წ. „ნიმუშების ეფექტიანობით" ("sample efficiency"), რაც ნიშნავს, რომ მოდელის წარმატებით გასაწვრთნელად კონკრეტულ ამოცანაზე — კერძოდ, მომხმარებლის მითითებების რეგულარულ რეჟიმში შესრულებისთვის — საჭირო მონაცემთა მოცულობა შედარებით მცირეა.[7] ამგვარად, პირველადად გაწვრთნილ მოდელზე დაყრდნობით, ზედამხედველობითი სწავლება შესაძლებელს ხდის "LLM"-ის პარამეტრების მიზნობრივად გასწორებასა და გაუმჯობესებას, რის შედეგადაც მოდელის თავდაპირველი, დაუმუშავებელი ენობრივი შესაძლებლობები გარდაიქმნება უფრო პირდაპირ და მიზანმიმართულ ქცევად. როგორც წესი, აღნიშნული ეტაპის დასრულების შემდეგ "LLM" უფრო ეფექტიანად მუშაობს.

2.2.2. წახალისებაზე დაფუძნებული სწავლება

ხელოვნური ინტელექტის მიერ მომხმარებლის მიერ გაცემული დავალების უშუალოდ შესრულება თავისთავად არ ნიშნავს, რომ იგი შესრულდება პასუხისმგებლიანად ან ეთიკურად. მართალია, ზედამხედველობითი სწავლება — ანუ წვრთნის მეორე ეტაპი — საშუალებას აძლევს "LLM"-ს მომხმარებელს გასცეს უფრო ეფექტიანი პასუხები, მაგრამ, როგორც წესი, ამ ეტაპზე მოდელს ჯერ კიდევ არ აქვს ფორმირებული ისეთი „ღირებულებები", როგორებიცაა გულწრფელობა და უვნებლობა (ზიანის არმიყენება). ამ დამატებით ღირებულებებთან უკეთ შესაბამისობის მისაღწევად "LLM"-ები გადიან წვრთნის შემდგომ ეტაპს, რომელიც ეფუძნება ე.წ. წახალისებაზე დაფუძნებულ სწავლებას ("reinforcement learning").

წახალისებაზე დაფუძნებული სწავლება წარმოადგენს მანქანური სწავლების ისეთ ფორმას, რომლის ფარგლებშიც მოდელი იწვრთნება დინამიკურ გარემოში მიღებულ უკუკავშირზე დაყრდნობით, რაც გარკვეულწილად „ცდისა და შეცდომის" ("trial and error") პროცესს ჰგავს. ზედამხედველობითი ან თვითსწავლებაზე დაფუძნებული მეთოდებისგან განსხვავებით, ამ შემთხვევაში ხელოვნური ინტელექტის მოდელის გაწვრთნა არ ხდება ე.წ. „სწორი ქცევის" მაგალითების განმეორებითი ჩვენების გზით. აღნიშნულის ნაცვლად, სწავლების პროცესში ცენტრალურ როლს ასრულებს წახალისებისა და დასჯის მექანიზმი. კერძოდ, მოდელი ჯილდოვდება იმ ქცევისათვის, რომელიც მას განსაზღვრული მიზნის მიღწევაში ან მისკენ დაახლოებაში ეხმარება, ხოლო ისჯება იმ ქმედებებისათვის, რომლებსაც საპირისპირო შედეგამდე მიჰყავს. სხვადასხვა სტრატეგიის გამოცდისა და

[7] იხ.: *Khandelwal U., Clark K., Jurafsky D. et al.*, Sample Efficient Text-Summarization Using a Single Pre-Trained Transformer, 2019, <https://doi.org/10.48550/arXiv.1905.08836> [25.11.2025].

მიღებული დადებითი ან უარყოფითი უკუკავშირის საფუძველზე, საკუთარი პარამეტრების განახლების გზით, მოდელი ეტაპობრივად აყალიბებს ოპტიმალურ „ქცევით პოლიტიკას“, რომელიც შესაბამის გარემოში მაქსიმალურ წახალისებას უზრუნველყოფს. ამდენად, წახალისებაზე დაფუძნებული სწავლება სხვა ტიპის მანქანურ სწავლებასთან შედარებით უფრო ღია და კვლევითი ხასიათისაა. სწორედ ამისთვის გამოიყენება იგი ხშირად სტრატეგიაზე დაფუძნებული ამოცანებისთვის, როგორებიცაა თამაშები, მაგალითად, “Go”[8] ან “StarCraft”.[9]

“LLM”-ების შემთხვევაში ის „თამაში“, რომლის შესრულებაზეც მოდელი იწვრთნება, გულისხმობს მომხმარებლის მითითებებზე ეთიკურ და სათანადო რეაგირებას. ერთი შეხედვით შეიძლება ჩანდეს, რომ ეს ამოცანა სტრატეგიული თამაშების — როგორიცაა “Go” ან “StarCraft” — სწავლების პროცესის ანალოგიურია; თუმცა უფრო სიღრმისეული ანალიზი ცხადყოფს, რომ ეთიკური გადაწყვეტილებების მიღება არსებითად განსხვავებული ხასიათისაა. სწორედ ეს განსხვავებები აჩენს რიგ სერიოზულ გამოწვევებს “LLM”-ების კონტექსტში წახალისებაზე დაფუძნებული სწავლების გამოყენებისას.

მთავარი სირთულე მდგომარეობს იმაში, რომ სტრატეგიული თამაშებისგან განსხვავებით, რომლებშიც მკაფიოდ არის განსაზღვრული, თუ რას წარმოადგენს „გამარჯვება“ — ე.ი. „თამაშის მოგება“ (მაგალითად, მაღალი ქულის მიღება ან მოწინააღმდეგის დამარცხება) — ეთიკაში არ არსებობს ზუსტი და ერთმნიშვნელოვანი განმარტება იმისა, თუ რა იქნება „გამარჯვება/მოგება“. ეთიკური ქმედება არ ხორციელდება წინასწარ განსაზღვრული საბოლოო მიზნის ან შედეგის მისაღწევად. მას არ აქვს რაიმე გარე მიზანი, რომლისკენაც მიმართულია ქცევა. პირიქით, ეთიკური მოქმედება ღირებულია თავად საკუთარი თავისთვის — უბრალოდ იმიტომ, რომ „სწორად მოქმედება სწორია“. როგორც არისტოტელე განმარტავს ამ განსხვავებას, „წარმოების [მაგ., სტრატეგიული თამაშის] მიზანი განსხვავებულია თავად ამ მოქმედებისგან, ხოლო ქმედების [ეთიკური მოქმედების] მიზანი ვერ იქნება სხვა, რადგან სწორედ ეთიკური მოქმედება თავად არის მიზანი.“[10]

ამ თავისებურებიდან გამომდინარე, ეთიკური მოქმედების კრიტერიუმები თავისთავად ბუნდოვანი და არაზუსტია. ისინი არ ექვემდებარება იმგვარ სიზუსტეს, რომელიც დამახასიათებელია მათემატიკისთვის ან საბუნებისმეტყველო მეცნიერებებისთვის. ეს ქმნის სერიოზულ პრობლემას წახალისებაზე დაფუძნებული სწავლებისთვის, ვინაიდან ზუსტად განსაზღვრული მიზნის არარსებობის პირობებში რთულია დადგინდეს, უნდა

[8] იხ.: *Silver D., Huang A., Maddison C. et al.*, Mastering the game of Go with deep neural networks and tree search, *Nature*, Vol. 529, 2016, 484–489, <https://doi.org/10.1038/nature16961> [25.11.2025].

[9] იხ.: *Vinyals O., Babuschkin I., Czarnecki W. et al.*, Grandmaster level in StarCraft II using multi-agent reinforcement learning, *Nature*, vol. 575, 2019, 350–354, <https://doi.org/10.1038/s41586-019-1724-z> [25.11.2025].

[10] იხ.: *Aristotle*, *Nicomachean Ethics*, 1140b8.

დაჯილდოვდეს თუ დაისაჯოს მოდელის მიერ არჩეული კონკრეტული ქმედება ან სტრატეგია. რადგან ეთიკურ მოქმედებას გარე მიზანი არ აქვს, წახალისებაზე დაფუძნებულ სწავლებას არ შეუძლია უბრალოდ განსაზღვროს ერთი კონკრეტული ობიექტური კრიტერიუმი, რომლითაც "LLM"-ის პასუხების შეფასება იქნებოდა შესაძლებელი.

წახალისებაზე დაფუძნებული სწავლების მეორე მნიშვნელოვანი გამოწვევა "LLM"-ების კონტექსტში უკავშირდება ეთიკური ღირებულებების მრავალფეროვნებას. ეთიკის „თამაში", რომლის შესრულებაზეც მოდელი იწვრთნება, არ მოიცავს მხოლოდ ერთ ღირებულებას (ან „სიქველეს", არისტოტელეს ტერმინოლოგიით), არამედ სამის ერთობლიობას. იმისათვის, რათა მომხმარებლის მითითებებზე ეთიკურად და სათანადოდ მოახდინოს რეაგირება, "LLM"-მა ერთდროულად უნდა დაიცვას გამოსადეგობის, გულწრფელობისა და უვნებლობის ღირებულებები.

ეს კი დამატებით სირთულეს ქმნის, რადგან აღნიშნული ღირებულებები ხშირად ერთმანეთს ემთხვევა და ზოგ შემთხვევაში ურთიერთსაწინააღმდეგო ხასიათსაც იძენს, განსაკუთრებით მაშინ, როდესაც ისინი უკიდურესობამდე არის მიყვანილი. მათი თანდაყოლილი ბუნდოვანების გამო, ეს ღირებულებები არ არის ერთმანეთთან სრულად თავსებადი ან, მანქანური სწავლების ტერმინოლოგიით რომ ვთქვათ, მათი ერთდროულად „მაქსიმიზება" შეუძლებელია. გამოსადეგობის, გულწრფელობისა და უვნებლობის ღირებულებებს შორის არსებობს წინააღმდეგობა, რომლის დროსაც ერთი ღირებულების ზედმეტად დაცვა - წინ წამოწევა - იწვევს სხვების შესუსტებას. ეს კიდევ უფრო ართულებს იმ ეთიკური მიზნის ტექნიკურად (პროგრამულად) ფორმირებას, რომლის საფუძველზეც შესაძლებელი იქნებოდა "LLM"-ების წვრთნა წახალისებაზე დაფუძნებული სწავლების გზით. შესაბამისად, პრობლემას წარმოადგენს არა მხოლოდ ეთიკური ღირებულებების პროგრამულად განსაზღვრა, არამედ ასევე იმის გადაწყვეტა, თუ რა პროპორციით უნდა იქნეს გამოყენებული თითოეული ღირებულება მომხმარებლის მითითებაზე პასუხის ფორმულირებისას.

ამგვარად, ჩნდება საკვანძო შეკითხვა: როგორ უნდა განისაზღვროს „გამარჯვება" ანუ „მოგება" ეთიკაში, როდესაც საქმე ეხება წახალისებაზე დაფუძნებულ სწავლებას "LLM"-ების კონტექსტში? ეთიკური კრიტერიუმების ბუნდოვანებისა და გამოსადეგობის, გულწრფელობისა და უვნებლობის ღირებულებებს შორის არსებული შეუთავსებლობის გათვალისწინებით, როგორ შეიძლება ჩამოყალიბდეს ზუსტი მიზანი ან ობიექტი, რომლის საფუძველზეც მოდელი უფრო ეთიკურად ქცევას ისწავლიდა?

ხანგრძლივი პერიოდის განმავლობაში ეს პრობლემა მნიშვნელოვნად აფერხებდა "LLM"-ების ეფექტიან გამოყენებას. გარდატეხა მოხდა სპეციალური ტექნიკის განვითარებით, რომელმაც შესაძლებელი გახადა წახალისებაზე დაფუძნებული სწავლების გამოყენება "LLM"-ების ისეთი ამოცანის შესასრულებლად თუ გასაწვრთნელად, როგორიცაა ეთიკური შეფასება. აღნიშნული მიდგომა ცნობილია, როგორც „ადამიანის უკუკავშირზე

დაფუძნებული წახალისებით სწავლება“ (“reinforcement learning from human feedback” – RLHF).[11]

“RLHF”-ის მუშაობის პრინციპი იმაში მდგომარეობს, რომ იგი პირდაპირ, პროგრამულად არ ცდილობს ეთიკური კრიტერიუმების განსაზღვრას. ამის ნაცვლად, “RLHF” იყენებს მანქანური სწავლების შესაძლებლობებს იმისათვის, რომ, შემფასებელთა ჯგუფის (ადამიანებისგან შემდგარი) პრეფერენციების მოდელირების გზით, არაპირდაპირ „აღმოაჩინოს“, ე.ი. განსაზღვროს ასეთი კრიტერიუმების მახასიათებლები. ზოგადად, ეს ტექნიკა ეფუძნება ხუთსაფეხურიან პროცესს:

1. ადამიანის შემფასებელთა ჯგუფს ეძლევა დავალება, შეაფასოს ერთი და იმავე მითითებაზე “LLM”-ის მიერ გენერირებული რამდენიმე პასუხი და დაალაგოს ისინი ყველაზე ეთიკურიდან ყველაზე ნაკლებად ეთიკურამდე, ე.ი. იმის მიხედვით, თუ რამდენად კარგად ახერხებს თითოეული პასუხი გამოსადეგობის, გულწრფელობისა და უვნებლობის ღირებულებების დაბალანსებას;
2. მიღებული მითითებების, პასუხებისა და შემფასებლების მიერ შედგენილი რეიტინგების საფუძველზე იქმნება ზედამხედველობითი სწავლებისთვის განკუთვნილი მონაცემთა ბაზა, სადაც სწორედ ეს რეიტინგი ასრულებს ეტიკეტის როლს;
3. აღნიშნული მონაცემების გამოყენებით იწვრთნება მოდელი, რომელიც სწავლობს იმ არაპირდაპირ მახასიათებლებს, რომლებიც განსაზღვრავს „მომგებიან“ პასუხს ეთიკის „თამაშში“, ანუ იმ კრიტერიუმებს, რომლებიც რეალურად ასახავს გამოსადეგობის, გულწრფელობისა და უვნებლობის ღირებულებებს;
4. ამგვარად გაწვრთნილი „პრეფერენციების მოდელი“ გამოიყენება, როგორც წახალისების ფუნქცია “LLM”-ისთვის (წახალისებაზე დაფუძნებული სწავლების გარემოში); და
5. საბოლოოდ, “LLM” დამატებით იწვრთნება იმგვარად, რომ მისი ქცევა შეესაბამებოდეს გამოსადეგობის, გულწრფელობისა და უვნებლობის ღირებულებებს — მოდელი ჯილდოვდება იმ პასუხებისთვის, რომლებიც პრეფერენციების მოდელის კრიტერიუმებს აკმაყოფილებს, ხოლო დასანქცირდება იმისთვის, რაც ამ კრიტერიუმებს არ შეესაბამება.

მიუხედავად იმისა, რომ “RLHF” საშუალებას იძლევა ეთიკური მიზანი განისაზღვროს წახალისებაზე დაფუძნებული სწავლებისთვის, ეთიკის „ავტომატიზაციის“ ეს მიდგომა მნიშვნელოვან ნაკლოვანებებს შეიცავს. მისი

[11] იხ.: *Christiano P., Leike J., Brown T. et al.*, Deep Reinforcement Learning from Human Preferences, 2017, <https://arxiv.org/abs/1706.03741> [25.11.2025]; *Ziegler D., Stiennon N., Wu J. et al.*, Fine-Tuning Language Models from Human Preferences, 2019, <https://arxiv.org/pdf/1909.08593.pdf> [25.11.2025]; ასევე იხ.: *Stiennon N., Ouyang L., Wu J. et al.*, Learning to summarize from human feedback, *34th Conference on Neural Information Processing Systems* (NeurIPS 2020), <https://proceedings.neurips.cc/paper/2020/file/1f89885d556929e98d3ef9b86448f951-Paper.pdf> [25.11.2025].

მთავარი ნაკლოვანება არის შემდეგი — ტექნიკა ვერ უზრუნველყოფს იმას, რომ ადამიანებისგან შემდგარი შემფასებელთა ჯგუფის მიერ მიღებული გადაწყვეტილებები რეალურად იყოს სათანადო ან ეთიკური. მხოლოდ ის ფაქტი, რომ ადამიანთა ჯგუფს ევალება შეფასების გაკეთება, თავისთავად არ ნიშნავს, რომ მიღებული შედეგები ეთიკურია. შემფასებლები შესაძლოა თავად იყვნენ მიკერძოებულნი ან მიდრეკილნი შეცდომებისკენ, რის შედეგადაც “RLHF” უბრალოდ ხელახლა დაამკვიდრებს მათ არაეთიკურ მიდგომებს, ამჯერად უკვე — ერთი შეხედვით „ობიექტური“ მათემატიკური პროცესის ფორმით.

გარდა ამისა, შემფასებლების მიუკერძოებელი ჯგუფის შემთხვევაშიც კი, ის პირობები, რომლებშიც მათ უწევთ დასკვნების გამოტანა, შესაძლოა იყოს იძულებითი ან ექსპლუატაციური, რაც უარყოფითად აისახება მათი შეფასების ხარისხზე. მაგალითად, “Time Magazine”-ის ცნობით, “OpenAI”-მ ამ პროცესში დაასაქმა კენიელი შემფასებელთა ჯგუფი, ჯგუფის წევრებს შესრულებული სამუშაოსთვის კი საათში 2 დოლარზე ნაკლებს უხდიდა.[12]

“RLHF”-თან დაკავშირებული კრიტიკის საპასუხოდ შემუშავდა კიდევ ერთი მიდგომა — „ხელოვნური ინტელექტის უკუკავშირზე დაფუძნებული წახალისებით სწავლება“ (“reinforcement learning from AI feedback” – RLAIF).[13] ეს ტექნიკა იმავე ზოგად პროცესს მისდევს, რომელსაც “RLHF”, თუმცა ორი მნიშვნელოვანი განსხვავებით: (1) ადამიანის ნაცვლად, რამდენიმე პასუხის შეფასებას თავად “LLM” ახორციელებს; და (2) ეთიკური ღირებულებების ზოგადი ნაკრების ნაცვლად, “LLM”-ს გადაეცემა ე.წ. „კონსტიტუცია“, რომელიც მოიცავს პრინციპების ერთობლიობას და ამ პრინციპებს გამოყენების შესაბამის ნიმუშებს. სწორედ ამ უკანასკნელი თავისებურების გამო “RLAIF”-ს ხშირად მოიხსენიებენ, როგორც „კონსტიტუციურ ხელოვნურ ინტელექტს“ (“constitutional AI”).

თუმცა, მიუხედავად იმისა, რომ “RLAIF”-მა შესაძლოა გაზარდოს შედეგების მასშტაბურობა, იგი, “RLHF”-ის მსგავსად, კვლავ მოიცავს მნიშვნელოვან ნაკლოვანებებს. კერძოდ, ისევე როგორც “RLHF” ვერ უზრუნველყოფს ადამიანებისგან შემდგარ შემფასებელთა ჯგუფის გადაწყვეტილებების რეალურ ეთიკურობას, “RLAIF” ასევე ვერ იძლევა გარანტიას, რომ “LLM”-ის მიერ განხორციელებული შეფასებები არ იქნება მიკერძოებული ან სხვაგვარად არასწორი. მეტიც, ეს რისკი შესაძლოა, კიდევ უფრო მძაფრად გამოვლინდეს “RLAIF”-ის შემთხვევაში, ვინაიდან მოდელს ეთიკური შეფასების გაკეთება ევალება იმ ეტაპზე, როდესაც იგი თვითონაც ჯერ კიდევ სრულად არ არის ამ მიმართულებით გაწვრთნილი.

[12] *Perrigo B.*, Open AI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic, *Time*, January 18, 2023, <https://time.com/6247678/openai-chatgpt-kenya-workers/> [25.11.2025].

[13] იხ.: *Bai Y., Kadavath S., Kundu S. et al.*, Constitution AI: Harmlessness from AI Feedback, December 2022, <https://arxiv.org/abs/2212.08073> [25.11.2025].

3. მონაცემთა დაცვასა და პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებული რისკები

დიდი ენობრივი მოდელების გამოყენება უკავშირდება მნიშვნელოვან რისკებს პირადი ცხოვრების ხელშეუხებლობის, პერსონალური მონაცემების დაცვისა და მონაცემთა უსაფრთხოების თვალსაზრისით. ამ რისკების ნაწილის პრევენცია ან შემსუბუქება შესაძლებელია, ხოლო ნაწილი შესაძლოა თავად სისტემების ბუნებრივი მახასიათებლიდან გამომდინარეობდეს. წინამდებარე ქვეთავში მიმოვიხილავთ იმ ძირითად რისკებს, რომლებიც "LLM"-ების გამოყენებასთან არის დაკავშირებული. ამასთან, გასათვალისწინებელია, რომ "LLM"-ები წარმოშობს ისეთ საფრთხეებსაც, რომლებიც, მიუხედავად იმისა, რომ უშუალოდ არ უკავშირდება პირადი ცხოვრების ხელშეუხებლობას ან მონაცემთა უსაფრთხოებას, მნიშვნელოვან გავლენას ახდენს ინდივიდებზე და შესაძლოა მოქცეული იყოს მონაცემთა დაცვის ორგანოების „მომხმარებელთა დაცვის მანდატში". ასეთ საფრთხეებს მოიცავს, მათ შორის, ინფორმაციის მანიპულირება, მონაცემთა დამუშავების მასშტაბების ზრდა, დეზინფორმაცია და მცდარი ინფორმაციის გავრცელება. აღნიშნულ ზიანზე ასევე იქნება საუბარი წინამდებარე ქვეთავის ბოლოს.

3.1. მონაცემთა დამუშავების მასშტაბის ზრდა

მასშტაბური სასწავლო მონაცემების საჭიროების გათვალისწინებით, ბევრი "LLM"-ის განმავითარებელი ქმნის სისტემებს, რომლებიც განურჩევლად და უწყვეტად აგროვებს მონაცემებს ინტერნეტიდან.[14] მიუხედავად იმისა, რომ ზოგიერთი კომპანია ამგვარად შეგროვებულ მონაცემებს გამოყენებამდე ამოწმებს და „ასუფთავებს", კარგი პრაქტიკის მაგალითად შეიძლება დასახელდეს "Google"-ის C4 მონაცემთა ბაზა, რომელიც ან საერთოდ არ ახორციელებს ამ შემოწმებას, ან ვერ ახერხებს შემოწმების პროცესის ხარისხის უზრუნველყოფას ინფორმაციის მოცულობის მნიშვნელოვნად შეზღუდვის გარეშე.[15] ამის შედეგად, სასწავლო მონაცემთა ბაზები შესაძლოა შეიცავდეს არაზუსტ, მიკერძოებულ ან დისკრიმინაციულ ინფორმაციას, მათ შორის – პერსონალურ მონაცემებს იმ პირების შესახებ, რომლებიც სრულად არ არიან ინფორმირებულნი იმ ფაქტის შესახებ, რომ მათი მონაცემები გამოიყენება "LLM"-ების გაწვრთნის პროცესში.

[14] მაგალითად იხ.: *Hines K.*, OpenAI Launces GPTBot With Details on How to Restrict Access, *Search Engine Journal*, Aug. 7, 2023, <https://www.searchenginejournal.com/openai-launches-gptbot-how-to-restrict-access/493394/> [25.11.2025]; *Schaul K. et al*., Inside the secret list of websites that make AI like ChatGPT sound smart, *Washington Post*, Apr. 19, 2023, <https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/> [25.11.2025].

[15] *Center for Countering Digital Hate*, Misinformation on Bard, Google's New AI Chat, April 5, 2023, <https://counterhate.com/research/misinformation-on-bard-google-ai-chat/> [25.11.2025].

3.2. მონაცემთა სუბიექტის უფლებების ხელყოფა

დიდი ენობრივი მოდელების ბუნება მნიშვნელოვნად ართულებს მონაცემთა სუბიექტების მიერ გარკვეული უფლებების პრაქტიკულად განხორციელებას, განსაკუთრებით კი პერსონალური მონაცემების გასწორების ან მათი წაშლის მოთხოვნის უფლებას, მაშინ, როდესაც ასეთი მონაცემები უკვე ინტეგრირებულია სასწავლო მონაცემთა ბაზებში. მართალია, ზოგიერთი მონაცემთა ბაზა შედარებით მკაცრად მოწმდება როგორც მონაცემთა მოპოვების, ისე მათი გამოყენების აუცილებლობის თვალსაზრისით, თუმცა განსაკუთრებით ვებწყაროებიდან მასობრივად შეგროვებული მონაცემები ხშირად შეიცავს ისეთ პერსონალურ მონაცემებს, რომელთა დამუშავებაც არ არის აუცილებელი კონკრეტული მიზნის მისაღწევად. გარდა ამისა, ასეთ მონაცემთა ბაზებში შესაძლოა, მოხვდეს პერსონალური მონაცემები, რომლებიც საჯაროდ ხელმისაწვდომი გახდა მონაცემთა უსაფრთხოების დარღვევის – ინციდენტის – შედეგად, ან წარმოადგენს კონკრეტული პირების შესახებ არაზუსტ ან ცილისმწამებლურ ინფორმაციას.

3.2.1. თავის სხვა პიროვნებად წარმოჩენა (იმპერსონაცია) და გამოძალვა

დიდი ენობრივი მოდელების შესაძლებლობები შესაძლოა, განზრახ ბოროტად იქნეს გამოყენებული. ამის მაგალითი შესაძლოა, იყოს კონკრეტული პირის პერსონალური მონაცემების ბოროტად გამოყენება ან ყალბი პერსონალური მონაცემების გენერირება, რომელთა უარყოფა ან გადამოწმება პრაქტიკაში მნიშვნელოვან გამოწვევებს უკავშირდება. აღნიშნულმა შეიძლება სერიოზულად დააზიანოს ინდივიდის ფსიქიკური ჯანმრთელობა, სოციალური ურთიერთობები, რეპუტაცია და სხვა მნიშვნელოვანი ინტერესები.

3.2.2. თაღლითობა

ინდივიდებს შეუძლიათ "LLM"-ების გამოყენება ავტომატიზებული ტექსტური შეტყობინებების, ელექტრონული წერილებისა და სხვა მასობრივი კომუნიკაციის საშუალებების შესაქმნელად. ამასთან, "LLM"-ების მიერ გენერირებული ტექსტი შესაძლოა, გამოყენებულ იქნეს ხელოვნურად შექმნილ აუდიო და ვიდეომასალასთან ერთად, რაც შესაძლებელს ხდის უფრო დამაჯერებელი იმიტაციის ან სხვა პირის სახელით კომუნიკაციის განხორციელებას. აღნიშნულის შედეგად იზრდება არა მხოლოდ თაღლითური აქტივობების საერთო მოცულობა, არამედ მნიშვნელოვნად ფართოვდება თაღლითობაში ჩართულ პირთა წრეც, ვინაიდან "LLM"-ები საშუალებას აძლევს იმ პირებსაც კი, რომელთაც კონკრეტულ ენაში ან კომუნიკაციის გარკვეულ ფორმებში შეზღუდული უნარები აქვთ, შექმნან ბუნებრივად

ჟღერადი და დამაჯერებელი ტექსტები, რომლებიც სხვა შემთხვევაში უფრო იოლად ამოიცნობა, როგორც თაღლითური.

3.3. მონაცემთა უსაფრთხოების რისკები

ჰაკერებს შეუძლიათ "LLM"-ების გამოყენება მავნე პროგრამული კოდის ("malware code") სხვადასხვა ვერსიის შემუშავებისა და დახვეწის მიზნით, აგრეთვე „ფიშინგისა" და „მიზნობრივი ფიშინგის" ("spear-phishing") კამპანიების განხორციელებისთვის, მათ შორის ბიზნესებზე მიმართული თაღლითური ელექტრონული წერილების შესაქმნელად, რომელთა მიზანია მომხმარებელთა ანგარიშის მონაცემების მოპოვება ან ელექტრონული კომუნიკაციის კომპრომეტირება.[16] გარდა ამისა, შესაძლოა, წარმოიშვას "LLM"-ებისთვის დამახასიათებელი ახალი სახის საფრთხეებიც, მათ შორის სასწავლო მონაცემთა ნაკრებებში შეტანილი ინფორმაციის მიზანმიმართული ამოღება („data mining") ან მონაცემთა ბაზების სტრატეგიული და განზრახ „დაბინძურება" არასაიმედო ან მავნე მონაცემებით.

3.4. მიკერძოება

დიდი ენობრივი მოდელები შეიძლება მარტივად იქცეს მიკერძოების წყაროდ, როგორც სასწავლო მონაცემთა ბაზებში არსებული მიკერძოებული ინფორმაციის ინტეგრირების შედეგად, ისე იმ ალგორითმების მეშვეობით, რომლებიც თავად ვითარდება მიკერძოებული მიმართულებით. შედეგად, მიკერძოება აისახება როგორც სისტემის შიდა პროცესებში, ისე "LLM"-ის მიერ გენერირებულ შედეგებში. მართალია, მიკერძოება შესაძლოა, არსებობდეს წინასწარ შერჩეულ და დამუშავებულ მონაცემთა ბაზებშიც, თუმცა განსაკუთრებით მაღალი რისკი წარმოიშობა იმ შემთხვევებში, როდესაც მონაცემთა ბაზები ყალიბდება ინტერნეტიდან მასობრივად შეგროვებული ინფორმაციის საფუძველზე. ასეთ პირობებში სასწავლო მონაცემთა ნაკრები მუდმივად იზრდება და, როგორც წესი, რეგულარულად არ მოწმდება სიზუსტის, მიკერძოების, გამოყენების მიზანშეწონილობისა და სხვა არსებითი კრიტერიუმების მიხედვით.

[16] მაგალითად იხ.: *SlashNext*, The State of Phishing 2023, *SlashNext Security*, Oct. 2023, <https://slashnext.com/state-of-phishing-2023/> [25.11.2025]; *Groll E.*, ChatGPT Shows Promise of Using AI to Write Malware*, CyberScoop*, December 6, 2022, <https://cyberscoop.com/chatgpt-ai-malware/> [25.11.2025]; *Hassold C.*, Executive Impersonation Attacks Targeting Companies Worldwide, *Abnormal Blog*, February 16, 2023, <https://abnormalsecurity.com/blog/midnight-hedgehog-mandarin-capybara-multilingual-executive-impersonation> [25.11.2025]; *Center for Strategic and International Studies*, A Conversation on Cybersecurity with NSA's Rob Joyce*, YouTube*, April 11, 2023, <https://youtu.be/MMNHNjKp4Gs?t=530> [25.11.2025]. (8:50 mark).

3.5. დეზინფორმაცია

დიდი ენობრივი მოდელები ხელს უწყობს დეზინფორმაციის უფრო დიდი მოცულობით გენერირებას, რომლის გავრცელებაც შესაძლებელია ადვილად, დაბალი დანახარჯით და გაცილებით მაღალი სიჩქარით. მსგავსი დეზინფორმაციის პოტენციური გავლენა განსაკუთრებით საგანგაშოა ისეთ სფეროებში, როგორებიცაა არჩევნები, პოლიტიკა და მედია – განსაკუთრებით ჯანმრთელობასა და უსაფრთხოებასთან დაკავშირებულ საკითხებში – ისევე როგორც სხვა კრიტიკულად მნიშვნელოვან სფეროებში.

3.6. მისინფორმაცია / ჰალუცინაციები

მისინფორმაცია დეზინფორმაციის მსგავს პრობლემებს წარმოშობს ერთი მნიშვნელოვანი განსხვავებით - მისინფორმაციის გამავრცელებელმა პირებმა შეიძლება დაიჯერონ, რომ ის ინფორმაცია, რომელსაც ავრცელებენ, ზუსტია. მისინფორმაცია შეიძლება გენერირებული იყოს მომხმარებლის მიერ მიწოდებული პარამეტრებიდან ან დიდი ენობრივი მოდელის მიერ გენერირებული არაზუსტი ინფორმაციიდან.

ზოგადად, ჰალუცინაციების ორი სახეობა არსებობს. პირველი და უფრო აშკარა ჰალუცინაციები, რომლებიც გამოწვეულია ცრუ ან შეცდომაში შემყვანი შინაარსის მინიშნებებით. მაგ., რაც მოხდა მეტა "Galactica"-ს დიდი ენობრივი მოდელის შემთხვევაში. თავდაპირველად იგი განსაზღვრული იყო, როგორც „სამეცნიერო ცოდნის" გაღრმავების მექანიზმი,[17] თუმცა ფუნქციონირება შეწყვიტა სამი დღის შემდეგ, რაც აღმოჩნდა, რომ ის ქმნიდა სამეცნიერო ჟღერადობის, მაგრამ სრულიად ცრუ ვიკიპედიის სტატიებს ისეთ გამოგონილ თემებზე, როგორიცაა „ნაკადის კონდენსატორი" ან „სტრიფ-სეინფელდის თეორემა".[18]

ჰალუცინაციების მეორე სახეობა დიდი ენობრივი მოდელისგან წარმოიშობა, რომლის შესახებ ინფორმაცია მომხმარებლისთვის უცნობია. ეს ჰალუცინაცია უფრო მავნეა და მისი აღმოჩენა რთულია. არსებობს მრავალი მაგალითი,[19] მაგრამ ერთი ცნობილი შემთხვევა ეხება პირის წინააღმდეგ წაყენებულ ცრუ სისხლის სამართლის ბრალდებას. კითხვაზე „რომელ გახმაურებულ საქმეებში მონაწილეობდნენ სამართლის პროფესორები?",[20] "ChatGPT"-მ წარმოადგინა ცრუ ნარატივი, რომელშიც დამტკიცებული იყო, რომ

[17] See *Taylor R., Kardas M., Cucurell G. et al.*, Galactica: A Large Language Model for Science, 2022, <https://arxiv.org/abs/2211.09085> [25.11.2025].

[18] See *Davis E. and Sundstrom A.*, Experiment with GALACTICA, 2022, <https://cs.nyu.edu/~davise/papers/ExperimentWithGalactica.html> [25.11.2025].

[19] See *Marcus G. and Davis E.*, Large Language Models like ChatGPT say The Darnedest Things, 2023, <https://garymarcus.substack.com/p/large-language-models-like-chatgpt> [25.11.2025].

[20] See *Volokh E.*, Large Libel Models: ChatGPT-3.5 Erroneously Reporting Supposed Felony Pleas, Complete with Made-Up Media Quotes?, *Reason*, 2023, <https://reason.com/volokh/2023/03/17/large-libel-models-chatgpt-4-erroneously-reporting-supposed-felony-pleas-complete-with-made-up-media-quotes/> [25.11.2025].

კონკრეტული პროფესორი სტუდენტის სექსუალურ შევიწროებაში იყო ბრალდებული. თუმცა კიდევ უფრო შემაშფოთებელი აღმოჩნდა ის, რომ ცრუ ნარატივის დასამოწმებლად მითითებული იყო ცრუ წყაროები, რომლებიც ამყარებდა აღნიშნულ ნარატივს.

4. კონფიდენციალობის პრინციპი და ტექნიკური ზომები

დიდი ენობრივი მოდელისთვის დამახასიათებელი მონაცემთა დაცვისა და კონფიდენციალობის რისკები ახალი არ არის. დიდი ენობრივი მოდელები და, ზოგადად, გენერირებადი ხელოვნური ინტელექტი, ხელოვნური ინტელექტის სხვა ფორმებისგან განსხვავებით, გამოირჩევა დამუშავებული მონაცემების მასშტაბით, მოდელის შემუშავებისა და მასში გამოყენებული ტექნიკის სირთულით, შემდგომში აღნიშნული მოდელის დანერგვის უპრეცედენტო მასშტაბითა და ტემპით.

ამ ნაწილში ჩვენ განვიხილავთ კონფიდენციალობის პრინციპის გამოყენებას დიდი ენობრივი მოდელისთვის, ასევე, გენერირებად ხელოვნურ ინტელექტთან დაკავშირებულ მონაცემთა დაცვისა და კონფიდენციალობის რისკებს.

4.1. კონფიდენციალობის პრინციპი

4.1.1. კანონიერი საფუძველი

პერსონალური მონაცემების დამუშავების პროცესში ხელოვნური ინტელექტის სისტემების შემქმნელებსა და განმათავსებლებს უნდა ჰქონდეთ მონაცემთა დამუშავების კანონიერი საფუძველი და მათი მოქმედებები შესაბამისობაში უნდა იყოს სხვა მოქმედ კანონმდებლობასთან (მაგ., საავტორო უფლებების შესახებ კანონი). ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლი გვთავაზობს ექვს სამართლებრივ საფუძველს, განსაკუთრებული კატეგორიის მონაცემებისთვის მე-9 მუხლით გათვალისწინებული დამატებითი მოთხოვნებით.

გენერირებადი ხელოვნური ინტელექტის საცდელი მონაცემების მისაღებად უმნიშვნელოვანესია, აღინიშნოს, რომ საჯაროდ ხელმისაწვდომი მონაცემები უმეტეს იურისდიქციაში კვლავ ექცევა მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობის ფარგლებში, როგორც ეს ხაზგასმულია პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეის (“GPA”) საერთაშორისო აღსრულების თანამშრომლობის სამუშაო ჯგუფის (“IEWG”) ბოლოდროინდელ განცხადებაში.[21] აგრეთვე, აშშ-ის

[21] *Global Privacy Assembly (GPA) International Enforcement Cooperation Working Group*, Joint statement on data scraping and the protection of privacy, August 2023, <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf> [25.11.2025].

ფედერალურ სასამართლოებსა და დიდ ბრიტანეთში საავტორო უფლებების დაცვის თაობაზე მისაღებ გადაწყვეტილებებს[22] შეიძლება მნიშვნელოვანი წონა ჰქონდეს კანონიერების პრინციპთან მიმართებით, თუ ჩაითვლება, რომ ვებგვერდიდან მოპოვებული საცდელი მონაცემები არღვევს საავტორო უფლებებისა და ინტელექტუალური საკუთრების კანონმდებლობას. მონაცემთა დაცვის საზედამხედველო ორგანოები, რა თქმა უნდა, ეყრდნობიან სასამართლოების მიერ მიღებულ გადაწყვეტილებებს.

4.1.2. მიზნის შეზღუდვა

დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელებმა და განმათავსებლებმა უნდა უზრუნველყონ, რომ პერსონალური მონაცემები დამუშავდეს კონკრეტული, მკაფიო და ლეგიტიმური მიზნებისთვის. გარდა ამისა, მონაცემები არ უნდა დამუშავდეს ფიზიკური პირების გონივრული მოლოდინის ფარგლებს გარეთ ან შეუთავსებელი მიზნებისთვის.

4.1.3. მონაცემთა მინიმიზაცია

დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელებმა და განმათავსებლებმა მონაცემთა დამუშავება უნდა შეზღუდონ იმით, რაც „აუცილებელია“ მათი მიზნისთვის. რაც უფრო დიდია დამუშავებული პერსონალური მონაცემების მოცულობა, მით უფრო დიდია რისკები.

ნებისმიერი ინფორმაციის ადრეული შეზღუდვა მნიშვნელოვანია მონაცემთა სუბიექტის უფლების დაცვისთვის. ამ მიზნით სისტემის შემქმნელები უნდა ეცადონ, რომ მონაცემთა ნაკრებებში პერსონალური მონაცემების ნებისმიერ შემთხვევაზე გამოიყენონ მონაცემთა მინიმიზაცია. გავრცელებული მიდგომაა მონაცემთა გამორიცხვისა და ანონიმიზაციის პროცედურის გამოყენება, თუმცა, ამ ტექნიკის გამოყენების შემთხვევაშიც კი, შეიძლება რთული იყოს იმის სრულად უზრუნველყოფა, რომ მონაცემთა ნაკრებები არ შეიცავდეს პერსონალურ ინფორმაციას. იმ შემთხვევებში, როდესაც წინასწარ შეგროვებული მესამე მხარის მონაცემთა ნაკრებები გამოიყენება სისტემის გამოსაცდელად, ასევე მნიშვნელოვანია პერსონალური ინფორმაციის ამოღება დამუშავების შემდგომ ეტაპებზე.

[22] *David E.*, Getty lawsuit against Stability AI to go to trial in the UK, *The Verge*, December 4, 2023, <https://www.theverge.com/2023/12/4/23988403/getty-lawsuit-stability-ai-copyright-infringement> [25.11.2025].

4.1.4. გამჭვირვალობა

დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელებმა და განმათავსებლებმა უნდა განახორციელონ გამჭვირვალობის უზრუნველმყოფი ზომები, განსაკუთრებით მონაცემთა სუბიექტებთან მიმართებით, რომლებსაც აქვთ ინფორმაციის მიღების უფლება. ეს უნდა მოიცავდეს ინფორმაციას იმის შესახებ, თუ რა მონაცემი, როგორ, როდის და რატომ გროვდება და გამოიყენება სისტემის სწავლების პროცესში, მათ შორის: საცდელი მონაცემების წყაროებს, პერსონალური ინფორმაციის წაშლის წინასწარ და შემდგომ დამუშავების ზომებს და გენერირებული ტექსტის სანდოობას.

4.1.5. უსაფრთხოება

დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელებმა და განმათავსებლებმა უნდა დანერგონ უსაფრთხოების ზომები. პერსონალური მონაცემები უსაფრთხოდ უნდა იყოს შენახული შენახვის, შემუშავების, ასევე დანერგვის შემდგომი პერიოდის განმავლობაში, რათა გათვალისწინებულ იქნეს ისეთი რთული საკითხები, როგორებიცაა სისტემაზე ე.წ. “სწრაფი ინექციის” შეტევები, მოდელის ინვერსიის შეტევები[23] და მონაცემთა გაჟონვა.

4.1.6. ანგარიშვალდებულება

დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელებმა და განმათავსებლებმა უნდა უზრუნველყონ, რომ მათ შეუძლიათ მონაცემთა დაცვის მოთხოვნებთან შესაბამისობის დემონსტრირება. ანგარიშვალდებულება, ფაქტობრივად, მეტაპრინციპია, რომელიც გარანტის ფუნქციას ასრულებს.

4.1.7. სიზუსტე

დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელებმა და განმათავსებლებმა უნდა უზრუნველყონ, რომ მათ მიერ დამუშავებული ნებისმიერი პერსონალური მონაცემი იყოს ისეთივე ზუსტი, სრული და განახლებული, როგორც ეს

[23] *Veale M., Binns R. and Edwards L.*, Algorithms that remember: model inversion attacks and data protection law, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, October 2018, <https://doi.org/10.1098/rsta.2018.0083> [25.11.2025].

აუცილებელია იმ მიზნებისთვის, რომლისთვისაც ისინი უნდა იქნეს გამოყენებული. ეს განსაკუთრებით ეხება პერსონალურ მონაცემებს, რომლებიც გამოიყენება დიდი ენობრივი მოდელების ან გენერირებადი ხელოვნური ინტელექტის სწავლებისთვის.

ამ პრინციპის მხარდასაჭერად სისტემა შეიძლება განახლდეს (მაგალითად, მოდელის დახვეწით ან გადამზადებით) იმ შემთხვევებში, როდესაც აღმოჩენილი იქნება არაზუსტი ან მოძველებული მონაცემები, როგორებიცაა სისტემის საცდელი მონაცემები. გარდა ამისა, მომხმარებელს უნდა ეცნობოს მონაცემების სიზუსტესთან დაკავშირებული ნებისმიერი ცნობილი პრობლემის ან შეზღუდვის შესახებ. ეს შეიძლება მოიცავდეს იმ შემთხვევებს, როდესაც საცდელი მონაცემები დროში შეზღუდულია (ანუ შეიცავს ინფორმაციას მხოლოდ გარკვეულ თარიღამდე); როდესაც შინაარსზე შეიძლება უარყოფითად იმოქმედოს გარკვეულმა წყაროებმა; ან როდესაც არსებობს კონკრეტული თემები ან მინიშნებები, რომლებიც, როგორც წესი, არაზუსტ შედეგებამდე მიგვიყვანს.

4.1.8. მონაცემთა სუბიექტის უფლებები

მონაცემთა სუბიექტების უფლებები მონაცემთა დაცვის ქვაკუთხედია. დიდი ენობრივი მოდელებისა და გენერირებული ხელოვნური ინტელექტის სისტემების შემქმნელები და განმათავსებლები, რომლებიც ამუშავებენ პერსონალურ მონაცემებს, ვალდებულნი არიან, უზრუნველყონ, რომ პირებს შეეძლოთ თავიანთ მონაცემებზე წვდომა, მათი გასწორება, წაშლა და დამუშავებაზე უარის თქმა, სხვა უფლებებთან ერთად. ეს ასევე მნიშვნელოვანია განსაკუთრებული კატეგორიის პერსონალურ მონაცემებთან და ბავშვთა უფლებების დაცვის საკითხთან დაკავშირებით.

4.2. ტექნიკური საკითხები

როდესაც საქმე დიდი ენობრივი მოდელის სწავლებას ეხება, არსებობს ტექნიკური ჩარევის რამდენიმე ეტაპი და ტიპი, რომელთა განხორციელებაც შესაძლებელია რისკის შესამცირებლად. ამ ნაწილში ჩვენ ყურადღებას გავამახვილებთ ჩარევის ზოგიერთი ვარიანტის გამოყენების უპირატესობებსა და ნაკლოვანებებზე.

4.2.1. მეთვალყურეობა და წინასწარი დამუშავება

დიდი ენობრივი მოდელები ფუნქციონირებისთვის საჭიროებს მასშტაბური რაოდენობით ტექსტურ მონაცემებს და, მათი დამახსოვრების

უნარის გათვალისწინებით,[24] მნიშვნელოვანია მოდელების ფუნქციონირების უზრუნველყოფა იმავე რისკის დაზღვევით, როგორც მათი მომზადებისას. მონაცემთა ნაკრებების შეგროვებისა და მეთვალყურეობის პროცესში შესაძლებელია გადაწყვეტილებების მიღება და ნაბიჯების გადადგმა აღნიშნული რისკის შესამცირებლად.

წყაროს მეთვალყურეობა: განხილვის საგანია, თუ რა ტიპის მონაცემები გამოიყენება მოდელის სწავლებისთვის.[25] ერთი მარტივი განსხვავება – არის თუ არა ეს ინფორმაცია პერსონალური მონაცემი, რადგან ამ ტიპის მონაცემებს აშკარა გავლენა აქვს კონფიდენციალობაზე, როდესაც ისინი გამოიყენება სისტემის გამოცდისთვის, მონაცემთა სუბიექტის სურვილის გათვალისწინების გარეშე. გასათვალისწინებელია საჯაროდ ხელმისაწვდომი და ღია მონაცემები. მიუხედავად იმისა, რომ ყველა საჯარო (ან ღია) მონაცემი საჯაროდ ხელმისაწვდომია, არ უნდა განიხილებოდეს ისე, თითქოს ის მისი ფართო გამოყენებისთვის კვლავ ნებადართულია. განსხვავება მდგომარეობს მონაცემების ხელმისაწვდომობის განზრახვასა და მოლოდინში: საჯარო მონაცემები ეხება მონაცემებს, რომლებიც შეიქმნა ფართოდ გაზიარებისა და გამოყენების მიზნით, მაგალითად, სამთავრობო მონაცემთა ნაკრებები და/ან ვიკიპედიის ტექსტური ნაწილი, მაშინ, როდესაც ზოგიერთი საჯაროდ ხელმისაწვდომი მონაცემი შეიძლება გაზიარებულიყო კონკრეტული შინაარსით გამოყენებისა და მოხმარების მიზნით, მაგალითად, სოციალური მედიის პოსტები და პროდუქტის მიმოხილვები. კვლევამ აჩვენა, რომ აკადემიური კვლევის კონტექსტშიც კი, სოციალური მედიის მომხმარებლები შეიძლება არ გრძნობდნენ თავს კომფორტულად, როდესაც მათი მონაცემები გამოიყენება მათი თანხმობის გარეშე,[26] მაშინაც კი, თუ ის საჯაროდ ხელმისაწვდომია. ამ მოდელების რისკის შესამცირებლად მნიშვნელოვანია მონაცემების მიღება იმ წყაროებიდან, რომლებშიც მონაცემების გამოყენების კონფიდენციალობის მოლოდინები შეესაბამება დიდი ენობრივი მოდელისთვის დასახულ მიზანს.

წინასწარი დამუშავება (მგრძნობიარე მონაცემების წაშლა): მონაცემთა ნაკრებების შედგენის შემდეგი ნაბიჯი გულისხმობს ამ მონაცემების წინასწარ დამუშავებას მოდელების მომზადებისთვის გამოყენებამდე. ამ ეტაპზე შესაძლებელია ავტომატიზებული მექანიზმების გამოყენება მგრძნობიარე ინფორმაციის აღმოსაჩენად და წასაშლელად, მაგალითად, პერსონალური ინფორმაციის, ჯანმრთელობის შესახებ ინფორმაციის და სხვა ინფორმაციის შესახებ. აღნიშნული მექანიზმები შეიძლება მოიცავდეს ამ ინფორმაციის აღმოჩენას და მისი ადამიანის მიერ განხილვისთვის მონიშვნას, ინფორმაციის ავტომატურ წაშლას, ჩანაცვლებას ან დაფარვას.

[24] *Carlini N., Tramer F., Wallace E. et al.*, Extracting Training Data from Large Language Models, *30th USENIX Security Symposium (USENIX Security 21)*, 2633–2650, <https://arxiv.org/abs/2012.07805> [25.11.2025].
[25] "Train" used here encompasses both initial training and any fine tuning or additional training steps.
[26] *Fiesler C. and Proferes N.*, 'Participant' Perceptions of Twitter Research Ethics, *Social Media + Society,* Vol. 4(1), 2018, <https://doi.org/10.1177/2056305118763366> [25.11.2025].

4.2.2. დიფერენციალური კონფიდენციალობა

დიდი ენობრივი მოდელის მომზადებისას შესაძლებელია კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების, მათ შორის, როგორიცაა ("DP"), [27] გამოყენება იმ მოდელების მოსამზადებლად, რომლებიც პირადი ხასიათისაა. ეს შეიძლება გაკეთდეს სხვადასხვა ეტაპზე (მაგ., საცდელი მონაცემები, გამოცდა, შედეგი), განხილვის სხვადასხვა ერთეულით (მაგ., განხილვის დონე, ჯგუფის დონე) და სხვადასხვა პირობებში (მაგ., ცენტრალური, ადგილობრივი, განაწილებული). თითოეულ მათგანს აქვს უნიკალური სარგებელი და ხარჯები, რომლებსაც ამ ნაწილში განვიხილავთ. სხვადასხვა მიდგომის, მათი განხორციელებისა და მოსაზრებების უფრო ყოვლისმომცველი წარმოდგენისთვის მკითხველს ვურჩევთ გაეცნოს სტატიას: „როგორ განვახორციელოთ ML DP-Fy".[28]

კონფიდენციალობის ერთეული: შესაბამისი ერთეულის განსაზღვრა კრიტიკულად მნიშვნელოვანია იმის უზრუნველსაყოფად, რომ არსებობდეს შესაბამისი დონე, რადგან ის განსაზღვრავს, თუ რა ჩაითვლება მონაცემთა ნაკრებად. განხილვის დონის მონაცემთა ბაზა უზრუნველყოფს დაცვას მონაცემთა ნაკრებში შემავალი თითოეული ნიმუშისთვის, ხოლო ჯგუფური დონის მონაცემთა ბაზა უზრუნველყოფს დაცვას აბსტრაქციის უფრო მაღალ დონეზე (მაგ., მომხმარებლის დონეზე, დოკუმენტის დონეზე და ა.შ.). დიდი ენობრივი მოდელებისთვის, შესაძლოა უკეთესი იყოს ჯგუფური დონის მონაცემთა ბაზა, რადგან ამ მოდელების გამოცდისას გამოყენებული თანმიმდევრობა არა მხოლოდ მოდელის მუშაობაზე იმოქმედებს, არამედ კონფიდენციალობის გარანტიებზეც და ამ ორი ფაქტორის გამოყოფა შეიძლება უფრო სასარგებლო იყოს. გარდა ამისა, განხილვის დონეზე მოქმედებათა გამეორების მაღალი ალბათობა, სავარაუდოდ, მნიშვნელოვნად შეასუსტებს გარანტიებს. თუმცა მაინც მნიშვნელოვანია ყურადღებით განვიხილოთ, დაჯგუფების რომელ დონეზეა მიზანშეწონილი კონფიდენციალობის ერთეულის განსაზღვრა. მაგალითად, მიუხედავად იმისა, რომ შეიძლება გვინდოდეს მომხმარებლის დონის "DP"-ის მიწოდება, იმის

[27] The definition of differential privacy that is being used in this section is the one proposed in *Dwork C., McSherry F., Nissim K. and Smith A.*, Calibrating noise to sensitivity in private data analysis, *Procedures of the Third Conference on Theory of Cryptography (TCC)*, 265–284, <http://dx.doi.org/10.1007/11681878_14> [25.11.2025]:

> ჩვენ ვამბობთ, რომ ორი მონაცემთა ნაკრები D და D′ მეზობლები არიან, თუ ისინი განსხვავდებიან ზუსტად ერთი ჩანაწერით; უფრო ზუსტად, ერთი მონაცემთა ნაკრები არის მეორის ასლი, მაგრამ ერთი ჩანაწერით დამატებული ან ამოღებული. დავუშვათ ε არის დადებითი სკალარი. მექანიზმი A უზრუნველყოფს ε-დიფერენციალურ კონფიდენციალობას, თუ ნებისმიერი ორი მეზობელი მონაცემთა ნაკრებისთვის D და D′ და ნებისმიერი S ⊆ Range(A)-სთვის,
>
> $$P[A(D) \in S] \leq \exp(\varepsilon) \times P[A(D') \in S]$$

[28] *Ponomareva N., Vassilvitskii S., Xu Z. et al.*, How to DP-fy ML: A Practical Tutorial to Machine Learning with Differential Privacy, *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23*), 2023, 5823–5824, <https://arxiv.org/abs/2303.00654> [25.11.2025].

გათვალისწინებით, რომ ამ მოდელების წვრთნისთვის ხშირად გამოყენებული მონაცემები ინტერნეტიდან საჯაროდ ხელმისაწვდომი ტექსტია, ამის გაკეთება შესაძლოა შეუძლებელი იყოს, რადგან შეუძლებელია იმის იდენტიფიცირება, თუ რომელი ნიმუშები იყო წარმოდგენილი მომხმარებელთა მიერ.

განხორციელების ეტაპი: არსებობს დეტალიზაციის რამდენიმე დონე, რომელიც დაკავშირებულია იმასთან, თუ როდის შეიძლება "DP"-ის იმპლემენტაცია. გამარტივების მიზნით, ეს ქვეთავი მას მხოლოდ მოდელის ტრენინგის დონეზე განიხილავს. მოდელის ტრენინგის ეტაპზე "DP"-ის გამოყენება იძლევა გარანტიას, რომ მეორე მხარე ვერ შეძლებს განასხვაოს მოდელები, რომლებიც მოიცავს ან არ მოიცავს კონკრეტულ განხილვას ტრენინგის მონაცემებში. ენობრივი მოდელებისთვის ყველაზე მიზანშეწონილი მიდგომები ეხება გრადიენტული მოქმედების საკითხს, რომელშიც ყველაზე ხშირად გამოყენებული ალგორითმია: "DP-SGD". მიზანშეწონილია, რომ დიფერენციალური კონფიდენციალობის დანერგვით დაინტერესებულმა პირებმა გაითვალისწინონ ექსპერტების აზრი ამ თემაზე ან, სულ მცირე, გამოიყენონ არსებული სამეცნიერო რესურსები.[29]

4.2.3. პოსტ-დამუშავება და მანქანური სწავლების გაუქმება

აქტუალური გახდა მიდგომა, რომელსაც მანქანური სწავლების გაუქმება ეწოდება და ორიენტირებულია უკვე გაწვრთნილი მოდელების მოდიფიცირებაზე, რათა მათ შეძლონ სასწავლო მონაცემების კონკრეტული ნაწილების „დავიწყება". ჩვენი კვლევა ორ მთავარ მიდგომაზეა ფოკუსირებული: „ზუსტი" სწავლების გაუქმება და „მიახლოებითი" სწავლების გაუქმება:[30]

- ზუსტი სწავლების გაუქმების მიზანია დიდი ენობრივი მოდელის მიზნობრივი სასწავლო მონაცემების სრულად ჩამოშორება მისგან, თავდაპირველი სასწავლო მონაცემების მრავალ ქვესიმრავლედ დაყოფით. როდესაც მონაცემთა წერტილები იდენტიფიცირებულია წასაშლელად, საჭიროა მხოლოდ იდენტიფიცირებულ მონაცემთა წერტილებთან დაკავშირებული ქვემოდელის ხელახლა პროგრამირება.[31] ეს აჩქარებს სისტემის ხელახალი გამოცდის პროცესს, რაც სხვა შემთხვევაში ძვირადღირებული პროცედურა იქნებოდა;
- მიახლოებითი სწავლების გაუქმება უშუალოდ მოდელზეა ორიენტირებული. შეცვლილი მონაცემებით ხელახალი მომზადების ნაცვლად, ის მოდელის მოცულობას შემდგომში არეგულირებს, რათა

[29] მაგ., იქვე.

[30] იხ.: *Xu J., Wu Z., Wang C. and Jia X.*, Machine Unlearning: Solutions and Challenges, 2024, <https://arxiv.org/abs/2308.07061> [25.11.2025].

[31] See *Yan H., Li X., Guo Z. et al.*, ARCANE: An Efficient Architecture for Exact Machine Unlearning, 2022, <https://www.ijcai.org/proceedings/2022/0556.pdf> [25.11.2025].

შეამციროს სამიზნე სწავლების მონაცემები. მიუხედავად იმისა, რომ ინფორმაციის ჩამოშორება ნაკლებად ზუსტია, იგი გარკვეულ შემთხვევებში შეიძლება ნაკლებად რთულ პროცედურას წარმოადგენდეს.

მიუხედავად იმისა, რომ მანქანური სწავლების გაუქმების მომხრეები ამბობენ, რომ ეფექტური მიდგომა, მისი შემუშავების შემთხვევაში, გააუმჯობესებს კონფიდენციალობას და ხელს შეუწყობს არაზუსტი ან მოძველებული მონაცემების არსებობას, აღნიშნული მონაცემების წაშლა არ შეიძლება უბრალოდ მათი მონაცემთა ბაზიდან წაშლით: მონაცემების გავლენა, როგორიცაა გავლენა მოდელის მოცულობაზე, ასევე უნდა მოიხსნას მანქანური სწავლების ძირითადი მოდელებიდან. გარდა ამისა, როგორც აღინიშნა, ბოლოდროინდელმა კვლევებმა აჩვენა, რომ მოდელის სასწავლო მონაცემებიდან მონაცემების კონკრეტული ფაქტორების ამოღებამ შეიძლება გამოავლინოს სხვა რისკები.[32] ამ ეტაპზე ეს სფერო ჯერ კიდევ შეუსწავლელია და არ არსებობს მკაფიო პასუხი იმის შესახებ, თუ რამდენად ეფექტიანი იქნება „მანქანური სწავლება" მომავალში. ამ პროცესში მონაცემთა სუბიექტის უფლებების პატივისცემა კვლავაც გამოწვევაა.[33]

5. დასკვნა

დიდ ენობრივ მოდელებთან დაკავშირებული საკითხები პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებისთვის ერთგვარ გამოწვევად გადაიქცა. აღნიშნულ ნაშრომში განხილული ტექნოლოგია, სხვა ხელოვნური ინტელექტის სისტემებთან შედარებით, არა მხოლოდ რთულია, უნიკალური დეტალებითა და განვითარების ეტაპებით, არამედ წარმოშობს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის სხვადასხვა რისკს, რომელთა გააზრება დამოკიდებულია ტექნოლოგიის ფუნქციონირების გაგებაზე.

ნაშრომში შევეცადეთ, მოგვეწოდებინა დიდი ენობრივი მოდელების სიღრმისეული ანალიზი, რათა ადამიანები უკეთესად მოემზადონ დიდი ენობრივი მოდელების მიერ შექმნილი გამოწვევების დასაძლევად. პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების პირველი კონტაქტი დიდ ენობრივ მოდელებთან და მასთან დაკავშირებულ გენერირებად ხელოვნურ ინტელექტთან დაკავშირებით მხოლოდ დასაწყისია. მოსალოდნელია, რომ სფეროს განვითარებასთან ერთად გამოწვევებიც გაიზრდება.

[32] See *Carlini et al.*, *supra* note 25.

[33] *Zhang D., Finckenberg-Broman P., Hoang T. et al.*, Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions, *Algorithms that forget: Machine unlearning and the right to erasure, 2023,* <https://arxiv.org/pdf/2307.03941> [25.11.2025].

ბიბლიოგრაფია:

1. *Askell A., Bai Y., Chen A. et al.*, A General Language Assistant as a Laboratory for Alignment, 2021, <https://doi.org/10.48550/arXiv.2112.00861> [25.11.2025].
2. *Aristotle*, *Nicomachean Ethics*, 1140b8.
3. *Bai Y., Kadavath S., Kundu S. et al.*, Constitution AI: Harmlessness from AI Feedback, December 2022, <https://arxiv.org/abs/2212.08073> [25.11.2025].
4. *Bommasani R., Hudson D., Adeli E. et al.*, On the Opportunities and Risks of Foundation Models, August 2021, <https://doi.org/10.48550/arXiv.2108.07258> [25.11.2025].
5. *Carlini N., Tramer F., Wallace E. et al.*, Extracting Training Data from Large Language Models, *30th USENIX Security Symposium (USENIX Security 21)*, 2633–2650, <https://arxiv.org/abs/2012.07805> [25.11.2025].
6. *Center for Countering Digital Hate*, Misinformation on Bard, Google's New AI Chat, April 5, 2023, <https://counterhate.com/research/misinformation-on-bard-google-ai-chat/> [25.11.2025].
7. *Center for Strategic and International Studies*, A Conversation on Cybersecurity with NSA's Rob Joyce*, YouTube*, April 11, 2023, <https://youtu.be/MMNHNjKp4Gs?t=530> [25.11.2025].
8. *Christiano P., Leike J., Brown T. et al.*, Deep Reinforcement Learning from Human Preferences, 2017, <https://arxiv.org/abs/1706.03741> [25.11.2025].
9. *Davis E. and Sundstrom A.*, Experiment with GALACTICA, 2022, <https://cs.nyu.edu/~davise/papers/ExperimentWithGalactica.html> [25.11.2025].
10. *David E.*, Getty lawsuit against Stability AI to go to trial in the UK, *The Verge*, December 4, 2023, <https://www.theverge.com/2023/12/4/23988403/getty-lawsuit-stability-ai-copyright-infringement> [25.11.2025].
11. *Dwork C., McSherry F., Nissim K. and Smith A.*, Calibrating noise to sensitivity in private data analysis, *Procedures of the Third Conference on Theory of Cryptography (TCC)*, 265–284, <http://dx.doi.org/10.1007/11681878_14> [25.11.2025].
12. *Fiesler C. and Proferes N.*, 'Participant' Perceptions of Twitter Research Ethics, *Social Media + Society,* Vol. 4(1), 2018, <https://doi.org/10.1177/2056305118763366> [25.11.2025].
13. *Global Privacy Assembly (GPA) International Enforcement Cooperation Working Group*, Joint statement on data scraping and the protection of privacy, August 2023, <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf> [25.11.2025].
14. *Groll E.*, ChatGPT Shows Promise of Using AI to Write Malware*, CyberScoop*, December 6, 2022, <https://cyberscoop.com/chatgpt-ai-malware/> [25.11.2025].

15. *Hassold C.*, Executive Impersonation Attacks Targeting Companies Worldwide, *Abnormal Blog*, February 16, 2023, <https://abnormalsecurity.com/blog/midnight-hedgehog-mandarin-capybara-multilingual-executive-impersonation> [25.11.2025].
16. *Hines K.*, OpenAI Launces GPTBot With Details on How to Restrict Access, *Search Engine Journal*, Aug. 7, 2023, <https://www.searchenginejournal.com/openai-launches-gptbot-how-to-restrict-access/493394/> [25.11.2025].
17. *IWGDPT*, *Working Paper on Large Language Models (LLMs)*, December 27, 2024, <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.pdf?__blob=publicationFile&v=2> [25.11.2025].
18. *Karpathy A.*, Let's build GPT: from scratch, in code, spelled out, January 2023, <https://www.youtube.com/watch?v=kCc8FmEb1nY> [25.11.2025].
19. *Knight W.*, A Stanford Proposal Over AI's 'Foundations' Ignites Debate, *Wired*, September 2021, <https://www.wired.com/story/stanford-proposal-ai-foundations-ignites-debate/> [25.11.2025].
20. *Khandelwal U., Clark K., Jurafsky D. et al.*, Sample Efficient Text-Summarization Using a Single Pre-Trained Transformer, 2019, <https://doi.org/10.48550/arXiv.1905.08836> [25.11.2025].
21. *Marcus G. and Davis E.*, Large Language Models like ChatGPT say The Darnedest Things, 2023, <https://garymarcus.substack.com/p/large-language-models-like-chatgpt> [25.11.2025].
22. *Perrigo B.*, Open AI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic, *Time*, January 18, 2023, <https://time.com/6247678/openai-chatgpt-kenya-workers/> [25.11.2025].
23. *Ponomareva N., Vassilvitskii S., Xu Z. et al.*, How to DP-fy ML: A Practical Tutorial to Machine Learning with Differential Privacy, *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23*), 2023, 5823–5824, <https://arxiv.org/abs/2303.00654> [25.11.2025].
24. *Schaul K. et al*., Inside the secret list of websites that make AI like ChatGPT sound smart, *Washington Post*, Apr. 19, 2023, <https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/> [25.11.2025].
25. *Silver D., Huang A., Maddison C. et al.*, Mastering the game of Go with deep neural networks and tree search, *Nature*, Vol. 529, 2016, 484–489, <https://doi.org/10.1038/nature16961> [25.11.2025].
26. *SlashNext*, The State of Phishing 2023, *SlashNext Security*, Oct. 2023, <https://slashnext.com/state-of-phishing-2023/> [25.11.2025].
27. *Stiennon N., Ouyang L., Wu J. et al.*, Learning to summarize from human feedback, *34th Conference on Neural Information Processing Systems* (NeurIPS 2020), <https://proceedings.neurips.cc/paper/2020/file/1f89885d556929e98d3ef9b86448f951-Paper.pdf> [25.11.2025].

28. *Taylor R., Kardas M., Cucurell G. et al.*, Galactica: A Large Language Model for Science, 2022, <https://arxiv.org/abs/2211.09085> [25.11.2025].
29. *Veale M., Binns R. and Edwards L.*, Algorithms that remember: model inversion attacks and data protection law, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, October 2018, <https://doi.org/10.1098/rsta.2018.0083> [25.11.2025].
30. *Vinyals O., Babuschkin I., Czarnecki W. et al.*, Grandmaster level in StarCraft II using multi-agent reinforcement learning, *Nature*, vol. 575, 2019, 350–354, <https://doi.org/10.1038/s41586-019-1724-z> [25.11.2025].
31. *Volokh E.*, Large Libel Models: ChatGPT-3.5 Erroneously Reporting Supposed Felony Pleas, Complete with Made-Up Media Quotes?, *Reason*, 2023, <https://reason.com/volokh/2023/03/17/large-libel-models-chatgpt-4-erroneously-reporting-supposed-felony-pleas-complete-with-made-up-media-quotes/> [25.11.2025].
32. *Xu J., Wu Z., Wang C. and Jia X.*, Machine Unlearning: Solutions and Challenges, 2024, <https://arxiv.org/abs/2308.07061> [25.11.2025].
33. *Yan H., Li X., Guo Z. et al.*, ARCANE: An Efficient Architecture for Exact Machine Unlearning, 2022, <https://www.ijcai.org/proceedings/2022/0556.pdf> [25.11.2025].
34. *Zhang D., Finckenberg-Broman P., Hoang T. et al.*, Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions, *Algorithms that forget: Machine unlearning and the right to erasure*, 2023, <https://arxiv.org/pdf/2307.03941> [25.11.2025].
35. *Ziegler D., Stiennon N., Wu J. et al.*, Fine-Tuning Language Models from Human Preferences, 2019, <https://arxiv.org/pdf/1909.08593.pdf> [25.11.2025].

პეტრუ ემანუელ ზლატესკუ*

საერთაშორისო თანამშრომლობის რჩეული ასპექტები შვეიცარიის მონაცემთა დაცვის ახალი ფედერალური აქტის მიხედვით**

შვეიცარიის მონაცემთა დაცვის სრულად განახლებული ფედერალური აქტი ("FADP") მიზნად ისახავს შვეიცარიაში ფიზიკურ პირთა მონაცემების დაცვის გაძლიერებას, კერძოდ, ერთი მხრივ, საერთაშორისო დონეზე მონაცემთა დაცვის სამართლის უახლეს მიღწევებთან შესაბამისობაში მოყვანით და, მეორე მხრივ, უახლეს ტექნოლოგიურ განვითარებასთან ადაპტაციით. ეს ასევე მოიცავს მონაცემთა დაცვისა და ინფორმაციის ფედერალური კომისრის ("FDPIC") უფლებამოსილებების გაძლიერებას. გარე მითითებებისგან დამოუკიდებლობისა და ავტონომიურობის განმტკიცების გარდა, ახალმა აქტმა ("FADP") მონაცემთა დაცვისა და ინფორმაციის ფედერალური კომისარი ("FDPIC") საერთაშორისო თანამშრომლობის სფეროში ახალი კომპეტენციების ფართო სპექტრით აღჭურვა. ამ სფეროს ქვაკუთხედს წარმოადგენს მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის საერთაშორისო ადმინისტრაციული დახმარება და დოკუმენტების უცხოეთში პირდაპირი ჩაბარება. განსახილველი ორივე სამართლებრივი კონცეფცია ფუნდამენტურად ემყარება ორმხრივობის ("reciprocity") პრინციპს.

საკვანძო სიტყვები: შვეიცარიის მონაცემთა დაცვისა და ინფორმაციის ფედერალური კომისარი, შვეიცარიის მონაცემთა დაცვის ფედერალური აქტი, ადმინისტრაციული დახმარება, საერთაშორისო თანამშრომლობა, დოკუმენტების პირდაპირი ჩაბარება.

*ფერნუნის უნივერსიტეტის სამართლის ფაკულტეტის უფროსი ლექტორი და მკვლევარი (შვეიცარია). შვეიცარიის მონაცემთა დაცვისა და ინფორმაციის ფედერალურ კომისართან ("FDPIC") არსებული საერთაშორისო საქმეთა დირექტორატის ხელმძღვანელის მოადგილე.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე“) წარდგენილი მოხსენების ტექსტს. სტატიაში გამოთქმული მოსაზრებები წარმოადგენს ექსკლუზიურად ავტორისას და არ ავალდებულებს მის დამსაქმებელს.

1. შვეიცარიის მონაცემთა დაცვის ახალი ფედერალური აქტი

შვეიცარიის მონაცემთა დაცვის სრულად განახლებული ფედერალური აქტი ("FADP") 2023 წლის 1-ელ სექტემბერს შევიდა ძალაში. ის მიზნად ისახავს მონაცემთა დაცვის გაძლიერებას მონაცემთა დამუშავების გამჭვირვალობის გაუმჯობესებითა და მონაცემთა სუბიექტების მიერ საკუთარ პერსონალურ მონაცემებზე კონტროლის გაზრდით. ამავდროულად, ახალი კანონი მიზნად ისახავს დამუშავებისთვის პასუხისმგებელ პირთა პასუხისმგებლობის გრძნობის გაზრდას, მაგალითად, იმ მოთხოვნის დაწესებით, რომ მათ მონაცემთა დამუშავების ახალი ოპერაციების დაგეგმვისას გაითვალისწინონ მონაცემთა დაცვის რეგულაციები. ასევე, უნდა გაუმჯობესდეს მონაცემთა დაცვის ფედერალურ სტანდარტებთან შესაბამისობისა და მათი გამოყენების ზედამხედველობა. დაბოლოს, შენარჩუნდეს და გაუმჯობესდეს გლობალურ ეკონომიკურ ბაზარზე, კერძოდ, სხვა ქვეყნებში ან საერთაშორისო ორგანიზაციებში პერსონალური მონაცემების გადაცემის ხელშეწყობითა და საზოგადოების დიგიტალიზაციის სფეროში ახალი ეკონომიკური სექტორების განვითარების წახალისებით, რაც დაცვის საერთაშორისოდ აღიარებულ მაღალ სტანდარტს ემყარება.

ახალი კანონის საერთაშორისო განზომილებამ საკვანძო როლი შეასრულა იმ ფართო კონტექსტში, რომლის ფონზეც პერსონალურ მონაცემთა დაცვის შესახებ ეს თანამედროვე საკანონმდებლო აქტი იქნა მიღებული. უახლეს ტექნოლოგიურ განვითარებასთან ადაპტაციის გარდა, აქტის ("FADP") სრული გადასინჯვის ძირითად მიზეზებს შორის იყო საერთაშორისო სამართლის უახლესი მოთხოვნების იმპლემენტაცია და უახლეს საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანა.[1] აქტმა ("FADP") მასშტაბური ცვლილებები განიცადა იმ საერთაშორისო სამართლებრივი ვალდებულებების შესრულების მიზნით, რომლებიც გამომდინარეობს მონაცემთა დაცვის სფეროში შვეიცარიის შენგენის ზონასთან ასოცირებიდან (კერძოდ, რეგულაცია (EU) 680/2016 [LED] [2]) და ევროპის საბჭოს 108+ კონვენციის (CETS No. 223) [3] მოთხოვნებიდან, რომელთა რატიფიცირებაც შვეიცარიამ მოახდინა. ასევე მნიშვნელოვანია ხაზგასმით აღინიშნოს, რომ ახალი აქტი ("FADP") მიზნად ისახავს შვეიცარიის მონაცემთა დაცვის კანონმდებლობის ევროკავშირის კანონმდებლობასთან შესაბამისობის უზრუნველყოფას და,

[1] *Epiney A., Zlătescu E P.,* Art. 1 FADP, in*: Bieri A., Powell J.,*(eds.), OFK DSG, Zurich 2023, note 4; see also *Frey N.,* Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter 17. September 2018.

[2] 2016 წლის 27 აპრილის ევროპარლამენტისა და საბჭოს დირექტივა (EU) 2016/680, კომპეტენტური ორგანოების მიერ სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის ან სისხლისსამართლებრივი სანქციების აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების შესახებ და საბჭოს ჩარჩო-გადაწყვეტილების 2008/977/JHA გაუქმების შესახებ, OJ 2016 L 119, 89.

[3] 2018 წლის 10 ოქტომბრის ოქმი, რომლითაც ცვლილება შედის „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ კონვენციაში" (CETS No. 223).

ამგვარად, "GDPR"-ით გათვალისწინებული ევროკავშირის ადეკვატურობის მოთხოვნების დაკმაყოფილებას[4].[5] 2000 წლიდან შვეიცარია უკვე სარგებლობდა ევროკავშირის მიერ 95/46/EC დირექტივის საფუძველზე მიღებული ადეკვატურობის შესახებ გადაწყვეტილებით[6]. 2024 წელს ევროკომისიამ, "GDPR"-ის შესაბამისად, დაადასტურა შვეიცარიაში მონაცემთა დაცვის დონის ადეკვატურობა[7]. უფრო მეტიც, ახალი აქტი ("FADP") ახდენს ადამიანის უფლებათა ევროპული სასამართლოსა ("ECtHR") და შვეიცარიის ფედერალური უზენაესი სასამართლოს პრეცედენტული სამართლის მრავალი ელემენტის კოდიფიცირებას და, მაგალითად, აწესებს წაშლის უფლებას ("FADP"-ის 32-ე მუხლის მე-2 პუნქტი).

2. "FDPIC"-ის ახალი უფლებამოსილებები და კომპეტენციები

ახალმა აქტმა ("FADP") მნიშვნელოვანი ცვლილებები შეიტანა მონაცემთა დაცვისა და ინფორმაციის ფედერალური კომისრის ("FDPIC") კომპეტენციებსა და უფლებამოსილებებში. კომისარს ახლა პარლამენტი ირჩევს, ხოლო მისი დამოუკიდებლობა და მითითებებისგან თავისუფლება გარანტირებულია ფედერალური აქტით.[8] მონაცემთა დაცვის ფედერალური ორგანოს ეს ინსტიტუციური გაძლიერება, უპირველეს ყოვლისა, საერთაშორისო სამართლიდან მომდინარეობს, კერძოდ, რეგულაციიდან (EU) 680/2016 ("LED"), რომელიც სავალდებულოა შვეიცარიისთვის მისი შენგენის სივრცესთან ასოცირების გამო. 2014 წელს ევროკავშირის მიერ შვეიცარიის მიერ შენგენის მოთხოვნებთან შესაბამისობის შეფასება ასევე ითვალისწინებდა, რომ კომისარი უფლებამოსილი უნდა ყოფილიყო იურიდიულად სავალდებულო გადაწყვეტილებების გამოცემაზე.[9] კომისრის დამოუკიდებლობისა და უფლებამოსილებების გაძლიერების დამატებითი საფუძვლები ასევე გამომდინარეობს ევროპის საბჭოს 108-ე კონვენციის მე-15 და მე-16 მუხლებიდან.

ზემოაღნიშნული პუნქტების გარდა, აღსანიშნავია, რომ სრულად განახლებული აქტი ("FADP") კომისარს ასევე ანიჭებს კომპეტენციებს,

[4] 2016 წლის 27 აპრილის ევროპარლამენტისა და საბჭოს რეგულაცია (EU) 2016/679, ფიზიკურ პირთა დაცვის შესახებ პერსონალურ მონაცემთა დამუშავებასთან და ასეთი მონაცემების თავისუფალ გადაადგილებასთან დაკავშირებით და 95/46/EC დირექტივის გაუქმების შესახებ (პერსონალურ მონაცემთა დაცვის ზოგადი რეგულაცია), OJ 2016 L 119, 1.

[5] *Epiney A., Frei N.,* Die völker- und europarechtliche Einbettung des DSG, in: *Bieri A., Powell J.*(eds.), OFK DSG, Zurich 2023, note 13 et seq.; ასევე იხილეთ, *Wiewiórowski W*., Welcome Letter, Journal of Personal Data Protection Law, 1/2023, 11.

[6] Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ 2000 L 215, 1.

[7] COM(2024) 7 final.

[8] Art. 43 FADP.

[9] *Epiney A., Frei N.,* Die völker- und europarechtliche Einbettung des DSG, in: *Bieri A., Powell J.(eds.),* OFK DSG, Zurich 2023, note 8.

რომლებიც უცხოურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან საერთაშორისო თანამშრომლობის სფეროში ეფექტიანი ჩართულობის საშუალებას იძლევა.[10] აღნიშნული შეესაბამება 108+ კონვენციით გათვალისწინებულ მონაცემთა დაცვის საზედამხედველო ორგანოების როლს. ის მთელ თავს უთმობს[11] მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის თანამშრომლობასა და ურთიერთდახმარებას. ასეთი თანამშრომლობა მიზნად ისახავს, მონაცემთა დაცვის საზედამხედველო ორგანოებს მისცეს საშუალება, შეასრულონ თავიანთი შესაბამისი ვალდებულებები ეროვნული კანონმდებლობის შესაბამისად. მიზანია იმ სულ უფრო ხშირი ტრანსსასაზღვრო შემთხვევების მოგვარება, რომლებშიც ერთი იურისდიქციის მონაცემთა სუბიექტების პერსონალური მონაცემები სხვა სახელმწიფოს ტერიტორიაზე მუშავდება. აქტის ("FADP") სხვადასხვა დებულება ითვალისწინებს კონკრეტულ საშუალებებს, რომლებიც მონაცემთა დაცვისა და ინფორმაციის ფედერალურმა კომისარმა ("FDPIC") შეიძლება გამოიყენოს ტრანსსასაზღვრო საქმეებში როგორც უცხოურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან, ისე უცხოეთში მყოფ დამუშავებისთვის პასუხისმგებელ პირებთან მიმართებით. დიგიტალიზაციის წინსვლისა და მასთან დაკავშირებული, გეოგრაფიული საზღვრებით შეუზღუდავი გლობალური ტექნოლოგიური კომპანიების მიერ თითქმის განუსაზღვრელი რაოდენობის პერსონალური მონაცემების დამუშავების გათვალისწინებით, მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის საერთაშორისო დონეზე თანამშრომლობა არსებითად მნიშვნელოვანია.[12]

შესაბამისად, "FADP"-ის 58-ე მუხლის პირველი პუნქტის „b" ქვეპუნქტი ადგენს, რომ "FDPIC"-მა უნდა ითანამშრომლოს მონაცემთა დაცვაზე პასუხისმგებელ უცხოურ ორგანოებთან. უფრო კონკრეტულად, "FADP"-ის 55-ე მუხლი კომისარს ანიჭებს უფლებამოსილებას, ორმხრივობის პრინციპის შესაბამისად, ჩაერთოს ადმინისტრაციულ დახმარებაში მონაცემთა დაცვის უცხოურ უწყებებთან, ხოლო "FADP"-ის 58-ე მუხლის მე-3 პარაგრაფი განსაზღვრავს "FDPIC"-ის (მონაცემთა დაცვისა და ინფორმაციის ფედერალური კომისრის) კომპეტენციას, განუცხადოს მონაცემთა დაცვის უცხოურ საზედამხედველო ორგანოებს, რომ მათი ოფიციალური დოკუმენტების პირდაპირი ჩაბარება დასაშვებია შვეიცარიაში მონაცემთა დაცვის სფეროში, იმ პირობით, რომ შვეიცარიის მიმართაც გამოყენებული იქნება ანალოგიური, რეციპროკული რეჟიმი. როგორც "FADP"-ის შესაბამისი დებულებებიდან ჩანს, ურთიერთობის უზრუნველყოფა წარმოადგენს ქვაკუთხედსა და ცენტრალურ წინაპირობას "FDPIC"-სა და სხვა იურისდიქციების მის კოლეგებს შორის თანამშრომლობის სხვადასხვა ფორმისთვის. გარდა ამისა, საერთაშორისო სამართლის მიხედვით, შვეიცარია ვალდებულია ითანამშრომლოს და

[10] Art. 58 para. 1 let. b FADP.
[11] Chapter V Convention 108+ (CETS No. 223).
[12] *Kerbosas C., Lennman C.,* in: *Meier P., Métille S.* (eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 55 N 1 *et seq*.

უზრუნველყოს ურთიერთდახმარება მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის: ზოგადად, ევროპის საბჭოს 108+ კონვენციის მე-16 და მომდევნო მუხლების შესაბამისად და სისხლისსამართლებრივი დევნის სფეროში, დირექტივის (EU) 680/2016 ("LED") 46-ე მუხლის პირველი პუნქტის „h" ქვეპუნქტისა და 50-ე მუხლის შესაბამისად.

3. ადმინისტრაციული დახმარება

3.1. ზოგადი შენიშვნები

ადმინისტრაციული დახმარება გულისხმობს "FDPIC"-სა და უცხოურ მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის ინფორმაციისა და პერსონალური მონაცემების გაცვლას კონკრეტულ საქმეში, იმ მიზნით, რომ მომთხოვნ მონაცემთა დაცვის საზედამხედველო ორგანოს მიეცეს თავისი სამართლებრივი მოვალეობებისა და კომპეტენციების შესრულების შესაძლებლობა.[13] 108+ კონვენციის მე-17 მუხლისა და დირექტივის (EU) 2016/860 50-ე მუხლის იმპლემენტაციის მიზნით, 55-ე მუხლი არეგულირებს მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის ურთიერთდახმარებას საერთაშორისო დონეზე.[14] როგორც 108+ კონვენციის მე-17 მუხლშია აღნიშნული, მონაცემთა დაცვის საზედამხედველო ორგანოები ვალდებულნი არიან ითანამშრომლონ იმ ფარგლებში, რომლებიც აუცილებელია მათი კანონისმიერი ამოცანებისა და უფლებამოსილებების შესასრულებლად.[15] "FADP" სრულად არეგულირებს იმ პირობებს, რომელთა საფუძველზეც "FDPIC"-ს შეუძლია ჩაერთოს ადმინისტრაციულ დახმარებაში საზღვარგარეთის მონაცემთა დაცვის საზედამხედველო ორგანოებთან. კომისრის კომპეტენცია, რომელიც განიხილებოდა საკანონმდებლო პროცესში და რომელიც მას უფლებამოსილებას მიანიჭებდა, დაერეგულირებინა თანამშრომლობის ფორმები თავის უცხოელ კოლეგებთან საერთაშორისო საჯარო სამართლის ხელშეკრულებების დადების გზით, კანონში არ იქნა შეტანილი.[16] თუმცა ეს კომპეტენცია "FADP"-ით დელეგირებულია ფედერალურ საბჭოზე, რომელსაც, "FADP"-ის 67-ე მუხლის შესაბამისად, შეუძლია მონაცემთა დაცვის სფეროში საერთაშორისო ხელშეკრულებების დადება. ასეთმა საერთაშორისო შეთანხმებებმა შესაძლოა ასევე დაარეგულიროს თანამშრომლობა მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის.

ხაზგასმით უნდა აღინიშნოს, რომ "FADP"-ის 55-ე მუხლის მოქმედების ფარგლებში, "FDPIC", პრინციპში, არ არის ვალდებული, ჩაერთოს

[13] *Baeriswyl B., in: Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023, Art. 55 N 5; *Rosenthal D.,* Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, note 190.

[14] *Kerbosas C.*, *Lennman C.,* in: *Meier P.*, *Métille S.*(eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 55 N 7.

[15] იხ.: Cécile de Terwagne, La nouvelle loi suisse de protection des données dans le contexte international, in *Epiney A., Moser S., Rovelli S.,* (eds.), Die revision des Datenschutzgesetzes des Bundes, Zurich 2022, 47, 86.

[16] Federal Council, Message accompanying the totally revised FADP, 7104.

ადმინისტრაციულ დახმარებაში. ეს დისკრეციული დებულება კომისარს ანიჭებს უფლებამოსილებას, გადაწყვიტოს, ჩაერთვება თუ არა და როდის ჩაერთვება ადმინისტრაციულ დახმარებაში. მაგალითად, "FDPIC"-ს შეუძლია უარი თქვას ადმინისტრაციული დახმარების მოთხოვნაზე, თუ მომთხოვნი მონაცემთა დაცვის საზედამხედველო ორგანოს კანონმდებლობა არ უზრუნველყოფს მონაცემთა დაცვის ადეკვატურ დონეს "FADP"-ის მე-16 მუხლის მნიშვნელობით.[17]

"FADP"-ის 55-ე მუხლის პირველი პუნქტის ფორმულირების მიუხედავად, სამართალდამცავ საკითხებში შენგენის ქვეყნებს შორის მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის ურთიერთდახმარების უფრო მკაცრი წესები მოქმედებს. მაგალითად, "LED"-ის 50-ე[18] მუხლის შესაბამისად, "FDPIC" ვალდებულია, ურთიერთდახმარება გაუწიოს შენგენის სხვა ქვეყნების მონაცემთა დაცვის საზედამხედველო ორგანოებს. მონაცემთა დაცვის საზედამხედველო ორგანოებმა უნდა მიაწოდონ ერთმანეთს შესაბამისი ინფორმაცია და გაუწიონ ურთიერთდახმარება "LED"-ის თანმიმდევრულად იმპლემენტაციისა და გამოყენების მიზნით, აგრეთვე, თანამშრომლობის ეფექტიანი ზომების დასანერგად. ეს დახმარება მოიცავს ინფორმაციის მოთხოვნას და საზედამხედველო ზომებს, როგორებიცაა კონსულტაციების, ინსპექტირებისა და გამოძიებების ჩატარების მოთხოვნები. "LED"-ის მოქმედების ფარგლებში კომისარი ვალდებულია, შენგენის სივრცის სხვა საზედამხედველო ორგანოს მოთხოვნას უპასუხოს გაუმართლებელი დაყოვნების გარეშე და ნებისმიერ შემთხვევაში, მოთხოვნის მიღებიდან არა უგვიანეს ერთი თვისა.

3.1.1. პირობები

3.1.1.1. ორმხრივობა

"FADP"-ის 55-ე მუხლი ადგენს ხუთ კუმულაციურ პირობას, რომლებიც უნდა დაკმაყოფილდეს იმისთვის, რომ "FDPIC" ჩაერთოს ადმინისტრაციულ დახმარებაში. როგორც ზემოთ აღინიშნა, მათგან პირველი და პრაქტიკაში ყველაზე რელევანტურია რეციპროკულობის მოთხოვნა. დოქტრინის[19] ნაწილის მიერ დაფიქსირებული მოსაზრების მიუხედავად, არც "FADP"-ის 55-ე მუხლის ფორმულირება და არც აქტის მიღების საფუძვლად არსებული საკანონმდებლო პროცესის მასალები არ მიუთითებს რაიმე ფორმალური მოთხოვნების არსებობაზე, როგორიცაა საერთაშორისო შეთანხმების დადება, და არც წინასწარ განსაზღვრული მინიმალური შინაარსის არსებობაზე, რომელიც უნდა იყოს გათვალისწინებული.

[17] იქვე, 7095.
[18] იხ. ასევე შვეიცარიის სისხლის სამართლის კოდექსის 349a და მომდევნო მუხლები.
[19] *Baeriswyl B.,* in*: Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023, Art. 55 note 6.

3.1.1.2 მიზნის შეზღუდვა

ადმინისტრაციული დახმარების არსებითი მახასიათებელია ის, რომ მონაწილე მონაცემთა დაცვის საზედამხედველო ორგანოების მიერ გაცვლილი ინფორმაცია და პერსონალური მონაცემები, სპეციალურობის პრინციპის შესაბამისად, გამოიყენება ექსკლუზიურად იმ კონკრეტული სამართალწარმოებისთვის, რომლისთვისაც მოთხოვნილი იყო ადმინისტრაციული დახმარება. შესაბამისად, "FDPIC"-მა უნდა უზრუნველყოს, რომ ამ მიზნის შეზღუდვა გარანტირებულია მიმღები მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ. მიზნის შეზღუდვის პრინციპის მნიშვნელობა ასევე ასახულია 108+ კონვენციის მე-19 მუხლში, რომლის თანახმადაც, მონაცემთა დაცვის საზედამხედველო ორგანომ, რომელმაც მიიღო ინფორმაცია თავისი ერთ-ერთი უცხოელი კოლეგისგან, მოთხოვნასთან ერთად ან საკუთარ მოთხოვნაზე საპასუხოდ, არ უნდა გამოიყენოს ეს ინფორმაცია მოთხოვნაში მითითებული მიზნებისგან განსხვავებული მიზნებისთვის.

3.1.1.3. პროფესიული, ბიზნეს და კომერციული საიდუმლოება

ადმინისტრაციულ დახმარებაში ჩართვის დამატებითი პირობაა მიმღები ორგანოს ვალდებულება, დაიცვას ადმინისტრაციული დახმარების კონტექსტში მიღებულ ინფორმაციაში მოცემული პროფესიული, ბიზნეს და საწარმოო საიდუმლოება. თუ გადასაცემ ინფორმაციაში ასეთი საიდუმლოებაა მოცემული, "FDPIC" ვალდებულია, ინფორმაციის უცხოური ორგანოსთვის გადაცემამდე შეატყობინოს დაინტერესებულ მხარეებს და მოსთხოვოს მათ მოსაზრებების წარმოდგენა, იმ პირობით, რომ ეს შეუძლებელი არ არის ან არ იწვევს არაპროპორციულ ძალისხმევას. პრაქტიკაში ამ მოთხოვნას შეიძლება შეზღუდული მოქმედების სფერო ჰქონდეს, რადგან, მაგალითად, "FADP"-ის 50-ე მუხლის მე-2 პუნქტის თანახმად, პროფესიული საიდუმლოება, პრინციპში, გამორიცხულია იმ ინფორმაციიდან, რომელიც "FDPIC"-ისთვის ხელმისაწვდომი უნდა გახდეს გამოძიების კონტექსტში.

3.1.1.4. მესამე პირებისთვის გამჟღავნება

მიმღები ორგანოს მიერ მესამე პირებისთვის გადაცემული ინფორმაციისა და პერსონალური მონაცემების გამჟღავნება მოითხოვს მონაცემთა გადამცემი მონაცემთა დაცვის საზედამხედველო ორგანოს წინასწარ თანხმობას.

3.1.1.5. პირობები ან შეზღუდვები

“FADP” ასევე უფლებას აძლევს გადამცემ მონაცემთა დაცვის საზედამხედველო ორგანოს, დაუწესოს პირობები ან შეზღუდვები მიმღებ ორგანოს გადაცემულ პერსონალურ მონაცემებსა და ინფორმაციასთან დაკავშირებით. დოქტრინის მიერ იდენტიფიცირებული შესაძლო პირობების მაგალითებია: პერსონალური მონაცემების ანონიმიზაციის მოთხოვნები, კონკრეტული ვადის დაწესება, რომლის ფარგლებშიც პერსონალური მონაცემები უნდა წაიშალოს მიმღები ორგანოს მიერ, ან პირობა, რომ ინფორმაცია და პერსონალური მონაცემები შეიძლება გადაიცეს მხოლოდ იმ შემთხვევაში, თუ FDPIC-ს ასევე ეცნობება უცხოეთში ჩატარებული გამოძიების შედეგები.[20]

3.1.2. ადმინისტრაციული დახმარების ობიექტი

იმ პერსონალურ მონაცემებსა და ინფორმაციასთან დაკავშირებით, რომლებიც “FDPIC”-მა შეიძლება გაუცვალოს თავის კოლეგა საზედამხედველო ორგანოებს ადმინისტრაციული დახმარების ფარგლებში, “FADP” გვთავაზობს არასრულ ჩამონათვალს. კერძოდ, ეს მოიცავს დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვინაობას, დამუშავებულ პერსონალურ მონაცემებს, დამუშავების მიზანს, მიმღებს ან მონაცემთა სუბიექტის ვინაობას. ეს უკანასკნელი შეიძლება გამჟღავნდეს მხოლოდ იმ შემთხვევაში, თუ მონაცემთა სუბიექტმა გასცა თანხმობა ან თუ ეს აუცილებელია პროცესში ჩართული ერთ-ერთი მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ სამართლებრივი ამოცანის შესასრულებლად.

4. დოკუმენტების პირდაპირი ჩაბარება უცხოეთში

4.1. ზოგადი მოსაზრებები

საზედამხედველო ორგანოებს შორის საერთაშორისო თანამშრომლობის სფეროში სრულად გადასინჯული "FADP“-ის კიდევ ერთი მნიშვნელოვანი სიახლე უკავშირდება მონაცემთა დაცვის უცხოური უწყებების მიერ ოფიციალური დოკუმენტების პირდაპირ ჩაბარებას. შვეიცარიის კანონმდებლობით, ოფიციალური დოკუმენტის უცხოეთში მყოფი ადრესატისთვის ან უცხოეთიდან შვეიცარიაში ჩაბარება წარმოადგენს საჯაროსამართლებრივ აქტს, რომელიც, ტერიტორიული სუვერენიტეტის გამო, არ შეიძლება სხვა სახელმწიფოს ტერიტორიაზე განხორციელდეს.

[20] *Baeriswyl B., in: Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023, Art. 55 note 11.

ზოგადად, ასეთი ქმედება უნდა განხორციელდეს ან ადრესატის საცხოვრებელი ქვეყნის მიერ საერთაშორისო საჯარო სამართლის ხელშეკრულების მეშვეობით, ან ნებადართული უნდა იყოს მეორე ქვეყნის მიერ. შესაბამისი ნებართვის არარსებობის შემთხვევაში, გადაწყვეტილებების, დადგენილებების ან სხვა ოფიციალური დოკუმენტების უცხოეთში პირდაპირი შეტყობინება, ადრესატის საცხოვრებელი სახელმწიფოს წინასწარი თანხმობის მიღებისა და ამ უკანასკნელის კანონმდებლობით ან ორმხრივი/მრავალმხრივი საერთაშორისო ხელშეკრულებით დადგენილი პროცედურების დაცვის გარეშე, წარმოადგენს აღნიშნული სახელმწიფოს სუვერენიტეტისა და დამოუკიდებლობის დარღვევას. ამ შემთხვევაში შეტყობინება, ფედერალური სასამართლოს პრეცედენტული სამართლის თანახმად, არის აბსოლუტურად ბათილი.[21]

შვეიცარიის კანონმდებლობა შეიცავს ორ სამართლებრივ საფუძველს, რომლებიც შვეიცარიის ტერიტორიული იურისდიქციის ფარგლებში უცხოური ოფიციალური დოკუმენტების ჩაბარების შესაძლებლობას იძლევა: "FADP"-ის 58-ე მუხლის მე-3 პუნქტი და 1977 წლის 17 ნოემბრის ადმინისტრაციულ საკითხებთან დაკავშირებული დოკუმენტების უცხოეთში ჩაბარების შესახებ ევროპული კონვენცია (CETS No. 094).

4.2. "FADP"-ის 58-ე მუხლის მე-3 პუნქტი

"FADP"-ის 55-ე მუხლით რეგულირებული, სიტყვის მკაცრი გაგებით, ურთიერთდახმარების პროცედურის გარდა, "FDPIC"-ს, "FADP"-ის 58-ე მუხლის მე-3 პუნქტის შესაბამისად, შეუძლია უფლება მისცეს უცხოურ მონაცემთა დაცვის საზედამხედველო ორგანოებს, პირდაპირ გადმოსცენ თავიანთი გადაწყვეტილებები შვეიცარიაში, შვეიცარიის სისხლის სამართლის კოდექსის 271-ე მუხლის დარღვევის გარეშე. "FADP"-ის 58-ე მუხლის მე-3 პუნქტის მნიშვნელობით პირდაპირი ჩაბარება მოითხოვს კომისრის მიერ უცხოური მონაცემთა დაცვის საზედამხედველო ორგანოს მიმართ ზოგადი და აბსტრაქტული განცხადების გაკეთებას. ის არ შემოიფარგლება კონკრეტული ინდივიდუალური შემთხვევით ან საქმეთა კონკრეტული კატეგორიით. 55-ე მუხლის მსგავსად, "FADP"-ის 58-ე მუხლის მე-3 პუნქტიც პირდაპირი ჩაბარების წინაპირობად ორმხრივობის უფლებას მოიაზრებს. ჩაბარება შეიძლება განხორციელდეს საფოსტო მომსახურებით ან გამგზავნი სახელმწიფოს დიპლომატიური ან საკონსულო წარმომადგენლობის მეშვეობით.[22]

"FADP"-ის 58-ე მუხლის მე-3 პუნქტის ფორმულირების თანახმად, პირდაპირი შეტყობინება შეიძლება ზოგადად ნებადართული იყოს "FDPIC"-ის მიერ, თუ დაკმაყოფილებულია სამი კუმულაციური პირობა: პირდაპირი

[21] Swiss Federal Supreme Court, BGE 143 III 28 cons.2.2.1.

[22] *Cattaneo G.,* in: *Meier P., Métille S*., (eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 58 note 79.

შეტყობინება შვეიცარიის პერსპექტივიდან შემოიფარგლება მონაცემთა დაცვის სფეროთი, შეტყობინებას ახორციელებს ადმინისტრაციული ორგანო, რომელსაც კონკრეტულად ევალება მონაცემთა დაცვა, და შვეიცარიას მინიჭებული აქვს „რეციპროკული“ უფლება. ამ პირობების გარდა, დოქტრინის ნაწილი მიიჩნევს, რომ აუცილებელია არსებული ინტერესების დაბალანსება, ნებართვის გაცემის პოტენციური შედეგების გათვალისწინებით შვეიცარიის სუვერენიტეტსა და უცხოური ოფიციალური აქტების ადრესატებზე. საჯარო ინტერესებს შორის, გასათვალისწინებელია კანონის უზენაესობის პატივისცემა (კერძოდ, კანონიერებისა და პროპორციულობის პრინციპები), საგარეო პოლიტიკური ინტერესები და შვეიცარიისთვის ნებართვის გაცემის ან მასზე უარის თქმის შედეგები, განსაკუთრებით ეკონომიკისა და პერსონალური მონაცემების დაცვის თვალსაზრისით. იმავე ავტორის თანახმად, კერძო ინტერესები უნდა მოიცავდეს კანონით დაცული საიდუმლოების პატივისცემას, უცხოურ სამართალწარმოებაში სამართლებრივი დაცვის ეფექტიანი საშუალებების ხელმისაწვდომობას, დამოუკიდებელი და მიუკერძოებელი სასამართლო კონტროლის არსებობას, ეკონომიკურ ინტერესებს, მონაცემთა სუბიექტების ინტერესებს მათი პერსონალური მონაცემების დაცვის კუთხით და სახელმწიფოს მონაცემთა დაცვის რეჟიმის ადეკვატურობას ნებართვის გაცემის მიზნებისთვის.[23]

4.2.1 ადმინისტრაციულ საკითხებთან დაკავშირებული დოკუმენტების უცხოეთში ჩაბარების შესახებ ევროპული კონვენცია

ევროპის საბჭოს ათმა წევრმა სახელმწიფომ[24] მოახდინა კონვენციის რატიფიცირება. კონვენციის პირველი მუხლის პირველი პუნქტი ადგენს, რომ ხელშემკვრელი სახელმწიფოები იღებენ ვალდებულებას, გაუწიონ ურთიერთდახმარება ადმინისტრაციულ საკითხებში დოკუმენტების ჩაბარებისას. პრინციპში, შეთანხმება ვრცელდება ყველა ადმინისტრაციულ საკითხზე, გარდა საგადასახადო და სისხლის სამართლის საკითხებისა. პირველი მუხლის მე-3 პუნქტის შესაბამისად, მხარეებს ასევე შეუძლიათ, გამორიცხონ სამართლის სხვა სფეროები. კონვენციის ხელმოწერისას შვეიცარიამ გააკეთა დეკლარაციული განცხადება, რომლის თანახმადაც, კონვენციის მოქმედების სფერო არ ვრცელდებოდა საფინანსო ბაზრების ზედამხედველობასა და სადაზვერვო საქმიანობის საკითხებზე. შესაბამისად, შეიძლება დავასკვნათ, რომ ამ კონვენციის დებულებები ვრცელდება მონაცემთა დაცვის სფეროზე. ამ მოსაზრებას ამყარებს ის ფაქტი, რომ, ერთი მხრივ, კონვენციის პირველი მუხლის მე-2 პუნქტში არ არსებობს მონაცემთა

[23] იქვე.

[24] რატიფიკაციების სტატუსის სანახავად, იხილეთ: <https://www.coe.int/en/web/conventions/full-list2?module=signatures-by-treaty&treatynum=094> [24.7.2025].

დაცვის შესახებ რაიმე პირდაპირი გამონაკლისი და, მეორე მხრივ, შვეიცარიას არ გაუკეთებია განცხადება იმის თაობაზე, რომ მონაცემთა დაცვა უნდა გამოირიცხოს კონვენციის მოქმედების სფეროდან. კერძოდ, კონვენცია ითვალისწინებს შეტყობინების განხორციელებას დიპლომატიური ან საკონსულო არხებით (მე-12 მუხლი), საფოსტო მომსახურებით (მე-11 მუხლი), მომთხოვნი სახელმწიფოს საკონსულო თანამდებობის პირების ან დიპლომატიური აგენტების მეშვეობით (მე-10 მუხლი), ან მოთხოვნილი სახელმწიფოს ცენტრალური ორგანოს მეშვეობით (მე-2 და მომდევნო მუხლები). როგორც წესი, კონვენციის მე-6 მუხლის შესაბამისად, მომთხოვნ ორგანოს შეუძლია, გადაუგზავნოს ბრძანება იმ ქვეყნის ცენტრალურ ორგანოს, სადაც ჩაბარება უნდა განხორციელდეს. აღნიშნული ორგანო შემდგომში დოკუმენტს ადრესატს ჩააბარებს და მომთხოვნ ორგანოს ჩაბარების დამადასტურებელ დოკუმენტს დაუბრუნებს. როგორც კონვენციის მე-2 მუხლის პირველ პუნქტშია აღნიშნული, თითოეული ხელშემკვრელი სახელმწიფო ნიშნავს ცენტრალურ ორგანოს, რომელიც პასუხისმგებელია სხვა ხელშემკვრელი სახელმწიფოების ორგანოებისგან ადმინისტრაციულ საკითხებში დოკუმენტების ჩაბარების შესახებ მოთხოვნების მიღებასა და ასეთ მოთხოვნებზე რეაგირებაზე. ფედერაციულ სახელმწიფოებს შეუძლიათ, დანიშნონ ერთზე მეტი ცენტრალური ორგანო. შვეიცარიამ გააკეთა განცხადება, რომლის თანახმადაც, კონვენციის მიზნებისთვის მისი ცენტრალური ორგანოა იუსტიციის ფედერალური სამსახური.

კონვენცია ავალდებულებს წევრ სახელმწიფოებს, გაუწიონ ურთიერთდახმარება ადმინისტრაციულ საკითხებში დოკუმენტების ჩაბარებისას.[25] ფედერალური საბჭოს გზავნილის თანახმად, შეთანხმება მიზნად ისახავს თანამშრომლობის ხელშეწყობას იმ შემთხვევებში, როდესაც არ არსებობს ურთიერთდახმარების მარეგულირებელი სამართლებრივი დებულებები. მიუხედავად იმისა, რომ "FADP"-ის 55-ე მუხლი არ ეხება დოკუმენტების ჩაბარებას, ის უნდა განიმარტოს საერთაშორისო სამართლის შესაბამისად და შეთანხმების ჭრილში. კონვენცია ასევე გასათვალისწინებელია "FADP"-ის 58-ე მუხლის მე-3 პუნქტის გამოყენებისას.

იმის გათვალისწინებით, რომ ფედერალური კანონი "FADP"-ის 58-ე მუხლის მე-3 პუნქტის სახით სრულყოფილად არ არეგულირებს მონაცემთა დაცვის სფეროში უცხოური ოფიციალური ადმინისტრაციული დოკუმენტების პირდაპირ ჩაბარებას, არამედ ამას აკეთებს ერთი ზოგადი დებულების მეშვეობით, შეგვიძლია ვივარაუდოთ, რომ "FADP" და კონვენცია თავსებადია, რადგან ორივე მიზნად ისახავს მონაცემთა დაცვის დებულებების სწრაფი და ეფექტიანი გამოყენებისა და აღსრულების გაძლიერებას. ნებისმიერ შემთხვევაში, "FADP"-ის 58-ე მუხლის მე-3 პუნქტი უნდა განიმარტოს საერთაშორისო სამართლის შესაბამისად. აგრეთვე, აღსანიშნავია, რომ საკანონმდებლო მასალები არ მიუთითებს იმაზე, რომ ფედერალურ ასამბლეას, აქტის სრული გადასინჯვისას "FADP"-ის 58-ე მუხლის მე-3 პუნქტის

[25] Federal Gazette, 2017 5957.

მიღებისას, განზრახული ჰქონდა, მიეღო კონვენციის საწინააღმდეგო დებულება. შესაბამისად, კონვენციით დადგენილი შეტყობინების პროცედურები ვრცელდება იმ შემთხვევებზე, როდესაც იმ ქვეყნების მონაცემთა დაცვის საზედამხედველო ორგანოები, რომლებმაც მოახდინეს კონვენციის რატიფიცირება, ითხოვენ დოკუმენტების ჩაბარებას შვეიცარიის ტერიტორიაზე.

5. დასკვნა

მიუხედავად იმისა, რომ საქმეების მასშტაბი, რომლებსაც მონაცემთა დაცვის საზედამხედველო ორგანოები თავიანთ ყოველდღიურ პრაქტიკაში აწყდებიან, შეიძლება უზარმაზარი იყოს, პროცედურული ასპექტები, რომლებსაც ისინი მართავენ, თანაბრად გადამწყვეტ როლს თამაშობს მათი ძალისხმევის შედეგების ფორმირებაში. შვეიცარიის მონაცემთა დაცვის ფედერალური აქტის საერთაშორისო განზომილების კონტექსტში პროცედურული საკითხები წინა პლანზე გამოდის. ისეთი თემები, როგორებიცაა მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის ადმინისტრაციული დახმარება ან მათი დოკუმენტების უცხოეთში პირდაპირი ჩაბარება, ასახავს საერთაშორისო თანამშრომლობაში ჩართულ რთულ პროცესებს. ეს ელემენტები ხაზს უსვამს ეფექტიანი კოორდინაციის მნიშვნელობას მნიშვნელოვანი საქმეების ეფექტიანად სამართავად. “FADP”-ის სხვადასხვა დებულება ითვალისწინებს კონკრეტულ საშუალებებს, რომლებიც “FDPIC”-მა შეიძლება გამოიყენოს ტრანსსასაზღვრო შემთხვევებში როგორც უცხოურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან, ისე უცხოეთში მყოფ დამუშავებისთვის პასუხისმგებელ პირებთან მიმართებით. საერთაშორისო თანამშრომლობის ამ ფორმების ფარგლებში „რეციპროკულობის“ იურიდიულად სავალდებულო გარანტია საკვანძო როლს ასრულებს.

ბიბლიოგრაფია:

1. „ადმინისტრაციულ საკითხებთან დაკავშირებული დოკუმენტების უცხოეთში ჩაბარების შესახებ ევროპული კონვენცია“ (CETS No. 094).
2. 2016 წლის 27 აპრილის ევროპარლამენტისა და საბჭოს დირექტივა (EU) 2016/680, კომპეტენტური ორგანოების მიერ სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის ან სისხლისსამართლებრივი სანქციების აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების შესახებ და საბჭოს ჩარჩო-გადაწყვეტილების 2008/977/JHA გაუქმების შესახებ, OJ 2016 L 119, 89.
3. 2016 წლის 27 აპრილის ევროპარლამენტისა და საბჭოს რეგულაცია (EU) 2016/679, ფიზიკურ პირთა დაცვის შესახებ პერსონალურ მონაცემთა დამუშავებასთან და ასეთი მონაცემების თავისუფალ გადაადგილებასთან დაკავშირებით და 95/46/EC დირექტივის გაუქმების შესახებ (პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია), OJ 2016 L 119, 1.
4. შვეიცარიის ფედერალური საბჭო, გზავნილი, რომელიც თან ახლავს მონაცემთა დაცვის ფედერალური აქტის სრულ გადასინჯვას და მონაცემთა დაცვის სფეროში სხვა ნორმატიული აქტების ცვლილებას, 2017 წლის 15 სექტემბერი, OJ 2017 9641.
5. *Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023.
6. *Bieri A., Powell J., (*eds.), OFK DSG – Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zurich 2023.
7. Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ 2000 L 215, 1.
8. *Epiney A., Moser S., Rovelli S.,* (eds.), Die Revision des Datenschutzgesetzes des Bundes, Zurich 2022.
9. *Frei N.,* Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter 17. September 2018.
10. *Meier P., Métille S. (*eds.), Loi fédérale sur la protection des données, Basel 2023.
11. *Rosenthal D.,* Das neue Datenschutzgesetz, in: Jusletter 16. November 2020.
12. Wiewiórowski W., Welcome Letter, Journal of Personal Data Protection Law 1/2023, 11.

რეიჩელ მასტერტონი[*]

საერთაშორისო თანამშრომლობა: შესაძლებლობების გაფართოება და გავლენის გაძლიერება[**]

პერსონალურ მონაცემთა დამუშავება ხშირად გლობალური მასშტაბით ხორციელდება და, შესაბამისად, გლობალური გავლენაც აქვს. რეგულირება კი, თავის მხრივ, გეოგრაფიული საზღვრების შესაბამისად არის აგებული. ამ გეოგრაფიული განსხვავებების აღმოფხვრა შესაძლებელია საერთაშორისო თანამშრომლობით, რომელიც ლოურენს ლესიგის[1] მიერ "Pathetic Dot" მოდელშია განსაზღვრული რეგულირების ოთხი მოდალობის გამოყენების გზით. ამ თანამშრომლობას შეუძლია გაზარდოს მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უწყებების შესაძლებლობები და გააძლიეროს მათი გავლენა.

საკვანძო სიტყვები: *ლესიგი, "Pathetic Dot" მოდელი, მონაცემთა დაცვა, საერთაშორისო თანამშრომლობა, რეგულირება, პირადი ცხოვრების ხელშეუხებლობა.*

1. შესავალი

პერსონალური მონაცემები იქცა გლობალურ ბიზნესად, რომელიც გეოგრაფიულ საზღვრებს სცდება. თუმცა იმ სუბიექტების რეგულირება, რომლებიც პერსონალური მონაცემებით სარგებელს იღებენ, კვლავ მყარად არის მიბმული ამ ტრადიციულ იურისდიქციულ საზღვრებთან. იმ შემთხვევაშიც კი, როდესაც კანონმდებლობა საერთოა რამდენიმე ქვეყნისთვის, როგორიცაა ევროკავშირის „მონაცემთა დაცვის ძირითადი

[*] სამართლის მაგისტრი (LLM), პერსონალურ მონაცემთა დაცვის კომისრის მოადგილე, გერნზის მონაცემთა დაცვის საზედამხედველო ორგანო.

[**] ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე") წარდგენილი მოხსენების ტექსტს.

[1] *Lessig L.,* Code Version 2.0, Basic Books, 2006.

რეგულაცია“[2], თითოეულ იურისდიქციას ჰყავს საკუთარი, ზოგ შემთხვევაში კი რამდენიმე უწყება, რომელსაც რეგულირება და აღსრულება ევალება.

შესაბამისად, მონაცემთა დაცვის საზედამხედველო ორგანოების საერთაშორისო თანამშრომლობა სასიცოცხლოდ მნიშვნელოვანია განსხვავებული სამართლებრივი ჩარჩოების ერთმანეთთან შესათავსებლად, რათა მოხდეს გლობალურ პრობლემებზე გლობალური რეაგირება. თუმცა საერთაშორისო თანამშრომლობით უფრო მეტის მიღწევაა შესაძლებელი, ვიდრე უბრალოდ სამართლებრივი განსხვავებების აღმოფხვრა.

წინამდებარე ნაშრომი მიზნად ისახავს, გამოიკვლიოს *ლოურენს ლესიგის*[3] მიერ შემოთავაზებული რეგულირების ოთხი მოდალობა — კანონი, სოციალური ნორმები, ბაზარი და არქიტექტურა — და კონკრეტული შემთხვევების ანალიზის საფუძველზე წარმოადგინოს, თუ როგორ შეუძლია ამ მოდალობებს, საერთაშორისო თანამშრომლობასთან ერთად, დაეხმაროს მონაცემთა დაცვის საზედამხედველო ორგანოებს შესაძლებლობების გაფართოებასა და გავლენის გაძლიერებაში.

2. *ლესიგის* რეგულირების მოდალობების გაგება

ლოურენს ლესიგმა რეგულირების ოთხი მოდალობის, იგივე “Pathetic Dot Model”-ის, შესახებ პირველად თავის წიგნში „კოდი და კიბერსივრცის კანონები“ დაწერა. მან წამოაყენა მოსაზრება, რომ სუბიექტი („წერტილი“) ემორჩილება ოთხ განსხვავებულ ძალას, რომლებიც მის ქცევას აკონტროლებს ან არეგულირებს. ეს ოთხი ძალაა: კანონი, სოციალური ნორმები, ბაზარი და არქიტექტურა — *ლესიგის* შემთხვევაში, კიბერსივრცის საფუძვლად არსებული „კოდი“.

კანონი ადგენს წესებს, რომლებითაც სახელმწიფო საქმიანობის გაკონტროლებას ისახავს მიზნად. ის კოდიფიცირებას უკეთებს იმას, თუ რა არის სწორი და რა — არასწორი, და ქმნის მექანიზმებს საქმიანობის კანონიერების შესაფასებლად და იმ ქმედებების სანქცირებისთვის, რომლებიც არასწორად იქნება მიჩნეული. ამგვარად, „წერტილი“ იგებს, თუ რა არის კანონიერი და რა შეიძლება მოჰყვეს კანონის დარღვევას.

სოციალური ნორმები არის ქცევის დაუწერელი წესები, რომლებიც საზოგადოების შიგნით მოქმედებს. მათ სახელმწიფო კი არ ადგენს, არამედ იმ საზოგადოების წევრები, რომლებსაც ეს ნორმები ეხებათ. თუ არ არსებობს თანაკვეთა რომელიმე საკანონმდებლო აქტთან, სოციალური ნორმის დარღვევის ან უგულებელყოფის შემთხვევაში ფორმალური სანქციები, როგორც წესი, არ წესდება. თუმცა საზოგადოება ხშირად თავად გამოდის ქცევის შემფასებლის როლში და საკუთარ დამოკიდებულებას სხვა გზებით

[2] ევროპის პარლამენტისა და საბჭოს რეგლამენტი (EU) 2016/679, 2016 წლის 27 აპრილის, პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოქცევის შესახებ [2016] OJ L119.

[3] *Lessig L.*, Code and the Other Laws of Cyberspace, Basic Books, 1999.

გამოხატავს. წარსულში ეს ზეპირსიტყვიერად ხდებოდა. დღეს, ციფრულ ეპოქაში, სოციალური ნორმებია იმის მიზეზი, რომ მომხმარებლების მიერ გენერირებული შეფასებების პლატფორმებს, მათ შორის როგორიცაა "TripAdvisor", ასეთი დიდი ძალაუფლება აქვთ. ისინი ასახავენ არა იმას, თუ რა ქცევაა კანონიერი ან უკანონო, არამედ იმას, თუ რამდენად დააკმაყოფილა ბიზნესის ქცევამ მომხმარებლის მოლოდინები და კარგისა და ცუდის შესახებ არსებული საზოგადოებრივი შეხედულება.

ბაზარი, რომელზეც „წერტილი" ოპერირებს, დიდი ხანია, რაც საქმიანობის რეგულირების ერთ-ერთ საშუალებას წარმოადგენს. ბაზრები ფასებს მიწოდებისა და მოთხოვნის საფუძველზე ადგენენ. ბიზნესს შეუძლია იშვიათ პროდუქტზე უფრო მაღალი ფასი დააწესოს, ვიდრე უფრო გავრცელებულზე, იმ შემთხვევაშიც კი, როდესაც ობიექტური შეფასებით, მათ შესაძლოა ერთნაირი ღირებულება ჰქონდეთ. ბაზრებს ასევე შეუძლიათ განსაზღვრონ, თუ რა არის მისაღები პროდუქტი ან მომსახურება, და ისინი, ვინც ამ სტანდარტს ვერ აკმაყოფილებენ, შედარებისას შესაძლოა წაგებულ პოზიციაში აღმოჩნდნენ.

არქიტექტურა გულისხმობს იმ ფიზიკურ და სიტუაციურ ფაქტორებს, რომლებიც „წერტილზე" შემზღუდავად მოქმედებს. როგორც *ლესიგი* აღნიშნავს, არქიტექტურა არის „ის, თუ როგორია სამყარო ან მისი კონკრეტული ასპექტები". არქიტექტურა აყალიბებს ადამიანის ქცევას. მაგალითად, ქალაქის გეგმარება აკონტროლებს ან ზღუდავს, თუ როგორ ურთიერთქმედებს მასთან ადამიანი. ადამიანს უწევს, მიჰყვეს გზებს და შენობებს გვერდი აუაროს, ვიდრე პირდაპირ ხაზზე („როგორც ყვავი დაფრინავს") გადაადგილდეს.

ლესიგის წიგნი უმეტესად კიბერსივრცის რეგულირებას ეხება და დაიწერა იმ ფართოდ გავრცელებული მოსაზრების საპასუხოდ, რომლის თანახმადაც, კიბერსივრცე არ ექვემდებარებოდა რეგულირებას. ამიტომ ამ საკითხს გარკვეული რეზონანსი აქვს მონაცემთა დაცვის სამყაროშიც და წინამდებარე ნაშრომში მოგვიანებით უფრო დეტალურად იქნება განხილული. თუმცა მოდელის განხილვისას ნათელი ხდება, რომ რეგულირების ოთხი მოდალობა მხოლოდ ონლაინ სამყაროსთვის არ არის დამახასიათებელი და მათი გამოყენება ქცევის რეგულირებისთვის სხვა სფეროებშიც შეიძლება. *ლესიგი* ამტკიცებს, რომ ეს ოთხი მოდალობა მოქმედებს „წერტილზე" როგორც ინდივიდუალურად, ისე ხშირად ერთდროულად, გარემოებების მიხედვით მეტ-ნაკლები ხარისხით, და რომ ყველა მოდალობის ერთად გამოყენებას უფრო დიდი გავლენა ექნება, ვიდრე მხოლოდ ერთ-ერთზე ფოკუსირებას.

მაგალითისთვის საკმარისია განვიხილოთ კლიმატის ცვლილებასთან ბრძოლის გლობალური ინიციატივა. ხელშეკრულებების ხელმოწერითა[4] და კანონმდებლობის მიღებით[5] ხდება ემისიების შემცირება და „სათბურის

[4] კლიმატის ცვლილების შესახებ გაეროს ჩარჩო კონვენციის პარიზის შეთანხმება, მიღებული 2015 წლის 12 დეკემბერს, T.I.A.S. No. 16-110.

[5] კლიმატის ცვლილების აქტი 2008 (c. 27).

აირების“ ზოგიერთი ყველაზე მავნე წყაროს აღმოფხვრა — ეს არის რეგულირება კანონით. სკოლები, კოლეჯები და მესამე სექტორის ორგანიზაციები ასწავლიან ადამიანებს, თუ რა ცვლილების მოხდენა შეუძლიათ ქცევის შეცვლით და სხვებსაც ცვლილებებისკენ მოუწოდებენ — ეს არის რეგულირება სოციალური ნორმებით. კომპანიები ცვლიან წარმოების მეთოდებს და ქმნიან ახალ, „უფრო მწვანე“ პროდუქტებს, რითაც საბაზრო წილს ართმევენ უფრო დამკვიდრებულ, მაგრამ მავნე პრაქტიკებს — ეს არის რეგულირება ბაზრის მიერ. ამასთანავე, არაგანახლებადი და მავნე ენერგიის წყაროების გლობალური მარაგები იწურება, რაც სამყაროს ალტერნატიულ ენერგიაზე დაფიქრებას აიძულებს — ეს არის რეგულირება არქიტექტურით.

ამ ოთხი მოდალობის ცენტრში იმყოფება „წერტილი“. მიუხედავად იმისა, წარმოადგენს თუ არა „წერტილი“ ამ მაგალითში ადამიანს თუ კომპანიას, ოთხივე მოდალობა მოქმედებს მასზე, ახდენს ზეწოლას სხვადასხვა გზით, მაგრამ საბოლოოდ ყველა მათგანი არეგულირებს „წერტილის“ ქცევას.

3. მონაცემთა დაცვის საერთაშორისო რეგულაციის ლანდშაფტი

2025 წლის 2 ივლისის მდგომარეობით, გაეროს ვაჭრობისა და განვითარების კონფერენციის („UNCTAD“[6]) მიერ გამოქვეყნებული სტატისტიკის თანახმად, მსოფლიოს ქვეყნების 79%-ს ჰქონდა მონაცემთა დაცვის ან პირადი ცხოვრების ხელშეუხებლობის შესახებ რაიმე ფორმის კანონმდებლობა, ხოლო ქვეყნების დამატებით 3%-ს — კანონპროექტი. მიუხედავად იმისა, რომ ეს კანონები ადგენს პერსონალურ მონაცემთა მოპოვების, გამოყენებისა და შენახვის ჩარჩოებს, არ არსებობს ერთიანი, ყოვლისმომცველი სამართლებრივი ინსტრუმენტი, რომელსაც 80%-ვე ქვეყანა აღიარებს. ორგანიზაციები, რომლებიც რამდენიმე სხვადასხვა იურისდიქციაში ოპერირებენ, ხშირად აწყდებიან ამ კანონებით შექმნილი მარეგულირებლების მოთხოვნებსა და მოლოდინებს შორის განსხვავებებს. ზოგ შემთხვევაში, მაგალითად, ამერიკის შეერთებულ შტატებში, კანონმდებლობა შტატზე[7] ან სექტორზეა[8] ორიენტირებული, რაც სხვადასხვა გარემოებაში განსხვავებული წესების არსებობას გულისხმობს, თუნდაც ერთი ქვეყნის შიგნით.

ამასთან, არსებობს ორი მნიშვნელოვანი სამართლებრივი ჩარჩო: ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ და ევროპის საბჭოს 108-ე[9] კონვენცია, რომლებიც მსოფლიოს მრავალი ქვეყნის მონაცემთა

[6] UN Trade & Development, ‘Data Protection and Privacy Legislation Worldwide’ <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

[7] The California Privacy Rights Act of 2020, implemented & enforced by the California Privacy Protection Agency <https://cppa.ca.gov/about_us/>.

[8] Health Insurance Portability and Accountability Act of 1996 (HIPAA) <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>.

[9] ევროპის საბჭო, პერსონალური მონაცემების ავტომატური დამუშავების დროს ფიზიკური პირების დაცვის შესახებ კონვენცია, ETS 108.

დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობის საფუძველს წარმოადგენს. ამ ორ ჩარჩოს შორის ბევრი საერთო მახასიათებელია. ორივე მათგანი ფუნდამენტურ პრინციპებს ემყარება: პერსონალურ მონაცემთა დამუშავება უნდა იყოს კანონიერი, სამართლიანი და გამჭვირვალე; მონაცემები უნდა შეგროვდეს კონკრეტული, ლეგიტიმური მიზნებისთვის და არ უნდა იქნას გამოყენებული ამ მიზნების მიღმა. ორივე ჩარჩო ფიზიკურ პირებს ანიჭებს უფლებებს მათ პერსონალურ მონაცემებზე. ესენია: პერსონალურ მონაცემებზე წვდომის, მათი შესწორებისა და წაშლის მოთხოვნის და დამუშავების შეწყვეტის მოთხოვნის უფლება.

ორივე ჩარჩო აქცენტს აკეთებს ანგარიშვალდებულებაზე და მოითხოვს მათგან, ვინც პერსონალურ მონაცემებს იყენებს, დანერგონ შესაბამისი ზომები კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად და შეეძლოთ ამ შესაბამისობის დემონსტრირება. და რადგან ორივე მათგანი შექმნილია იურისდიქციების მიღმა გამოსაყენებლად, ორივე ჩარჩო შეიცავს დებულებებს მონაცემთა საერთაშორისო გადაცემის შესახებ, რათა დაეხმაროს ბიზნესს ოპერირებაში და უზრუნველყოს, რომ ამ ჩარჩოებით გათვალისწინებული დაცვის გარანტიები პერსონალურ მონაცემებს თან სდევდეს.

თუმცა, ფართო მსგავსებების მიუხედავად, ამ ორ ჩარჩოს შორის მნიშვნელოვანი განსხვავებებიც არსებობს. “GDPR” ევროკავშირის რეგულაციაა და, შესაბამისად, პირდაპირ მოქმედებს ევროკავშირის წევრ სახელმწიფოებში. ის ასევე დეტალური და იმპერატიულია, რაც ქმნის მყარ ჩარჩოს, რომელიც ერთნაირია მთელ ევროკავშირსა და ევროპის ეკონომიკურ სივრცეში. “GDPR” ითვალისწინებს მექანიზმს, რომლის მიხედვითაც მესამე ქვეყნებს შეუძლიათ მიმართონ, რათა მათი მონაცემთა დაცვის კანონმდებლობა და მარეგულირებელი ჩარჩოები ადეკვატურად იქნას ცნობილი. მესამე ქვეყნის “GDPR”-თან არსებითად ეკვივალენტურად შეფასება უზრუნველყოფს პერსონალური მონაცემების თავისუფალ მიმოქცევას ევროკავშირსა და ადეკვატურ იურისდიქციებს შორის, იმ დამატებითი გარანტიების გარეშე, რომლებსაც ევროკავშირის საზღვრებს გარეთ მონაცემთა გადაცემა ჩვეულებრივ მოითხოვს. დღეისათვის მიღებულია 16 ასეთი გადაწყვეტილება.

ამის საპირისპიროდ, 108-ე კონვენცია საერთაშორისო ხელშეკრულებაა და, მიუხედავად იმისა, რომ სახელმძღვანელო პრინციპებს ადგენს, ის არ არის ისეთივე იმპერატიული, როგორიც “GDPR”. ხელმომწერ იურისდიქციებს მოეთხოვებათ, მიიღონ საკუთარი შიდა სამართლებრივი აქტები კონვენციის პრინციპების იმპლემენტაციისთვის. შესაბამისად, მიუხედავად იმისა, რომ მისი მოქმედების არეალი უფრო ფართოა, ვიდრე “GDPR”-ის, შესაძლოა არსებობდეს განსხვავებები იმპლემენტაციაში იმ 55 იურისდიქციას შორის, რომლებმაც ის მიიღეს — ევროპის საბჭოს 47 წევრი სახელმწიფო და ხუთი არაევროპული ქვეყანა[10].

[10] Council of Europe ‘Chart of signatures and ratifications of Treaty 108’. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

მიუხედავად იმისა, რომ კანონმდებლობა შესაძლოა განსხვავდებოდეს მსოფლიოს მასშტაბით, მსგავსი მიზნების მქონე სხვადასხვა იურისდიქციის მარეგულირებლებს შორის თანამშრომლობა დიდი ხანია, რაც მარეგულირებელი სფეროს მნიშვნელოვანი ნაწილია. 1979 წელს, გერმანიის ქალაქ ბონში, მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კომისართა პირველი საერთაშორისო კონფერენცია გაიმართა[11]. ეს კონფერენცია, რომელიც ყოველწლიურად სხვადასხვა ქვეყანაში ტარდება (გარდა "COVID-19" პანდემიის დროს გამართული ორი „დისტანციური" ღონისძიებისა) და რომელსაც ადგილობრივი მონაცემთა დაცვის ან პირადი ცხოვრების ხელშეუხებლობის მარეგულირებელი მასპინძლობს, გაიზარდა როგორც მასშტაბით, ისე სამოქმედო არეალით. ორგანიზაციას სახელი შეეცვალა და ეწოდა პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეა[12] ("GPA"). "GPA", რომელსაც ხელმძღვანელობს აღმასრულებელი კომიტეტი და მხარს უჭერს სამდივნო, იზიარებს შემდეგ ხედვას: პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეის ლიდერობის კონსოლიდაცია პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის სფეროში, მისი ხმისა და გავლენის გაზრდა გეოგრაფიულ და ლინგვისტურ ქსელებში და უწყებების აღსრულების შესაძლებლობების გაძლიერება მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უფრო მაღალი გლობალური დონის მისაღწევად, რაც უზრუნველყოფს მონაცემთა სუბიექტების ეფექტურ დაცვას.[13]

გარდა იმისა, რომ "GPA" თავისი 130-ზე მეტი წევრისა და დამკვირვებლისთვის ყოველწლიურ სადისკუსიო ფორუმს წარმოადგენს, მან ასევე მიიღო გეგმა[14], რომელიც მის სტრატეგიულ მიზნებს ასახავს. ეს მიზნები ფოკუსირებულია მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უფრო მაღალი გლობალური დონის მიღწევაზე, "GPA"-სა და მისი წევრების ხმისა და გავლენის გაზრდა და აღსრულების შესაძლებლობების გაძლიერებაზე. ამ მიზნების მისაღწევად

"GPA"-ს აქვს რამდენიმე სამუშაო ჯგუფი[15], რომლებიც აერთიანებენ წევრ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უწყებებს. ისინი ერთობლივად მუშაობენ, რათა მიაღწიონ იმაზე მეტს, ვიდრე ცალ-ცალკე შეეძლოთ.

[11] Global Privacy Assembly 'History of the Assembly' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.

[12] Global Privacy Assembly <https://globalprivacyassembly.org/.

[13] Global Privacy Assembly 'Mission and Vision' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/>.

[14] Global Privacy Assembly 'Strategic Plan 2023 – 2025' <https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf>.

[15] Global Privacy Assembly 'Working Group Reports' <https://globalprivacyassembly.org/document-archive/working-group-reports/>.

წინამდებარე ნაშრომის თემისთვის განსაკუთრებით აქტუალურია საერთაშორისო აღსრულებისა და თანამშრომლობის სამუშაო ჯგუფი[16]. 2019 წელს მუდმივმოქმედ სამუშაო ჯგუფად ჩამოყალიბებულ "IEWG"-ს აქვს მანდატი, „ჩაუყაროს საფუძველი "IEWG"-სა და "GPA"-ს მიერ პრაქტიკული აღსრულების კუთხით თანამშრომლობის ხელშეწყობას[17]", განსაკუთრებული აქცენტით გლობალურ საკითხებზე, რომლებმაც შეიძლება გავლენა მოახდინოს ადამიანების მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უფლებებზე. ის ასევე ისახავს მიზნად, შეიმუშაოს და ხელი შეუწყოს პრაქტიკული ინსტრუმენტების დანერგვას საერთაშორისო აღსრულების სფეროში თანამშრომლობისთვის და განავითაროს საკომუნიკაციო ხაზები სხვა რელევანტურ ჯგუფებთან და პირადი ცხოვრების ხელშეუხებლობის უწყებებთან „შესაძლებლობების კოორდინირებისა და გამოყენების"[18] მიზნით. "IEWG"-ის მიერ მხარდაჭერილი ერთ-ერთი ინსტრუმენტია აღსრულების სფეროში თანამშრომლობის სახელმძღვანელო[19], რომელიც განსაზღვრავს გზებს, თუ როგორ შეუძლიათ უწყებებს ერთად იმუშაონ საერთო მიზნების მისაღწევად. "IEWG"-ის მუშაობა და ეს სახელმძღვანელო განხილული იქნება ნაშრომის შემდეგ ნაწილში.

პირადი ცხოვრების ხელშეუხებლობის დაცვის აღსრულების გლობალური ქსელი[20] ("GPEN") შეიქმნა ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის ("OECD") რეკომენდაციის საპასუხოდ, რომელიც პირადი ცხოვრების ხელშეუხებლობის დაცვის კანონების აღსრულებაში ტრანსსასაზღვრო თანამშრომლობას ეხებოდა[21]. ამ დოკუმენტის 21-ე პუნქტი მოითხოვდა „პირადი ცხოვრების ხელშეუხებლობის დაცვის აღსრულების უწყებებისა და სხვა შესაბამისი დაინტერესებული მხარეების არაფორმალური ქსელის შექმნას" თანამშრომლობის საკითხების განსახილველად და ტრანსსასაზღვრო პრობლემებთან გამკლავების საუკეთესო პრაქტიკის გასაზიარებლად. "GPEN"-ის ერთ-ერთი მთავარი ინიციატივაა ყოველწლიური „შემოწმება" ("Sweep") — მექანიზმი, რომელიც „მიზნად ისახავს პირადი ცხოვრების ხელშეუხებლობის უფლებებისა და პასუხისმგებლობების შესახებ ცნობიერების ამაღლებას, პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობასთან შესაბამისობის წახალისებას და საერთაშორისო პირადი ცხოვრების ხელშეუხებლობის აღსრულების უწყებებს შორის თანამშრომლობის გაძლიერებას[22]". "GPEN"-ის სამოქმედო გეგმის ნაწილია

[16] Global Privacy Assembly 'International Enforcement Working Group Report – July 2024' <https://globalprivacyassembly.org/wp-content/uploads/2024/11/9.-IEWG-GPA-Annual-Report-2024.pdf>.
[17] იქვე.
[18] იქვე.
[19] Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.
[20] Global Privacy Enforcement Network <https://privacyenforcement.net/content/home-public>.
[21] OECD, Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352.
[22] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

„ქსელების ქსელის[23]“ შექმნა, რომელიც მოიცავს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის სხვა ქსელებს, ასევე, სხვა მარეგულირებელ ქსელებს, რომელთა ინტერესებიც “GPEN”-ის ინტერესებს კვეთს. ერთ-ერთი მაგალითია 2024 წლის „შემოწმება“, რომლის ფარგლებშიც “GPEN”-მა ითანამშრომლა მომხმარებელთა უფლებების დაცვის აღსრულების საერთაშორისო ქსელთან[24] ვებგვერდებსა და აპლიკაციებში შეცდომაში შემყვანი დიზაინის პატერნების შესასწავლად[25]. ეს საკითხი, როგორც თანამშრომლობის სარგებლის მაგალითი, უფრო დეტალურად იქნება განხილული შემდეგ ნაწილში.

4. “Pathetic Dot” მოდელის გამოყენება მონაცემთა დაცვის სფეროში საერთაშორისო თანამშრომლობისთვის

მარეგულირებელთა საერთაშორისო თანამშრომლობის კონტექსტში *ლესიგის* “Pathetic Dot” მოდელის განხილვისას კანონის მოდალობის შესაბამისობა აშკარაა. მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის ყველა მარეგულირებელი კანონის საფუძველზეა შექმნილი; ისინი კანონმდებლობით არიან დაფუძნებული და სწორედ კანონმდებლობა ანიჭებთ მათ უფლებამოსილებებსა და მოვალეობებს. კანონი ადგენს მოთხოვნებს ორგანიზაციებისთვის პერსონალურ მონაცემთა დამუშავებისას და განსაზღვრავს ფიზიკური პირების უფლებებს. კანონი ითვალისწინებს დარღვევის შესახებ შეტყობინებისა და საჩივრის მექანიზმებს, ჩარჩოებს; თუ როგორ უნდა განიხილონ მარეგულირებლებმა ასეთი საკითხები, და სანქციებს, რომლებიც შეიძლება დაწესდეს დარღვევისთვის. როგორც *ლესიგმა* აღნიშნა, კანონი უბიძგებს რეგულირებად სუბიექტებს მოიქცნენ სახელმწიფოს მოთხოვნების შესაბამისად და სჯის მათ, ვინც ამ მოთხოვნებს არ იცავს.

როგორც კანონის საფუძველზე შექმნილი სუბიექტებისთვის ციფრულ სამყაროში, რომელიც საზღვრებს არ ცნობს, ალბათ გარდაუვალია, რომ მონაცემთა მასშტაბური დარღვევების გამოძიება თანამშრომლობის მთავარი საგანია. დიდი კომპანიების მიერ ჩადენილი დიდი დარღვევები ხშირად ძლიერ რეაგირებას მოითხოვს და ერთი მონაცემთა დაცვის საზედამხედველო ორგანოსთვის შესაძლოა სასარგებლო აღმოჩნდეს სხვა იურისდიქციის მსგავსი შეხედულებების მქონე მარეგულირებელთან ძალების გაერთიანება.

საერთაშორისო თანამშრომლობის უახლესი მაგალითი იყო გენეტიკური ტესტირების კომპანია “23andMe”-ის მიერ მონაცემთა დარღვევის ფაქტზე ერთობლივი გამოძიება, რომელსაც კანადის პირადი ცხოვრების

[23] Global Privacy Enforcement Network ‘Action Plan for the Global Privacy Enforcement Network (GPEN)’ <https://privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>.
[24] ICPEN <https://www.icpen.org/>.
[25] Global Privacy Enforcement Network ‘2024 GPEN Sweep on deceptive design patterns’ <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

ხელშეუხებლობის კომისრის ოფისი ("OPC")[26] და გაერთიანებული სამეფოს ინფორმაციის კომისარი[27] ("ICO") ატარებდნენ. ეს თანამშრომლობა, ალბათ, გასაკვირი არ არის იმის გათვალისწინებით, რომ ორივე მარეგულირებელმა მთავარი წვლილი შეიტანა აღსრულების სფეროში თანამშრომლობის სახელმძღვანელოს[28] შექმნაში, რომელიც, სხვა საქმიანობებთან ერთად, აღწერს, თუ როგორ შეიძლება ჩატარდეს ერთობლივი გამოძიებები.

2023 წლის ოქტომბერში ერთ-ერთმა პირმა განაცხადა, რომ მან შეაღწია "23andMe"-ის სისტემებში და ხელთ ჰქონდა პერსონალური მონაცემების ასლები, რომლებსაც გასაყიდად სთავაზობდა. იმავე თვის ბოლოს "23andMe"-მ აცნობა "OPC"-სა და "ICO"-ს, რომ დაზარალებულ პირთა ნაწილი მათი იურისდიქციებიდან იყო.

მიუხედავად იმისა, რომ ორ იურისდიქციას საკუთარი კანონმდებლობა ჰქონდა, მათ შორის საკმარისი მსგავსება არსებობდა, რათა ერთობლივი გამოძიება განხორციელებადი ყოფილიყო. ეს შესაძლებელი გახდა ორ მარეგულირებელს შორის გაფორმებული ურთიერთგაგების მემორანდუმით, "PIPEDA"-ს[29] 23.1-ე სექციისა და გაერთიანებული სამეფოს "GDPR"-ის 50-ე მუხლის შესაბამისად. 2025 წლის ივნისში გამოქვეყნებული ერთობლივი გამოძიების შედეგად დადგინდა დარღვევები როგორც "PIPEDA"-ს, ისე გაერთიანებული სამეფოს "GDPR"-ის მიხედვით. გამოძიების მსვლელობისას "23andMe"-მ აღმოფხვრა ეს ხარვეზები, რის გამოც საკითხები მოგვარებულად ჩაითვალა[30]. თუმცა საკანონმდებლო ჩარჩოებს შორის განსხვავების მაგალითად, "ICO"-ს ჰქონდა დაჯარიმების უფლებამოსილება და დარღვევის დადგენის გარდა, 2,310,000[31] ფუნტი სტერლინგის ოდენობის ფულადი ჯარიმაც დააკისრა.

"Pathetic Dot" მოდელის კანონის მოდალობის გამოყენება ბუნებრივია მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის მარეგულირებლებისთვის, ხოლო საერთაშორისო პარტნიორებთან თანამშრომლობას შეუძლია მარეგულირებლის შესაძლებლობების გაფართოება და მისი გავლენის გაძლიერება. თუმცა გამოძიებები შეიძლება იყოს ხანგრძლივი და ფოკუსირებული მხოლოდ ერთი ორგანიზაციის ქცევაზე. "23andMe"-ის მიმართ ჩატარებული გამოძიებისა და დაწესებული სანქციის ეფექტიანობაში ეჭვის შეტანა შეუძლებელია. გამოძიების პერიოდში, ორი მარეგულირებლის განსაკუთრებული დაკვირვების ქვეშ ყოფნისას, კომპანიამ

[26] Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.

[27] ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.

[28] Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.

[29] Personal Information Protection and Electronic Documents Act (PIPEDA).

[30] Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.

[31] ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.

აღმოფხვრა ხარვეზები და გააუმჯობესა კანონმდებლობასთან შესაბამისობა. მაგრამ რთულია შეფასდეს, თუ რა გავლენა იქონია ამ შემთხვევამ სხვა ორგანიზაციებზე, გაითვალისწინეს თუ არა მათ "23andMe"-ის მიერ მიღებული გაკვეთილები და იქცა თუ არა დაკისრებული ჯარიმა შემაკავებელ ფაქტორად. სწორედ ამის გათვალისწინებით უნდა განვიხილოთ "Pathetic Dot" მოდელის დანარჩენი სამი მოდალობა და ის, თუ როგორ შეუძლიათ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უწყებებს მათი გამოყენება ქცევის რეგულირებისთვის საერთაშორისო თანამშრომლობის გზით.

ამის საჩვენებლად წინამდებარე ნაშრომში განხილული იქნება გერნზის მონაცემთა დაცვის საზედამხედველო ორგანოს სამსახურის[32] ("ODPA") მიერ საერთაშორისო თანამშრომლობის გამოყენების ორი მაგალითი. როგორც მსოფლიოში ერთ-ერთი ყველაზე მცირე მონაცემთა დაცვის საზედამხედველო ორგანო[33], ის საერთაშორისო თანამშრომლობას განიხილავს როგორც მოქმედების დამატებითი შესაძლებლობების მოსაპოვებლად, ისე საკუთარი ქმედებების გავლენის გასაზრდელად. როგორც საერთაშორისო ფინანსური ცენტრი, გერნზის ბეილივიკი[34] უკვე საკუთარ შესაძლებლობებზე მეტს აღწევს და მონაცემთა დაცვის მყარი რეჟიმი ამ პოზიციის გამყარებას შეუწყობს ხელს. გარდა ამისა, რადგან ტექნოლოგია გეოგრაფიულ საზღვრებს არ ცნობს, ბეილივიკის მოქალაქეები იმავე მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის პრობლემების წინაშე დგანან, როგორც ბევრად უფრო დიდი იურისდიქციები, და იმსახურებენ მარეგულირებელს, რომელიც შეძლებს მათ წარდგენას საერთაშორისო ასპარეზზე და ამავდროულად შექმნის ღირებულებასა და სარგებელს ადგილობრივ დონეზე.

2024 წელს "ODPA" გახდა მონაცემთა „სკრაპინგისა" და პირადი ცხოვრების ხელშეუხებლობის დაცვის[35] შესახებ ერთობლივი განცხადების ხელმომწერი, რომელიც "GPA"-ს "IEWG"-ის ინიციატივა იყო. ეს ერთობლივი განცხადება, რომელსაც მონაცემთა დაცვის 14-მა საერთაშორისო საზედამხედველო ორგანომ დაუჭირა მხარი, ასახავდა მონაცემთა „სკრაპინგით" გამოწვეულ პირადი ცხოვრების ხელშეუხებლობის რისკებს, იმას, თუ როგორ შეეძლოთ სოციალური მედიის კომპანიებსა და სხვა ვებსაიტების ოპერატორებს მომხმარებელთა მონაცემების დაცვა და რა ქმედებების განხორციელება შეეძლოთ ფიზიკურ პირებს საკუთარი თავის დასაცავად. როგორც ბეილივიკის კომისარმა, *ბრენტ ჰომანმა,* განაცხადა: „მონაცემთა „სკრაპინგი" გლობალურ რისკს წარმოადგენს, რომელიც გლობალურ რეაგირებას ჩვენს საერთაშორისო პარტნიორ მონაცემთა დაცვის უწყებებთან ძალების გაერთიანებით, ჩვენ

[32] ოფიციალურად ცნობილია მონაცემთა დაცვის (გერნსის ბეილივიკის) 2017 წლის კანონში, როგორც მონაცემთა დაცვის ორგანო

[33] წერის მომენტისთვის — 14 თანამშრომელი.

[34] გერნზის ბეილივიკი მოიცავს კუნძულებს: გერნზის, ოლდერნის, სარკსა და ჰერმს, და მდებარეობს ლა-მანშის სრუტეში. როგორც ბრიტანეთის გვირგვინის დამოკიდებული ტერიტორია, ის წარმოადგენს თვითმმართველ იურისდიქციას, რომელიც ბრიტანეთის გვირგვინისადმი ერთგულებას ინარჩუნებს.

[35] ODPA 'ODPA joins international efforts to prevent unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=5a294e41-9eea-ee11-a204-6045bd8c5a56>.

ვადგენთ ძირითად გლობალურ მოლოდინებს სოციალური მედიის კომპანიების მიმართ, რათა უზრუნველყონ არაავტორიზებული სკრაპინგის წინააღმდეგ ბრძოლის შესაბამისი გარანტიები“[36].

2023 წლის აგვისტოში ერთობლივი განცხადების გამოქვეყნების შემდეგ ხელმომწერები წამყვან სოციალური მედიის კომპანიებთან ჩაერთნენ დიალოგში, რათა გაეგოთ, რა ტექნიკური გამოწვევების წინაშე იდგნენ ისინი უკანონო მონაცემთა „სკრაპინგთან“ ბრძოლაში და რა ქმედებებს ახორციელებდნენ. ვირტუალურმა შეხვედრებმა “ODPA”-ს საშუალება მისცა, პირდაპირ დაესვა კითხვები ამ კომპანიებისთვის, რაც თითქმის შეუძლებელი იქნებოდა ამ ინიციატივაში ჩართული სხვა მარეგულირებლების გაერთიანებული ძალისხმევის გარეშე. ხელმომწერები ასევე შეხვდნენ არაავტორიზებული სკრაპინგის შემცირების ალიანსის[37] (“MUSA”) წარმომადგენლებს — ორგანო, რომელიც აერთიანებს „ინდუსტრიის ლიდერებს მონაცემების არაავტორიზებული მოპოვებისა და ბოროტად გამოყენებისგან დასაცავად“[38].

ამ მნიშვნელოვან შეხვედრებზე მიღებული ინფორმაცია საფუძვლად დაედო შემაჯამებელი ერთობლივი განცხადების გამოქვეყნებას, რომელშიც ჩამოყალიბდა დამატებითი მოლოდინები. მათ შორის: ხელოვნური ინტელექტის დიდი ენობრივი მოდელების ტრენინგისას გათვალისწინებული უნდა იყოს მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობა; უკანონო „სკრაპინგის“ წინააღმდეგ მიმართული დაცვის ზომები რეგულარულად უნდა გადაიხედოს ტექნოლოგიურ პროგრესთან შესაბამისობის შესანარჩუნებლად; და მონაცემთა „სკრაპინგი“, რომელიც დასაშვებია კომერციული ან საზოგადოებრივად სასარგებლო მიზნებისთვის, კანონიერად უნდა განხორციელდეს[39].

ამ ინიციატივის “Pathetic Dot” მოდელის ჭრილში განხილვისას მოქმედებს კანონის მოდალობა, რადგან ერთობლივ განცხადებებში ჩამოყალიბებული მოლოდინების საფუძველი იყო ორგანიზაციებზე დაკისრებული სამართლებრივი ვალდებულებები პერსონალურ მონაცემთა დამუშავებისას. თუმცა ეს არ იყო ერთადერთი მოქმედი მოდალობა. წამყვან სოციალური მედიის კომპანიებთან ურთიერთობით, ხელმომწერი მხარეები ბაზარს სთხოვდნენ, თავად მოეხდინა ზეწოლა სუბიექტებზე, რათა მათ მისაღები ქცევის ნორმები დაეცვათ.

იქნება ეს კანონშესაბამისი პრაქტიკის კონკურენტულ უპირატესობად გამოყენება, კონფიდენციალურობაზე ორიენტირებული პირებისთვის მიმართვა თუ მავნე პრაქტიკის მხილება, იმის უზრუნველყოფა, რომ ბაზარმა ან ინდუსტრიამ კარიბჭის მცველის როლი შეასრულოს, შეიძლება იყოს

[36] იქვე.
[37] MUSA <https://antiscrapingalliance.org/>.
[38] იქვე.
[39] ODPA ‘Guernsey joins global partners to combat unlawful data scraping’ <https://www.odpa.gg/news/news-article/?id=f5ed30b6-3595-ef11-8a69-6045bdf2d3b5>.

დამატებითი ბიძგი, რომელიც გამონაკლის სუბიექტებს სჭირდებათ. ბაზრის ამ ბერკეტის გამოყენება კიდევ უფრო ნათლად გამოჩნდა "MUSA"-სთან თანამშრომლობით. ეს ორგანიზაცია უკვე არსებობდა და ცდილობდა კარგი პრაქტიკის ხელშეწყობას საზოგადოებრივი ცნობიერების ამაღლებასთან ერთად. "MUSA"-სთვის სასარგებლო იყო მარეგულირებლებთან თანამშრომლობის დემონსტრირება, მაგრამ, თავის მხრივ, ეს მარეგულირებლებისთვის იყო კიდევ ერთი შესაძლებლობა, აემოქმედებინათ ბაზრის მოდალობა, რაც სარგებელს მოუტანდა როგორც ფიზიკურ პირებს, ისე კანონმორჩილ კომპანიებს.

ბაზრის მოდალობის გამოყენების გარდა, პრესრელიზებისა და საჯარო გამოსვლების მეშვეობით, "ODPA"-მ შეძლო სოციალური ნორმების მოდალობის ამოქმედებაც. ამან მას საშუალება მისცა, საზოგადოებისთვის მიეწოდებინა ინფორმაცია იმის შესახებ, თუ როგორ შეიძლებოდა მათი პერსონალური მონაცემების გამოყენება ისე, როგორც ამას არ ელოდნენ და არ ისურვებდნენ. ეს აძლევს მათ შესაძლებლობას, თავად გადადგან ნაბიჯები საკუთარი თავის დასაცავად, იქნება ეს ვებპლატფორმებისთვის გაზიარებული მონაცემების შეზღუდვა თუ არჩევნის გაკეთება იმის მიხედვით, თუ რამდენად პასუხისმგებლიანია ოპერატორი. იმ იდეის უარყოფით, რომ „ყოველთვის ასე იყო და ვერაფერს შევცვლი", გარე კომუნიკაციებს შეუძლია საზოგადოების გააქტიურება, რათა შეცვალონ სოციალური ნორმა და ამგვარად მოახდინონ ზეწოლა რეგულირებად სუბიექტებზე.

არაოფიციალური მონაცემებით, "ODPA"-ს პრესრელიზების შემდეგ მონაცემთა სკრაპინგი საუბრის თემად იქცა როგორც რიგით მოქალაქეებს შორის, ისე სამმართველო დონეზე, რაც აჩვენებს, რომ სხვა მოდალობების გამოყენებას შეუძლია გზავნილის გავრცელება და ნარატივზე გავლენის მოხდენა.

საერთაშორისო თანამშრომლობის ძალის კიდევ ერთი მაგალითი იყო 2024 წლის "GPEN"-ის „შემოწმება[40]". თემა ეხებოდა შეცდომაში შემყვანი დიზაინის პრაქტიკას, ანუ „ბნელ პატერნებს" — ვებსაიტისა და აპლიკაციის დიზაინის იმ ასპექტებს, რომლებიც მომხმარებელს უბიძგებს პირადი ცხოვრების ხელშეუხებლობისთვის ყველაზე ნაკლებად ხელსაყრელი ვარიანტისკენ, კომპანიის სასარგებლოდ და ფიზიკური პირის საზიანოდ. შემოწმების ფარგლებში "GPEN"-მა ძალები გააერთიანა მომხმარებელთა უფლებების დაცვის აღსრულების საერთაშორისო ქსელთან[41], მის კოლეგა ორგანიზაციასთან მომხმარებელთა დაცვის სფეროში, რათა ვებსაიტებსა და აპლიკაციებში „ბნელი პატერნების" ინდიკატორები გამოევლინათ.

ამ ინიციატივის ფარგლებში ათასზე მეტი ვებსაიტი და აპლიკაცია „შემოწმდა" 26 პირადი ცხოვრების ხელშეუხებლობის დაცვის აღსრულების უწყებისა და 27 "ICPEN"-ის წევრი უწყების მიერ, რამაც ეს „შემოწმება"

[40] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>
[41] ICPEN <https://www.icpen.org/>.

„დღეისათვის, პირადი ცხოვრების ხელშეუხებლობისა და მომხმარებელთა დაცვის უწყებებს შორის უწყებათაშორისი თანამშრომლობის ყველაზე ვრცელ მაგალითად“ აქცია[42]. საერთო ჯამში, განხილული ვებსაიტებისა და აპლიკაციების 97%-ში შეცდომაში შემყვანი დიზაინის პატერნების სულ მცირე ერთი ინდიკატორი გამოვლინდა[43].

გერნზის ბეილივიკში ერთ-ერთი წამყვანი ინდუსტრია ონლაინ აზარტული თამაშებია. ამ სექტორს ოლდერნის აზარტული თამაშების კონტროლის კომისია[44] (“AGCC”) არეგულირებს. აზარტულ თამაშებზე დამოკიდებულების გავრცელებისა და ონლაინ აზარტული თამაშების ვებსაიტებისა და აპლიკაციების ზოგიერთი მომხმარებლის მოწყვლადობის გათვალისწინებით, “ODPA”-მ თავისი „შემოწმების“ ფარგლებში ყურადღება გაამახვილა “AGCC”-ის მიერ ლიცენზირებულ კომპანიებზე და შედეგებიც მას მიაწოდა. 2024 წლის თებერვლის დასაწყისში 19 კომპანია „შემოწმდა“ და თითოეულ მათგანში შეცდომაში შემყვანი დიზაინის პრაქტიკის სულ მცირე ერთი ინდიკატორი გამოვლინდა, განსაკუთრებული შეშფოთება კი დამუშავების გამჭვირვალობასთან დაკავშირებით დაფიქსირდა[45].

„შემოწმების“ შედეგად, “ODPA”-მ წერილობით მიმართა თითოეულ კომპანიას და გამოხატა თავისი შეშფოთება როგორც ზოგადად ინდუსტრიის, ისე კონკრეტულად მათი ვებსაიტებისა და აპლიკაციების მიმართ. სამ თვეზე ნაკლებ დროში “ODPA”-მ ამ კომპანიების 78%-ისგან მიიღო პრაქტიკის გაუმჯობესებისა და კონკრეტული პრობლემების მოგვარების შესახებ ვალდებულება[46]. ერთ-ერთ შემთხვევაში მონაცემთა დაცვის ოფიცერი მიესალმა “ODPA”-ს წერილს, რადგან ის იმეორებდა იმ შეშფოთებას, რომელიც მათ ადრე შიდა დონეზე ჰქონდათ გამოთქმული და “ODPA”-ს ჩარევა დაეხმარა მათ, მიეღწიათ სასურველი ცვლილებისთვის.

ბაზრისა და სოციალური ნორმების მოდალობების მოქმედების მაგალითად, 2024 წლის ბოლოსთვის ყველა კომპანიამ აიღო გაუმჯობესების ვალდებულება. ბოლო კომპანიამ თავისი ვალდებულება დაადასტურა ინდუსტრიის კონფერენციის შემდეგ, რომელზეც “ODPA”-ს კომისარმა მადლიერება გამოხატა იმ კომპანიების მიმართ, რომლებმაც უკვე აიღეს ცვლილებების ვალდებულება. ეს კომპანია მიხვდა, რომ არსებობდა რისკი, ინდუსტრიის კოლეგების მიერ ცუდ შუქზე წარმოჩენილიყო (ბაზრის მოდალობა) და რომ მომხმარებლები უკეთესს მოელოდნენ (სოციალური ნორმების მოდალობა). მიუხედავად იმისა, ეს პირადი ინტერესის საქმე იყო თუ

[42] Global Privacy Enforcement Network ‘GPEN Sweep 2024: “Deceptive Design Patterns” Report’ <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf>.

[43] იქვე.

[44] Alderney Gambling Control Commission <https://www.gamblingcontrol.org/>.

[45] ODPA ‘ODPA examines Bailiwick’s gambling sector for harmful privacy practices as part of global sweep’ <https://www.odpa.gg/news/news-article/?id=baea8752-d03d-ef11-8409-7c1e5226329b>.

[46] ODPA ‘Bailiwick’s gambling sector pledges to make improvements after ODPA shares concerns of harmful privacy practices’ <https://www.odpa.gg/news/news-article/?id=cd258672-9f79-ef11-a670-6045bd97f872>.

გაუმჯობესების გულწრფელი სურვილი, საბოლოო შედეგი იყო გასაოცარი — 100%-იანი ვალდებულება გაუმჯობესების შესახებ. ამ შედეგის მიღწევას მრავალი წელი დასჭირდებოდა, ეს საკითხი გამოძიებების გზით რომ გადაჭრილიყო.

რაც შეეხება მეოთხე მოდალობას — არქიტექტურას, ტექნოლოგია სწრაფად ვითარდება და ინოვაციების დანერგვასთან ერთად საკუთარ ქცევით შეზღუდვებსაც აწესებს. რაც უფრო ნათელია მარეგულირებლების მოლოდინები და რაც უფრო თანმიმდევრულია ეს მოლოდინები გლობალურად, მით უფრო მეტად შეუძლიათ დეველოპერებს ამ მოლოდინების საკუთარ პროდუქტებში ინტეგრირება. "GDPR"-ის ძალაში შესვლამდე პერიოდში ორგანიზაციების ელექტრონული ფოსტა სავსე იყო რეგულაციისთვის განკუთვნილი ტექნიკური გადაწყვეტილებების რეკლამებით. ზოგიერთი მათგანი უფრო ლეგიტიმური იყო, ვიდრე სხვები, მაგრამ ეს აჩვენებს, რომ ანგარიშვალდებულებასა და ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინებაზე გაკეთებულმა აქცენტმა ტექნოლოგიური განვითარება განაპირობა.

ისეთი აქტივობები, როგორიცაა "GPEN"-ის „შემოწმება" ან მონაცემთა „სკრაპინგის" შესახებ ერთობლივი განცხადებები, აყალიბებს მოლოდინებსა და მოთხოვნებს. დეველოპერების მზაობა, შექმნან გადაწყვეტილებები საერთო პრობლემებისთვის, რომელთა გაყიდვასაც ისინი შეძლებენ, როგორც მარეგულირებლების მოლოდინებზე პასუხს, იწვევს იმას, რომ არქიტექტურის მოდალობა საკუთარ ზეწოლას ახდენს "Pathetic Dot" მოდელზე. მარეგულირებლების თანამშრომლობას შეუძლია გლობალური ტექნიკური პრობლემების გლობალური ტექნიკური გადაწყვეტილებების მიღება.

5. დასკვნა

ლოურენს ლესიგის "Pathetic Dot" მოდელი აჩვენებს, რომ, მიუხედავად იმისა, რომ მონაცემთა დაცვა და პირადი ცხოვრების ხელშეუხებლობა სამართლებრივი კონსტრუქციებია, რეალურად, რეგულირებადი სუბიექტის ან წერტილის ქცევას მხოლოდ კანონი არ არეგულირებს. ზეწოლის, შეზღუდვებისა და სტიმულის გამოყენება თანაბრად ეფექტიანად შეიძლება სოციალური ნორმის, ბაზრისა და არქიტექტურის მეშვეობით, რომლებთანაც სუბიექტი ურთიერთქმედებს და ამ ოთხი მოდალობის გამოყენება შესაძლებელია გაუმჯობესების მისაღწევად ყველა დაინტერესებული მხარის სასარგებლოდ.

მნიშვნელოვანია, რომ, მიუხედავად იმისა, რომ ამის მიღწევა მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის მარეგულირებლებს დამოუკიდებლადაც შეუძლიათ. საერთაშორისო თანამშრომლობას შეუძლია გააძლიეროს აღნიშნული მოდალობები და გადაჭრას განსხვავებული

საკანონმდებლო მექანიზმებით გამოწვეული პრობლემები. წინამდებარე ნაშრომი ასევე აჩვენებს, რომ დადებითი ცვლილებების მისაღწევად საერთაშორისო თანამშრომლობას არ სჭირდება რესურსების ინტენსიურ გამოყენებასთან დაკავშირებული ერთობლივი გამოძიებების ფორმა ჰქონდეს. მსოფლიოს სხვადასხვა ქვეყნის მარეგულირებლების მიერ შემუშავებულ ერთიან, თანმიმდევრულ პოზიციას შეიძლება სუბიექტზე იგივე, თუ არა მეტი, გავლენა ჰქონდეს, როგორც კონკურენტისთვის დაკისრებულ დიდ ჯარიმას.

საერთაშორისო თანამშრომლობა მარეგულირებლის არსენალში ფასდაუდებელი ინსტრუმენტია. მიუხედავად იმისა, მარეგულირებელი დიდი იქნება თუ პატარა, საქმიანობის მრავალწლიანი გამოცდილებით თუ ახალბედა, საერთაშორისო თანამშრომლობას შეუძლია, გაზარდოს მისი შესაძლებლობები და გააძლიეროს გავლენა.

ბიბლიოგრაფია:

1. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალური მონაცემების დამუშავებასთან დაკავშირებით ფიზიკური პირების დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების შესახებ [2016] OJ L119.
2. ევროპის საბჭო, კონვენცია ფიზიკური პირების დაცვის შესახებ პერსონალური მონაცემების ავტომატურ დამუშავებასთან დაკავშირებით, ETS 108 (ხელმოსაწერად გახსნილია 1981 წლის 28 იანვარს).
3. კლიმატის ცვლილების შესახებ გაეროს ჩარჩო კონვენციის პარიზის შეთანხმება, მიღებული 2015 წლის 12 დეკემბერს, T.I.A.S. No. 16-1104.
4. კლიმატის ცვლილების აქტი 2008 (c. 27).
5. OECD, Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352.
6. *Lessig L.,* Code and the Other Laws of Cyberspace, Basic Books 1999.
7. *Lessig L., Code* Version 2.0, Basic Books 2006.
8. Alderney Gambling Control Commission <https://www.gamblingcontrol.org/>.
9. BBC News ‘GDPR: Are you ready for the EU’s huge data privacy shake-up?’ <https://www.bbc.co.uk/news/technology-43657546n>.
10. Council of Europe ‘Chart of signatures and ratifications of Treaty 108’ <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.
11. Global Privacy Assembly <https://globalprivacyassembly.org/>.
12. Global Privacy Assembly ‘An Enforcement Cooperation Handbook’ <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.

13. Global Privacy Assembly 'History of the Assembly' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.
14. Global Privacy Assembly 'International Enforcement Cooperation Working Group Report - July 2024' <https://globalprivacyassembly.org/wp-content/uploads/2024/11/9.-IEWG-GPA-Annual-Report-2024.pdf>.
15. Global Privacy Assembly 'Mission and Vision' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/>.
16. Global Privacy Assembly 'Strategic Plan 2023 - 2025' <https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf>.
17. Global Privacy Assembly 'Working Group Reports' <https://globalprivacyassembly.org/document-archive/working-group-reports/>.
18. Global Privacy Enforcement Network <https://privacyenforcement.net/content/home-public>.
19. Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.
20. Global Privacy Enforcement Network 'Action Plan for the Global Privacy Enforcement Network (GPEN)' <https://privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>.
21. Global Privacy Enforcement Network 'GPEN Sweep 2024: "Deceptive Design Patterns" Report' <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf>.
22. ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>
23. ICPEN <https://www.icpen.org/>.
24. MUSA <https://antiscrapingalliance.org/>.
25. ODPA 'Bailiwick's gambling sector pledges to make improvements after ODPA shares concerns of harmful privacy practices' <https://www.odpa.gg/news/news-article/?id=cd258672-9f79-ef11-a670-6045bd97f872>.
26. ODPA 'Blog: Dark patterns and the gambling industry' <https://www.odpa.gg/news/news-article/?id=dccb80cb-3156-ef11-bfe3-000d3a2d37f7>.
27. ODPA 'Guernsey joins global partners to combat unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=f5ed30b6-3595-ef11-8a69-6045bdf2d3b5>.

28. ODPA 'ODPA examines Bailiwick's gambling sector for harmful privacy practices as part of global sweep' <https://www.odpa.gg/news/news-article/?id=baea8752-d03d-ef11-8409-7c1e5226329b>.
29. ODPA 'ODPA joins international efforts to prevent unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=5a294e41-9eea-ee11-a204-6045bd8c5a56>
30. Office of the Privacy Commissioner of Canada, 'Concluding joint statement on data scraping and the protection of privacy' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2024/js-dc_20241028/>.
31. Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.
32. Office of the Privacy Commissioner of Canada, 'Joint statement on data scraping and the protection of privacy' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/js-dc_20230824/>.
33. UN Trade & Development, 'Data Protection and Privacy Legislation Worldwide' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

ჯოვანი მარია რიჩიო*

ბრიუსელის ეფექტი, პერსონალურ მონაცემთა დაცვა და ხელოვნური ინტელექტის შესახებ აქტი

წინამდებარე სტატია იკვლევს შედარებითი სამართლის როლს ახალი ტექნოლოგიებიდან გამომდინარე სამართლებრივი გამოწვევების გააზრებისა და მათზე რეაგირების პროცესში. სტატიაში განხილულია შემდეგი საკითხები: მიზეზები, თუ რატომ ადგენს ევროკავშირი გლობალურ მარეგულირებელ სტანდარტებს, რაც ილუსტრირებულია "GDPR"-ის მაგალითით; ამერიკის შეერთებული შტატების ინოვაციური პოტენციალის განმაპირობებელი ფაქტორები და ევროკავშირის სამართლებრივი მოდელის სამომავლო გავრცელების პერსპექტივა.

საკვანძო სიტყვები: *პერსონალურ მონაცემთა დაცვა, ევროკავშირი, "GDPR", მარეგულირებელი სამართალი, კერძო სამართალი, ხელოვნური ინტელექტის აქტი, ბრიუსელის ეფექტი, სამართლებრივი ფრაგმენტაცია, ნეოლიბერალიზმი, ციფრული ბაზრები, ჩინური ტექნოლოგიური კომპანიები, შესაბამისობის სირთულეები.*

1. შედარებითი სამართლის სარგებლიანობა ახალი ტექნოლოგიების შესწავლაში

ხელოვნური ინტელექტის თემის შედარებითსამართლებრივი პერსპექტივიდან განხილვა მარტივი ამოცანა არ არის. ეს, პირველ რიგში, მკითხველში არარეალისტური მოლოდინების თავიდან აცილების მიზნით, ანალიზის მასშტაბის დაზუსტებას მოითხოვს. მათ, ვინც ეძებს დეტალურ ინფორმაციას სხვადასხვა სამართლებრივი სისტემის კონკრეტული რეგულაციების შესახებ, ვურჩევთ, შეწყვიტონ კითხვა და უფრო სასარგებლო საქმიანობით დაკავდნენ.

*იურიდიული ფირმა e-Lex-ის (რომი) დამფუძნებელი და უფროსი პარტნიორი; შედარებითი სამართლის სრული პროფესორი; სალერნოს უნივერსიტეტის მონაცემთა დაცვის ოფიცერი ("DPO"). მიმდინარე სასწავლო კურსები: საავტორო სამართალი, კულტურული მემკვიდრეობის სამართალი, ხელოვნების სამართალი.

რასაკვირველია, საყოველთაოდ უნდა იყოს ცნობილი, თუმცა ამის გამეორება მაინც ღირს, რომ შედარებითი სამართალი არსებითად მეთოდია, მიუხედავად იმისა, რომ შედარებითსამართლებრივი კვლევების მეთოდებსა და ფუნქციებზე სამეცნიერო დებატების ინტენსივობა, როგორც ჩანს, იკლებს[1]. თუმცა ჩვენ შეგვიძლია დანამდვილებით ვთქვათ, თუ რა *არ* არის შედარებითი სამართალი: ის არ არის უცხოური სამართლებრივი სისტემების თავისთავად შესწავლა, არც მხოლოდ სამართლებრივი ინფორმაციის კრებული — იგი, უპირველეს ყოვლისა, შედარებაა.[2]

შედარებითი სამართალი, რა თქმა უნდა, ემსახურება ალტერნატიული გადაწყვეტების ძიებას, მაგრამ ის ასევე ღირებული ინსტრუმენტია შიდასახელმწიფოებრივი სამართლის ჩვენეული გაგების გასაღრმავებლად. იგი არ შემოიფარგლება მხოლოდ საკანონმდებლო ტექსტების ანალიზით, არამედ მიისწრაფვის სამართლებრივი ფორმალიზმის ფარგლებს გასცდეს. უკანასკნელ ათწლეულებში ამ ფორმანტების იდენტიფიცირებაც კი — ან, უფრო ზუსტად, მათი საზღვრების მოხაზვა — სულ უფრო რთული გახდა. მაგალითად, განვიხილოთ საკანონმდებლო ფორმატი, რომელშიც ეროვნული კანონმდებლობა, ზენაციონალური სამართალი და დამოუკიდებელი ადმინისტრაციული ორგანოების მიერ გამოცემული გადაწყვეტილებები და ზომები ახლა ერთდროულად არსებობს და ურთიერთქმედებს.

უკვე ათწლეულებია, რაც პოლიცენტრული სამართლის აღზევების მოწმენი ვართ, რაც სამართლებრივი ნორმების შექმნაზე სახელმწიფოს მონოპოლიის ეროზიის შედეგია[3]. ეს ეკონომიკური გლობალიზაციის პროდუქტია, რომლის მიხედვითაც ეროვნულ საკანონმდებლო სუვერენიტეტს უწევს თანაარსებობა სამართლებრივი ნორმების შექმნის ახალ ცენტრებთან, მათ შორის, საერთაშორისო ეკონომიკურ და პროფესიულ საზოგადოებებთან[4]. ზოგჯერ ეს სამართალი ზემოდან არ არის თავსმოხვეული, არამედ სპონტანურად ჩნდება საერთაშორისო კომერციული პრაქტიკიდან; სხვა შემთხვევაში, ეს არის სახელმწიფო სამართალი, რომელიც გამდიდრებულია

[1] იხ.: *Stanzione P.*, Sui metodi del diritto comparato, Introduzione a *Ancel M.,* Utilità e metodi del diritto comparato, trad. it., Camerino, 1974, XXIII, ასევე, ფრანგულ ენაზე: Rev. *int. droit comparé*, 1973, 885; L.-J. Costantinesco, Il metodo comparativo, ed. it., Torino, 2000.

[2] According to *Sacco R.*, Circolazione e mutazione dei modelli giuridici, in Dig disc. priv., sez. civ., II, Torino, 1988, 365, შედარებითი სამართალი მხოლოდ უცხოური სამართლებრივი სისტემების ანალიზი რომ ყოფილიყო, მისი ფუნქცია აღწერითი საქმიანობით შემოიფარგლებოდა და რეალურ გავლენას ვერ მოახდენდა შიდასახელმწიფოებრივი სამართლის გააზრებასა და განვითარებაზე. ამის საპირისპიროდ, შედარებითი სამართალი გვთავაზობს საკუთარი სამართლებრივი სისტემის კრიტიკულად შესწავლის მეთოდს, რომელიც ალტერნატიულ სამართლებრივ მოდელებთან შედარებით ავლენს არა მხოლოდ მის განმასხვავებელ ნიშნებს, არამედ პოტენციურ ხარვეზებსა თუ არაეფექტიანობას. (*Sacco R.*, Introduzione al diritto comparato, in Tratt. dir. comp. dir., da R. Sacco, 5ª ed., Torino, 1992).

[3] Cf. *Ferrajoli L.*, Crisi del diritto e dei diritti nell'età della globalizzazione, in Questione Giustizia, 2023, <https://www.questionegiustizia.it/articolo/crisi-del-diritto-e-dei-diritti-nell-eta-della-globalizzazione>.

[4] ამ შემთხვევაშიც ბიბლიოგრაფია შეიძლება ვრცელი იყოს; თუმცა, მეთოდოლოგიური ანალიზისთვისაც იხილეთ: *Grossi P.*, Aspetti giuridici della globalizzazione economica, in I Georgofili. Atti della Accademia dei Georgofili, 2013.

კერძო წესების მარეგულირებელი შინაარსით — როგორც ეს ხდება ხელოვნური ინტელექტის აქტში ჰარმონიზებულ სტანდარტებზე მითითების შემთხვევაში[5].

საკმარისია აღინიშნოს, რომ ინოვაციების მარეგულირებელი სამართლებრივი ნორმების უმეტესობა დღეს ევროკავშირიდან მომდინარეობს, მათ შორის, ხელოვნურ ინტელექტთან დაკავშირებული ნორმები. კავშირის დონეზე შეინიშნება აშკარა გადასვლა დირექტივებიდან რეგულაციებზე, რაც სამართლებრივი ჰარმონიზაციიდან უნიფიკაციაზე გადასვლას მიანიშნებს. ეს არჩევანი, სხვა ფაქტორებთან ერთად, ასახავს ზოგიერთი ეროვნული სამართლებრივი სისტემის სურვილს, შეინარჩუნოს საკუთარი საკანონმდებლო სუვერენიტეტი — ხშირად პოლიტიკური ან ლობისტური ზეწოლის საპასუხოდ, რაც საფრთხის ქვეშ აყენებს ევროკავშირის მიერ ამ სფეროში დეკლარირებულ მიზანს: ბარიერებისგან თავისუფალი შიდა ბაზრის შექმნას, რომელიც ხელშეკრულებების ძირითად მიზნებს განახორციელებს.

მეტიც — და ეს კვლავაც საყოველთაოდ ცნობილია კომპარატივისტებისთვის — სამართლებრივი ფორმანტების ანალიზი აუცილებლად უნდა იყოს შერწყმული კრიპტოტიპების[6] ანალიზთან: იმ ელემენტების ერთობლიობასთან, რომლებიც დაკავშირებულია ხალხის სამართლებრივ ტრადიციასთან, ცოდნის გადაცემის გზებთან, სოციალურ და

[5]ჰარმონიზებული სტანდარტი, (ევროკავშირის) №1025/2012 რეგულაციის თანახმად, არის ტექნიკური სპეციფიკაცია, რომელიც მიღებულია ევროპული სტანდარტიზაციის ორგანოს მიერ (მაგალითად, CEN – სტანდარტიზაციის ევროპული კომიტეტი; "CENELEC" – ელექტროტექნიკური სტანდარტიზაციის ევროპული კომიტეტი; "ETSI" – ევროპის ტელეკომუნიკაციის სტანდარტების ინსტიტუტი) ევროკომისიის მოთხოვნის საფუძველზე. აღნიშნული სტანდარტები შემუშავებულია ევროკავშირის კანონმდებლობის იმპლემენტაციის ხელშეწყობისა და უფრო ეფექტიანი ერთიანი ბაზრის უზრუნველყოფის მიზნით. ჰარმონიზებული სტანდარტის შექმნის პროცესი რამდენიმე ეტაპს მოიცავს. პირველ რიგში, ევროკომისია გასცემს მანდატს, რომელიც განსაზღვრავს მარეგულირებელ საჭიროებას და ევროპული სტანდარტიზაციის ერთ-ერთ ორგანოს (CEN, CENELEC ან ETSI) ავალებს კონკრეტული სტანდარტის პროექტის შემუშავებას. აღნიშნული ორგანოები შეიმუშავებენ სტანდარტს ტექნიკური ექსპერტებისა და დაინტერესებული მხარეების ჩართულობით, რათა უზრუნველყონ მისი შესაბამისობა ბაზრის საჭიროებებთან და ევროკავშირის კანონმდებლობასთან. საბოლოოდ, სტანდარტი მიიღება და ქვეყნდება ევროკავშირის ოფიციალურ ჟურნალში. თუმცა პრეამბულის 117-ე პარაგრაფი აწესებს დამატებით მოთხოვნას, რომლის თანახმადაც, ჰარმონიზებული სტანდარტი „ხელოვნური ინტელექტის ოფისის" მიერ მიჩნეულ უნდა იქნას ვარგისად შესაბამისი ვალდებულებების დასარეგულირებლად.

[6] კრიპტოტიპები, შედარებით სამართალში, არის სამართლებრივი სისტემის ის იმპლიციტური ელემენტები, რომლებიც პირდაპირ გამოხატულებას არ პოულობენ სამართლის ფორმალურ წყაროებში (კანონმდებლობა, სასამართლო პრაქტიკა და დოქტრინა), მაგრამ ღრმა გავლენას ახდენენ ნორმების ფუნქციონირებასა და გამოყენებაზე. ისინი მოიცავენ კულტურულ ღირებულებებს, დამკვიდრებულ პრაქტიკებს, სამართლებრივ მენტალიტეტსა და დაუწერელ პრინციპებს, რომლებიც განსაზღვრავენ, თუ როგორ ხდება სამართლის განმარტება და გამოყენება კონკრეტულ საზოგადოებაში. კრიპტოტიპების კონცეფცია შეიმუშავა *როდოლფო საკომ*, რომელმაც ხაზი გაუსვა, რომ ექსპლიციტური ფორმანტების პარალელურად, არსებობს ეს ლატენტური ელემენტები, რომლებიც აყალიბებენ კონკრეტული სამართლებრივი წესრიგის სამართალს. ისინი განსაკუთრებით რელევანტურია სხვადასხვა ტრადიციის მქონე სამართლებრივი სისტემების ანალიზისას, რადგან შესაძლებელს ხდიან რეალური სამართლებრივი დინამიკის გააზრებას ნორმატიული მონაცემების მიღმა.

კულტურულ კონტექსტთან და ეკონომიკურ გარემოსთან, და რომლებიც აყალიბებენ იურისტების მომზადებასა და მსოფლმხედველობას. ეს განსაკუთრებით მნიშვნელოვანი ხდება, როდესაც დასავლური სამართლებრივი ტრადიციის ფარგლებს გავცდებით. როგორც ამას ხელოვნური ინტელექტის ტექნოლოგიების სამართლებრივი რეგულირება აუცილებლად მოითხოვს, ჩვენ მართლაც ხშირად ვხვდებით არადასავლურ სამართლებრივ სისტემებს, რომელთა იურისტები და პოლიტიკოსები ჩამოყალიბებულნი არიან ღირებულებათა განსხვავებული იერარქიით, ისეთით, რომელიც შეიძლება მნიშვნელოვნად განსხვავდებოდეს მათი დასავლელი კოლეგების ღირებულებებისგან.

არც ის უნდა გამოგვრჩეს, განსაკუთრებით ხელოვნური ინტელექტის სისტემების რეგულირების კონტექსტში, რომ ეთიკა სულ უფრო ცენტრალურ როლს ასრულებს. ეთიკამ უნდა წარმართოს ასეთი სისტემების დიზაინი, რათა თავიდან ავიცილოთ დისკრიმინაციული მიკერძოება ან ექსპლუატაცია, რომელიც ეწინააღმდეგება საერთაშორისო საზოგადოების საერთო ღირებულებებს. ამასთან დაკავშირებით მნიშვნელოვანია, აღინიშნოს, რომ ტერმინ „etica“-ს (ეთიკა) სემანტიკური არეალი რომანულ ენებში სრულად არ ემთხვევა „ethics“-ის უფრო ფართო ანგლო-ამერიკულ კონცეფციას: პირველ შემთხვევაში, ეთიკას უპირატესად სუბიექტური კონოტაცია აქვს და გამიჯნულია სამართლებრივი ნორმებისგან, რომლებიც ფორმალური კრიტერიუმებით განისაზღვრება; მეორე შემთხვევაში, ეთიკა უფრო ფართოა და ხშირად ჩართულია „რბილი სამართლის“ ფორმებში, როგორიცაა ეთიკის ან ქცევის კოდექსები.

შედარებითი სამართლის, როგორც მეთოდის, განსაზღვრა ნიშნავს იმის აღიარებას, რომ ის სცილდება უცხოური სამართლებრივი სისტემების შესახებ მონაცემთა უბრალო შეგროვებას[7]. ეს სამართლებრივი სფერო არ შემოიფარგლება მხოლოდ სხვადასხვა ქვეყნის წესების ჩამოთვლითა და ანალიზით, არამედ ფოკუსირებულია სხვადასხვა სამართლებრივ კონტექსტში მიღებული სტრუქტურების, პრინციპებისა და გადაწყვეტების იდენტიფიცირებაზე. წინამდებარე ნაშრომში ჩვენ მიზნად ვისახავთ, გამოვკვეთოთ ევროპული და აშშ-ის სისტემებისთვის დამახასიათებელი ზოგიერთი ძირითადი მახასიათებელი. ჩვენ განზრახ გვერდს ავუვლით იმ შეხედულებებს, რომლებიც შეიძლება აზიური სამართლებრივი სისტემების ანალიზიდან გამომდინარეობდეს. ყურადღებას არ გავამახვილებთ ცალკეულ სამართლებრივ ინსტიტუტებზე, არამედ შევეცდებით, გამოვავლინოთ ის გაბატონებული ელემენტები, რომლებიც სამართლებრივი პოლიტიკის არჩევანს უდევს საფუძვლად.

ეს მიდგომა გამომდინარეობს იმის გაცნობიერებიდან, რომ ბოლო ოცდაათი წლის განმავლობაში სამართლებრივმა სისტემებმა ღრმა

[7] *Gorla G.*, Diritto comparato, in Enc. dir., XII, Milano, 1964, 930; *Ascarelli T.*, Premesse allo studio del diritto comparato, in Studi di diritto comparato e in tema di interpretazione, Milano, 1952, 6 ss.

ტრანსფორმაცია განიცადა. სახელმწიფოებს შორის მზარდი ურთიერთდაკავშირების ეპოქაში შედარებითი სამართალი სულ უფრო მნიშვნელოვან როლს ასრულებს, რადგან სამართლებრივი სისტემები იზოლირებულად აღარ არსებობენ და მუდმივად ურთიერთქმედებენ საერთაშორისო ხელშეკრულებების, ზენაციონალური ინსტიტუტებისა და სამართლის რეცეფციისა და ჰარმონიზაციის პროცესების მეშვეობით[8].

დაბოლოს, შედარებითი მიდგომა მოითხოვს ფორმალიზმზე უარის თქმას და მხოლოდ კანონმდებლობის ანალიზის ფარგლებს გასვლას. იგი მოითხოვს მრავალი ფაქტორის გათვალისწინებას, რომლებიც გავლენას ახდენენ სამართლის შექმნასა და გამოყენებაზე, მათ შორის, არასამართლებრივი მიზეზების, სხვადასხვა სამართლებრივ ფორმანტს შორის ურთიერთქმედებისა და მათი ურთიერთგავლენის გათვალისწინებას. ამ მიზეზით, როგორც უკვე აღინიშნა, ჩვენ ყურადღებას გავამახვილებთ ხელოვნური ინტელექტის სფეროში მიღებული სხვადასხვა მარეგულირებელი მიდგომის უკან მდგარი პოლიტიკური (და, შესაბამისად, სამართლებრივი) საფუძვლების შედარებაზე.

2. რატომ ქმნის ევროკავშირი წესებს: “GDPR”-ის მაგალითი

მასმედიის რიტორიკაში დამკვიდრდა გავრცელებული ნარატივი — უაღრესად რედუქციული და ემპირიულ მტკიცებულებებს მოკლებული — რომლის თანახმადაც, ამერიკის შეერთებული შტატები ქმნის ინოვაციებს, ჩინეთი „აკოპირებს“, ევროკავშირი კი არეგულირებს. გარდა იმისა, რომ ეს მტკიცება ზედმეტად გამარტივებულია, იგი უფრო დეტალურ განხილვას იმსახურებს, რათა გავიგოთ ასეთი კლასიფიკაციის მიზეზები.

დავიწყოთ ბოლოდან, ანუ იმ იდეიდან, რომ ევროპა ნაკლებ ინვესტიციას დებს ინოვაციებში, მაგრამ წარმატებულია სამართლებრივი ნორმების შექმნაში.

ეს ვარაუდი შეცდომაში შემყვანია პროცენტული თვალსაზრისით, მაგრამ, სამწუხაროდ, რეალისტურია აბსოლუტური მაჩვენებლებით. 2024 წლის დეკემბერში გამოქვეყნებული „ევროკავშირის სამრეწველო კვლევებსა და განვითარებაში ინვესტიციების შეფასების ანგარიშის“ უახლესი გამოცემის თანახმად, 2023 წელს ევროპულმა ინდუსტრიამ პირველად გადააჭარბა აშშ-ის (+5.9%) და ჩინური (+9.6%) კომპანიების ზრდას, 9.8%-იანი ზრდის ტემპით.

მიუხედავად იმისა, რომ ეს მაჩვენებელი იმედისმომცემია, ის არ ითვალისწინებს სამ მნიშვნელოვან ფაქტორს.

პირველი, ევროკავშირის წევრ ქვეყნებს შორის არსებული დიდი უთანასწორობა, სადაც უფრო მაღალი მაჩვენებლებია ისეთ განვითარებულ

[8] *Mattei U.*, Comparative Law and Economics, Univ. of Michigan Press, 1997; *Hoecke Van M.*, Epistemology and Methodology of Comparative Law, Hart Publishing, 2004; *Zeno-Zencovich V.,* Comparison Involves Pluralism*:* A Rejected View-Point, in Comparative Law Rev., 2025, 6.

ქვეყნებში, როგორიცაა: საფრანგეთი და გერმანია, ხოლო სხვები, მათ შორის იტალია, ჩამორჩებიან; მეორე, რომ ეს პროცენტული მაჩვენებლები სრულიად განსხვავებულ აბსოლუტურ მნიშვნელობებს ეფუძნება; და მესამე, რომ ევროპული ინვესტიციები ხშირად გადანაწილებულია მრავალ მცირე მასშტაბის პროექტზე, ნაცვლად იმისა, რომ კონცენტრირებული იყოს რამდენიმე სტრატეგიულ ინიციატივაზე. ამის კარგი მაგალითია პროგრამა „ჰორიზონტი 2020“, რომელმაც დააფინანსა უამრავი მცირე სამეწარმეო წამოწყება, რომელთაგან ყველა არ დასრულებულა სამრეწველო შედეგით.

შემდეგ დგება რეგულირების საკითხი, რომელიც ეფუძნება ეგრეთ წოდებული „ბრიუსელის ეფექტის“ კონცეფციას, რომელიც ახლა ფართოდ არის ცნობილი და შესაძლოა კარგავს აქტუალობას. ეს გულისხმობს ევროკავშირის უნარს, თავისი მარეგულირებელი გავლენა გაავრცელოს გეოგრაფიული და იურისდიქციული საზღვრების მიღმა, რითაც აყალიბებს ბიზნეს პრაქტიკას, ეროვნულ სამართლებრივ ჩარჩოებს და საერთაშორისო შეთანხმებებსაც კი.

„ბრიუსელის ეფექტის“[9] ცენტრალური საყრდენი ევროკავშირის სამართლის ექსტრატერიტორიული გამოყენებაა: რეგულაციები ვრცელდება არა მხოლოდ კავშირის შიგნით დაფუძნებულ სუბიექტებზე, არამედ მის ფარგლებს გარეთ არსებულ სუბიექტებზეც, რომლებიც საქონელს ან მომსახურებას სთავაზობენ ევროკავშირის ბაზარზე ან ამუშავებენ ევროკავშირის მოქალაქეების მონაცემებს. ყველაზე პარადიგმული მაგალითია მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”), რომელიც ვრცელდება ევროკავშირის ფარგლებს გარეთ მყოფ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებზე, როდესაც ისინი ამუშავებენ კავშირის ტერიტორიაზე მყოფი ფიზიკური პირების პერსონალურ მონაცემებს (“GDPR”-ის მე-3 მუხლი). ეს ბევრ არაევროკავშირის წევრ კომპანიას უქმნის საჭიროებას, თავისი მონაცემთა დამუშავების პრაქტიკა ევროკავშირის სტანდარტებს შეუსაბამოს. ასეთი ნორმატიული მოქმედების სფერო გამართლებულია როგორც

[9] ტერმინი ეკუთვნის *ა. ბრედფორდს* (A. Bradford), ნაშრომში „ბრიუსელის ეფექტი: როგორ მართავს ევროკავშირი სამყაროს“ (The Brussels Effect: How the European Union Rules the World, Oxford Univ. Press, 2020). ავტორი ამ მარეგულირებელი გავლენის მთავარ მიზეზად ევროპის შიდა ბაზრის მასშტაბსა და ძლიერ მარეგულირებელ პოტენციალს მიიჩნევს: ევროკავშირის ბაზარზე წვდომის მოსაპოვებლად, გლობალური კომპანიები ემორჩილებიან ევროპულ სტანდარტებს, რომლებსაც, საბოლოო ჯამში, სხვა ბაზრებზეც იყენებენ, რაც *de facto* ჰარმონიზაციის ეფექტს ქმნის. წიგნში ნაჩვენებია, თუ როგორ ხდება ეს სტრატეგიულ სექტორებში, როგორებიცაა პერსონალურ მონაცემთა დაცვა (“GDPR”), სურსათის უვნებლობა, კონკურენცია, გარემოს მდგრადობა და ფინანსები, და ქმნის ნარატივს, რომლის მიხედვითაც კავშირი მოქმედებს, როგორც „მარეგულირებელი ზესახელმწიფო“, რომელსაც, აშკარად გამოხატული იმპერიული ან იძულებითი სტრატეგიის არქონის მიუხედავად, შესწევს უნარი, დაადგინოს გლობალური თამაშის წესები. ანალიზი გამოირჩევა თავისი სამართლებრივ-ეკონომიკური მიდგომით, ამასთან, პოლიტიკური წაკითხვითაც, რომელიც ევროპის მარეგულირებელ ძალაუფლებას ინსტიტუციური რბილი ძალის ფორმად აღიარებს. ეს უკანასკნელი ემყარება ტექნოკრატიას, პროცედურულ გამჭვირვალობასა და ევროპული მარეგულირებელი მოდელის მიმზიდველობას. ამგვარად, ბრიუსელის ეფექტი წარმოჩინდება, როგორც უპირატესად ცალმხრივი პროცესი, რომელიც არა მრავალმხრივი მოლაპარაკებების, არამედ ევროკავშირის სტრუქტურული ძალაუფლებისა და გლობალური კომპანიების ეკონომიკური რაციონალურობის შედეგია.

საერთაშორისო სამართლის „შედეგების დოქტრინით“, ისე ევროკავშირის საბაზრო ძალით, რომლის მიხედვითაც შიდა ბაზარზე წვდომა მისი წესების დაცვას მოითხოვს.[10]

ფორმალური ექსტრატერიტორიულობის მიღმა, გლობალური კომპანიები ხშირად ნებაყოფლობით — ან უფრო ზუსტად, *de facto* — იღებენ ევროკავშირის სტანდარტებს მარეგულირებელი თანმიმდევრულობისა და ეკონომიკური ეფექტიანობის მიზნით. ხშირად უფრო მარტივია ერთიანი, მკაცრი სტანდარტის — როგორც წესი, ევროკავშირის სტანდარტის — დაცვა, ვიდრე თითოეული ბაზრისთვის შესაბამისობის ინდივიდუალურად მორგება. ეს განსაკუთრებით ეხება ისეთ სფეროებს, როგორებიცაა: გარემოს დაცვა, სურსათის უვნებლობა, პირადი ცხოვრების ხელშეუხებლობა და კონკურენციის სამართალი.

“GDPR” კვლავაც ნათელი მაგალითია: ტექნოლოგიურმა გიგანტებმა, როგორებიცაა: “Google”, “Apple” და “Microsoft”, გლობალურად დანერგეს “GDPR”-ის შთაგონებით შექმნილი მონაცემთა დაცვის პოლიტიკა იმ კონტექსტშიც კი, სადაც ამის ფორმალური ვალდებულება არ ჰქონდათ. ანალოგიურად, გარემოსდაცვით სფეროში იაპონურმა და აშშ-ის ავტომწარმოებლებმა გამონაბოლქვის სტანდარტები ევროკავშირის მოთხოვნებს შეუსაბამეს ბაზარზე წვდომის შესანარჩუნებლად და ხშირად ეს სტანდარტები გლობალურადაც გაავრცელეს[11].

„ბრიუსელის ეფექტის“ კიდევ ერთი ვექტორია მესამე ქვეყნების მიერ რეგულაციების გადმოღება, რომლებსაც არ აქვთ ამერიკის შეერთებული

[10] იქვე, შენიშვნა 9, 5: “the EU can unilaterally externalize its laws outside its borders through market mechanisms”.

[11] ბრიუსელის ეფექტი ვრცელდება საერთაშორისო დონეზეც როგორც მრავალმხრივ სავაჭრო შეთანხმებებში ევროპული სტანდარტების გავრცელებით, ისე ისეთი სუპრანაციონალური ორგანიზაციების მიერ მათი ტექნიკურ სტანდარტებად მიღებით, როგორებიცაა ISO (სტანდარტიზაციის საერთაშორისო ორგანიზაცია), *Codex Alimentarius*-ის კომისია ან ICAO (სამოქალაქო ავიაციის საერთაშორისო ორგანიზაცია). სავაჭრო შეთანხმებების კონტექსტში ევროკავშირი ხშირად რთავს მარეგულირებელ პუნქტებს, რომლებიც მოითხოვს ევროპული ან მისი ეკვივალენტური სტანდარტების მიღებას. ასეთია შემთხვევა ასოცირების ან თავისუფალი ვაჭრობის შესახებ შეთანხმებებისა (მაგ., CETA კანადასთან, EPA იაპონიასთან), რომლებიც შეიცავს დებულებებს გარემოს მდგრადობის, მონაცემთა დაცვისა და პროდუქტის უსაფრთხოების შესახებ. მსგავს შეთანხმებებში ევროკავშირი აწესებს მინიმალურ მოთხოვნებს, რითაც ხელს უწყობს თავისი სტანდარტების გავრცელებას მესამე ქვეყნებში. სამართლებრივი ჩარჩოს მიღმა, მნიშვნელოვანია ხაზი გაესვას, რომ ბრიუსელის ეფექტი არაფორმალურადაც ვლინდება ჰარმონიზებული წესებისა და ინდუსტრიული ნორმების განსაზღვრის გზით. მრავალი ევროპული ტექნიკური სტანდარტი, თავისი სიზუსტისა და პრაქტიკული სარგებლიანობის გამო, გლობალურ პრაქტიკად იქცევა. მრავალეროვნული კომპანიები მათ იმ რისკის თავიდან ასაცილებლად იღებენ, რომელიც სხვადასხვა ბაზრისთვის დიფერენცირებული პროდუქტების შექმნას უკავშირდება. ტექნიკური სტანდარტების გავრცელებას კიდევ უფრო შეიძლება შეუწყოს ხელი „რბილმა სამართალმა“ (“soft law”), ანუ არასავალდებულო ინსტრუმენტებმა (სახელმძღვანელო პრინციპები, რეკომენდაციები, ქცევის კოდექსები), რომლებიც შემუშავებულია ევროპული სააგენტოებისა თუ სტანდარტიზაციის ორგანოების მიერ. “GDPR”-ით (მუხლები 40-41) გათვალისწინებული ქცევის კოდექსების მაგალითი, მიუხედავად მათი არასავალდებულო ხასიათისა, აჩვენებს, თუ როგორ შეუძლიათ ამ ინსტრუმენტებს იმოქმედონ, როგორც მარეგულირებელი კონვერგენციის კატალიზატორებმა, განსაკუთრებით ტექნოლოგიურ ან ციფრულ სექტორებში.

შტატების მსგავსი ეკონომიკური გავლენა. ევროკავშირის წესების ტექნიკურმა ხარისხმა, შიდა თანმიმდევრულობამ და ბაზრის განმსაზღვრელმა ეფექტმა ისინი მრავალი ეროვნული კანონმდებლობის მოდელად აქცია. იმიტაცია შეიძლება გამომდინარეობდეს პრაგმატული მიზნებიდან (მაგალითად, ევროკავშირის ბაზარზე წვდომის ხელშეწყობა), მაგრამ ასევე სამართლებრივი პრესტიჟიდან და ნორმატიული დაახლოების სურვილიდან.

ამ ეფექტისთვის ყველაზე ნაყოფიერი ნიადაგი პერსონალურ მონაცემთა დაცვის სამართალი აღმოჩნდა. მაგრამ გარემოსდაცვით სამართალშიც ევროკავშირის მიერ ქიმიური ნივთიერებების რეგულირება ("REACH") მოდელად იქცა ისეთი ქვეყნებისთვის, როგორებიცაა ჩინეთი და თურქეთი, რამაც ხელი შეუწყო ცალმხრივი მარეგულირებელი გლობალიზაციის ფენომენს — არა თავსმოხვევით, არამედ ევროკავშირის სტანდარტებთან ნებაყოფლობითი შესაბამისობით, თავსებადობისა და სტრატეგიული უპირატესობის მოპოვებას[12].

"GDPR"-ის შემთხვევაში, იმიტაცია მერყეობდა პირდაპირი „კოპირებიდან" შერჩევით მიღებამდე. განსაკუთრებით აღსანიშნავია მე-5(2) მუხლით გათვალისწინებული ანგარიშვალდებულების პრინციპი. ეს პრინციპი მოითხოვს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა (სუბიექტი, რომელიც განსაზღვრავს დამუშავების მიზნებსა და საშუალებებს) უზრუნველყოს მონაცემთა დაცვის ფუნდამენტური პრინციპების — კანონიერების, სამართლიანობის, გამჭვირვალობის, მონაცემთა მინიმიზაციის, მთლიანობის და ა. შ. — დაცვა არა ვალდებულებათა ფიქსირებული სიით, არამედ იმის დემონსტრირებით, რომ დამუშავება უზრუნველყოფს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების ადეკვატურ დაცვას.

მაგალითად, ბრაზილიის პერსონალურ მონაცემთა დაცვის ძირითადი კანონი ("LGPD") — 2018 წლის კანონი № 13.709 — ძალიან ჰგავს GDPR-ს[13]: იგი ვრცელდება ყველა სუბიექტზე (საჯარო თუ კერძო, ფიზიკურ თუ იურიდიულ პირზე), რომლებიც ამუშავებენ ბრაზილიაში მყოფი ფიზიკური პირების პერსონალურ მონაცემებს, მონაცემთა დამუშავებაზე პასუხისმგებელი პირის ადგილსამყოფელის მიუხედავად; ის მოითხოვს მონაცემთა სუბიექტებისთვის მკაფიო და ამომწურავი ინფორმაციის მიწოდებას; ავალდებულებს მაღალი რისკის შემცველი დამუშავებისთვის გავლენის შეფასების ჩატარებას; და დამუშავების ოპერაციების რეესტრის წარმოებას[14].

[12] See *Almada M., Petit N.,* The EU AI Act: A Medley of Product Safety and Fundamental Rights, EUI, RSC, Working Paper, 2023/59.

[13] *Liz dos Santos A.L.*, Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais", Revista dos Tribunais, (2020), 105.

[14] For further details, see *Viola M., L. Heringer.,* Um olhar internacional: Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados, in *Souza C.A., Magrani E., Silva P., (eds.),* Lei Geral de Proteção de Dados(LGPD): caderno especial, São Paulo, Thomson Reuter, 2019, 227.

“LGPD”-ის 50-ე მუხლი დამუშავებაზე პასუხისმგებელ პირებსა და დამუშავებაზე უფლებამოსილ პირებს — ინდივიდუალურად ან ასოციაციების მეშვეობით — საშუალებას აძლევს, შეიმუშაონ კარგი პრაქტიკისა და მმართველობის კოდექსები, შიდა ზედამხედველობის მექანიზმები, რისკის შემცირების სტრატეგიები და, განსაკუთრებით, ტექნიკური და უსაფრთხოების სტანდარტები. ამ ნაწილში “LGPD” და “GDPR” ერთმანეთისგან განსხვავდება: მიუხედავად იმისა, რომ ეს უკანასკნელი უშვებს ქცევის კოდექსების შემუშავებას, იგი მკაფიოდ არ არეგულირებს საერთო ტექნიკური და უსაფრთხოების სტანდარტების განსაზღვრას, რაც ოპერატორებს საუკეთესო პრაქტიკასთან დაკავშირებით გაურკვევლობაში ტოვებს.

ბრაზილიის კანონმდებლობა ასევე ითვალისწინებს, რომ მონაცემთა მართვის პოლიტიკა უნდა ეფუძნებოდეს რისკისა და გავლენის სისტემატურ შეფასებას, რომელიც ორგანიზაციის ზომის, საქმიანობის მასშტაბისა და მონაცემთა სენსიტიურობის პროპორციულია. “GDPR”-ის მსგავსად, “LGPD”-ის 50-ე მუხლი მოითხოვს, რომ დამუშავებისთვის პასუხისმგებელ პირებმა დაამტკიცონ მიღებული ზომების ადეკვატურობა; თუმცა სავალდებულო უსაფრთხოების ზომების მინიმალური ბაზისის არსებობა, სავარაუდოდ, ამარტივებს შესაბამისობას — ყოველ შემთხვევაში, პროცედურულად — ბრაზილიური კომპანიებისა და ადმინისტრაციებისთვის.

მსგავსი შედარებითსამართლებრივი ანალიზი ვრცელდება შვეიცარიის პერსონალურ მონაცემთა დაცვის განახლებულ კანონზეც, რომელიც 2017 წელს დაწყებული საკანონმდებლო პროცესის შედეგად 2020 წელს შევიდა ძალაში. სხვა ელემენტებთან ერთად, იურიდიული პირები აღარ შედიან „პერსონალური მონაცემების“ განმარტებაში. ბრაზილიის მსგავსად, დამუშავებაზე პასუხისმგებელ პირებმა უნდა აწარმოონ დამუშავების რეესტრი. მაღალი რისკის შემცველი დამუშავებისთვის სავალდებულოა გავლენის შეფასება და პერსონალურ მონაცემთა დაცვის დარღვევების შესახებ უნდა ეცნობოს საზედამხედველო ორგანოს (მონაცემთა დაცვისა და ინფორმაციის ფედერალურ კომისარს)[15].

შვეიცარიის კანონმდებლობა ასევე ითვალისწინებს ადგილობრივი წარმომადგენლის დანიშვნას უცხოეთში დაფუძნებული დამუშავებისთვის პასუხისმგებელი პირებისთვის. რაც შეეხება მონაცემთა სუბიექტის უფლებებს, ახალი კანონი, “GDPR”-ის შესაბამისად, აწესებს მონაცემთა პორტაბელურობის უფლებას და უფლებას, რომ არ დაექვემდებარო მხოლოდ ავტომატიზებულ გადაწყვეტილებას. საზედამხედველო ორგანოს უფლებამოსილებები გაფართოვდა და მოიცავს ინსპექტირებასა და სავალდებულო ძალის მქონე გადაწყვეტილებების მიღებას.

ბევრმა სხვა ქვეყანამ მიიღო “GDPR”-ის შთაგონებით შექმნილი რეგულაციები, მათ შორის ნიგერიის მონაცემთა დაცვის რეგულაცია (“NDPR”), რომელიც 2019 წლის იანვარში გამოიცა, და ეგვიპტის 2020 წლის კანონი № 151. მცირე ქვეყნებისთვის ეს ასახავს ევროკავშირთან ვაჭრობის ხელშეწყობის

[15] Cf. *Meier P., Métille S.,* Loi fédérale sur la protection des données, Helbing Lichtenhahn Verlag, 2023.

აშკარა სურვილს იმ სამართლებრივი პრესტიჟის მიღმა, რომელსაც "GDPR"-მა აშკარად მიაღწია. შვეიცარიის მიერ ამ სტანდარტებთან დაახლოება თითქმის გარდაუვალი ჩანს მისი გეოგრაფიული მდებარეობის გათვალისწინებით, მიუხედავად იმისა, რომ ის ევროკავშირის წევრი არ არის. უფრო გასაკვირი ის არის, რომ ისეთმა გლობალურმა ეკონომიკურმა ძალამ, როგორიცაა ბრაზილია, მიიღო მსგავსი სტანდარტები.

ცალკე, თუმცა მოკლე, განხილვას იმსახურებს ჩინეთის მონაცემთა დაცვის რეფორმა. პერსონალური ინფორმაციის დაცვის კანონი ("PIPL") ძალაში 2021 წლის 1 ნოემბერს, ხანგრძლივი საკანონმდებლო დებატების შემდეგ შევიდა. ის, სავარაუდოდ, წარმოადგენს მნიშვნელოვან ცვლილებას გლობალურ სამართლებრივ ლანდშაფტში, რადგან ჩინეთმა მიიღო ევროკავშირის შთაგონებით შექმნილი რამდენიმე მარეგულირებელი ელემენტი და გაიმეორა "GDPR"-ის მრავალი დებულება[16].

კანონის მოქმედების სფერო სამ ძირითად სცენარს მოიცავს:

ა) ჩინეთის ტერიტორიაზე განხორციელებული დამუშავების ოპერაციები;

ბ) ჩინეთის მოქალაქეებისთვის საქონლის ან მომსახურების მიწოდება, ან მათი ქცევის ანალიზი;

გ) ეროვნული კანონმდებლობით გათვალისწინებული სხვა შემთხვევები.

როდესაც უცხოური სუბიექტი ("Foreign entity") ამუშავებს პერსონალურ მონაცემებს "PIPL"-ის იურისდიქციის ფარგლებში, 53-ე მუხლი მას ავალდებულებს, ჩინეთში დააფუძნოს წარმომადგენლობა ან დანიშნოს წარმომადგენელი, რომლის დეტალებიც უნდა წარედგინოს შესაბამის ორგანოებს. 72-ე მუხლი, "GDPR"-ის მსგავსად, პერსონალური ან საყოფაცხოვრებო მიზნებით მონაცემთა დამუშავებას "PIPL"-ის მოქმედების სფეროდან ათავისუფლებს.

"PIPL"-ი, "GDPR"-ის მსგავსად, ერთმანეთისგან მიჯნავს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებსა და დამუშავებაზე უფლებამოსილ პირებს და მათ მსგავს როლებს ანიჭებს: მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები განსაზღვრავენ დამუშავების მიზნებსა და საშუალებებს, დამუშავებაზე უფლებამოსილი პირები მოქმედებენ მათი მითითებით. ძლიერი პარალელები ჩნდება მონაცემთა შეგროვებისას მისაწოდებელ სავალდებულო ინფორმაციასთან დაკავშირებითაც, რომელიც ძალიან ჰგავს "GDPR"-ის მე-13 მუხლს[17].

"PIPL"-ის მიხედვით, სენსიტიური მონაცემები მოიცავს რელიგიურ მრწამსისა და ჯანმრთელობის შესახებ მონაცემებს (როგორც "GDPR"-ში), მაგრამ ასევე ფინანსურ ინფორმაციასა და პირად აქტივებს — კატეგორიებს, რომლებიც ევროკავშირის კანონმდებლობით სენსიტიურად არ არის

[16] *Moriconi C.*, Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China, 9 Nordic Journal of Law and Social Research, (2019) 248; *Santoni G.*, Personal data as a market commodity: legal irritants from China "experience", 1 European Journal of Privacy Law and Technology, (2023), 1.

[17] *Creemers R.*, China's Emerging Data Protection Framework, (November 16, 2021), SSRN: https://ssrn.com/abstract=3964684.

კლასიფიცირებული. ბიომეტრიული მონაცემები, 14 წლამდე არასრულწლოვანთა შესახებ ინფორმაცია და გეოლოკაციის მონაცემები პირდაპირ არის შეტანილი სენსიტიურ კატეგორიებში, რაც ამ საკითხებზე გლობალური შეშფოთების ზრდას უსვამს ხაზს.

მონაცემთა დამუშავების სამართლებრივი საფუძვლები, "PIPL"-ის მიხედვით, ძალიან ჰგავს "GDPR"-ში არსებულ საფუძვლებს. თანხმობა უნდა იყოს ნებაყოფლობითი, კონკრეტული და გამოხმობადი (მუხლი 14). "GDPR"-ის მსგავსად, თანხმობა არ არის საჭირო, თუ მონაცემთა დამუშავება აუცილებელია სახელშეკრულებო ვალდებულებების შესასრულებლად ან კანონის მოთხოვნათა დასაცავად. საზოგადოებრივი ჯანმრთელობის საგანგებო მდგომარეობა და სიცოცხლისთვის ან ჯანმრთელობისთვის საფრთხის შემცველი სიტუაციები ასევე აღიარებულია მოქმედ სამართლებრივ საფუძვლებად[18].

"PIPL" განსაკუთრებულ ყურადღებას უთმობს მონაცემთა გადაცემას და მოითხოვს წინასწარი შეფასების პროცედურებს, რომლებიც "GDPR"-ის "DPIA"-ს მსგავსია, მაგრამ უფრო მკაცრი პირობებით[19]. ეს შეფასებები უნდა ეხებოდეს გადაცემის მართებულობას, აუცილებლობასა და პროპორციულობას; მონაცემთა კატეგორიებსა და სენსიტიურობას; და მიმღების ტექნიკურ და ორგანიზაციულ უსაფრთხოების ზომებს[20].

მე-40 მუხლის თანახმად, ეს შეფასებები უნდა ჩაატაროს კიბერსივრცის ადმინისტრირების სახელმწიფო დეპარტამენტმა და ძირითადად დაეფუძნოს უსაფრთხოების კრიტერიუმებს. ეს ვალდებულება ვრცელდება კრიტიკული ინფრასტრუქტურის ოპერატორებსა და დამუშავებაზე პასუხისმგებელ პირებზე, რომლებიც ამუშავებენ პერსონალურ მონაცემებს იმავე დეპარტამენტის მიერ დადგენილ ზღვრულ მაჩვენებლებზე მეტი მოცულობით.

---

[18] *Calzada I.*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL), 5 Smart Cities, (2022) 1140.

[19] "PIPL"-ის (პერსონალური ინფორმაციის დაცვის კანონი) 38-ე მუხლი ითვალისწინებს საზღვარგარეთ პერსონალური მონაცემების გადაცემის ოთხ განსხვავებულ და ალტერნატიულ კრიტერიუმს: ა) ჩინეთის კიბერსივრცის ეროვნული ადმინისტრაციის მიერ ორგანიზებული უსაფრთხოების შეფასების გავლა, ამავე კანონის მე-40 მუხლის შესაბამისად; ბ) ჩინეთის კიბერსივრცის ეროვნული ადმინისტრაციის დებულებების თანახმად, სპეციალიზებული ორგანოს მიერ გაცემული პერსონალური ინფორმაციის დაცვის სერტიფიკატის მოპოვება; გ) უცხოელ მიმღებთან იმავე ადმინისტრაციის მიერ შემუშავებული სტანდარტული ხელშეკრულების საფუძველზე ხელშეკრულების დადება, რომელიც განსაზღვრავს ორივე მხარის უფლებებსა და მოვალეობებს; დ) კანონებით, ადმინისტრაციული რეგულაციებით ან ჩინეთის კიბერსივრცის ეროვნული ადმინისტრაციის მიერ გათვალისწინებული სხვა პირობები. PIPL-ის თარგმანი შესრულებულია როგიერ კრემერსისა (Rogier Creemers) და გრეჰემ ვებსტერის (Graham Webster) მიერ, რომელიც ეფუძნება DigiChina-ს მიერ შემუშავებული კანონის მეორე პროექტის წინასწარ ინგლისურ ვერსიას და ხელმისაწვდომია შემდეგ ბმულზე: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> ჩასატარებელი შეფასების შესახებ დამატებითი განხილვისთვის, იხილეთ აგრეთვე: *Zheng G.,* Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China, 43 Computer Law Security Rev. 105610, 2021.

[20] *Voss W. G., Pernot-Leplay E.,* China Data Flows and Power in the Era of Chinese Big Tech, 44 Nw. J. Int'l L. & Bus. (2024) 1.

მთავარი განსხვავება ევროკავშირისა და ჩინეთის მოდელებს შორის შეფასებაზე პასუხისმგებელ ორგანოშია. ჩინეთში თვითშეფასება დაუშვებელია: საჯარო ორგანოებმა უნდა მოახდინონ ყველა ზომის ვალიდაცია, ერთიანი სტანდარტების შესაბამისად. ამის საპირისპიროდ, "GDPR" დამუშავებისთვის პასუხისმგებელ პირებს აძლევს თავისუფლებას, მიიღონ ის უსაფრთხოების ზომები, რომლებსაც თავად მიიჩნევენ შესაფერისად. ამ თვალსაზრისით, ჩინეთის მოდელი ფორმალურად უფრო პროგნოზირებადი ჩანს, მაგრამ ის ასევე გულისხმობს ინფორმაციის ნაკადებზე მუდმივ სახელმწიფო ზედამხედველობას.

"GDPR"-ისა და "PIPL"-ის პარალელი ირღვევა კერძო სამართლიდან საჯარო სამართალზე გადასვლისას, განსაკუთრებით სახელმწიფოსა და მოქალაქეებს შორის ურთიერთობაში. როგორც ჩანს, "PIPL" ორი მიმართულებით მოძრაობს: ერთი მხრივ, უახლოვდება ევროკავშირის წესებს კომერციული გაცვლის ხელშესაწყობად; მეორე მხრივ, ინარჩუნებს აშკარა დისტანციას საჯაროსამართლებრივი მიდგომის თვალსაზრისით[21].

მაგალითად, „განსაკუთრებული კატეგორიის მონაცემების" განმარტება მოიცავს ნებისმიერ ინფორმაციას, რომლის უკანონო გამჟღავნებამ შეიძლება ზიანი მიაყენოს ღირსებას, ეროვნულ უსაფრთხოებას ან პირად საკუთრებას, რაც ასახავს აშკარა დისბალანსს ინდივიდებსა და სახელმწიფო ხელისუფლებას შორის. სპეციალური კატეგორია, რომელიც ევროკავშირის სამართალში არ არსებობს, მოიცავს მონაცემთა დამუშავებას ჟურნალისტური, პოლიტიკური ან საზოგადოებრივი ინტერესის მიზნებისთვის.

დაბოლოს, აღსანიშნავია, რომ "PIPL"-ს არ უკავია ისეთი ცენტრალური ადგილი ჩინეთის ციფრულ მარეგულირებელ ჩარჩოში, როგორიც "GDPR"-ს აქვს ევროკავშირში. ის უფრო ფართო სამართლებრივ არქიტექტურაშია ჩაშენებული, რომელშიც დომინირებს კიბერუსაფრთხოების კანონი. სისტემაში, რომელშიც ფუნდამენტური უფლებები ექვემდებარება სახელმწიფოს სხვა პრიორიტეტებს, პერსონალურ მონაცემთა დაცვა მეორეხარისხოვან საზრუნავად რჩება.

3. რატომ ქმნის (ან შექმნიდა) ამერიკის შეერთებული შტატები ინოვაციებს?

ახლა დავუბრუნდეთ იმ თავდაპირველ დაშვებას, რომ ამერიკის შეერთებული შტატები „დიდი ინოვატორის" როლს ასრულებს და გავაანალიზოთ ის საკანონმდებლო მიდგომა, რომელმაც ხელი შეუწყო ტექნოლოგიურ განვითარებას. მიუხედავად იმისა, რომ აშშ-ის კომპანიების ტექნოლოგიური პროგრესის დონეს სხვა ქვეყნები ვერ შეედრებიან, ასევე

[21] Cfr. *Pernot-Leplay E.,* China's Approach on Data Privacy Law: A Third Way between the US and the EU? 49 Penn State Journal of Law & International Affairs, (2020) 49, secondo cui la Cina rappresenterebbe un modello terzo rispetto a Stati Uniti ed Europa.

უდავოა, რომ ამ განვითარებაზე მნიშვნელოვანი გავლენა მოახდინა პოლიტიკურმა და საკანონმდებლო გადაწყვეტილებებმა.

ამ გადაწყვეტილებების საფუძვლად მდებარე ნეოლიბერალური რიტორიკა ყოველთვის ეფუძნებოდა ერთ მთავარ დაშვებას: „ტექნოლოგია ექსპონენციალურად იცვლება, ხოლო სოციალური, ეკონომიკური და სამართლებრივი სისტემები — ეტაპობრივად“.[22] ეს ქმნის „ტემპის“ პრობლემას, რაც გულისხმობს, რომ სამართალი ტექნოლოგიურ პროგრესზე ნელა ვითარდება და, შესაბამისად, ინსტიტუტებმა თავი უნდა შეიკავონ ციფრულ ინოვაციებზე შეზღუდვების დაწესებისგან, სანამ ტექნოლოგიები სრულად არ მომწიფდება. თუმცა ეს გამარტივებული მიდგომა დეტალურ შესწავლას იმსახურებს. მართალია, ტექნოლოგია საკანონმდებლო პროცესებზე სწრაფად ვითარდება, მაგრამ ისიც მართალია, რომ სამართლის ფუნქცია უნდა იყოს არა მხოლოდ ტექნოლოგიის წინსვლის ხელშეწყობა, არამედ მისთვის საზღვრების დაწესებაც, როდესაც ტექნოლოგიური განვითარება საფრთხეს უქმნის აღიარებულ და კოდიფიცირებულ ღირებულებებს.

ყველაზე სიღრმისეული აკადემიური ნაშრომები საუბრობენ „მეოცე საუკუნის სინთეზზე“ — ნეოლიბერალურ პარადიგმაზე, რომელიც სამ ძირითად საყრდენს ეფუძნება: ბაზრის ეფექტიანობა, როგორც უზენაესი კრიტერიუმი, რომელიც უგულებელყოფს ძალაუფლებისა და უთანასწორობის საკითხებს; სამართლებრივი ნორმების ფორმალური ნეიტრალიტეტი, რომელიც ფარავს ფარულ ძალაუფლებრივ დინამიკას; და „ანტიპოლიტიკური“ მიდგომა, რომელიც ამცირებს დემოკრატიული პოლიტიკის როლს ტექნიკური გადაწყვეტილებების მიღების სასარგებლოდ[23].

---

[22] ეს სიტყვები ეკუთვნის ლ. დაუნსს (*Larry Downes*), ნაშრომში დესტრუქციის კანონები: ახალი ძალების ათვისება, რომლებიც მართავენ ცხოვრებასა და ბიზნესს ციფრულ ეპოქაში (The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009). წიგნი აანალიზებს ციფრული ტექნოლოგიების გავლენას სამართალსა და საზოგადოებაზე, იმ თეზისიდან გამომდინარე, რომ კანონი და მარეგულირებელი ინსტიტუტები ვითარდება ხაზოვანი ტემპით, მაშინ როდესაც ტექნოლოგია - ექსპონენციალურად. ეს დისბალანსი იწვევს მარეგულირებელ დესტრუქციას, რა დროსაც ტრადიციული სამართლებრივი ნორმები ვეღარ ეგუება ახალ ციფრულ სცენარებს, რაც სათავეს უდებს „დესტრუქციის ცხრა კანონს“. ეს კანონები ხაზს უსვამს, თუ როგორ ცვლის ტექნოლოგია ძირეულად დამკვიდრებულ სექტორებს და მოძველებულად აქცევს წინაციფრულ ეპოქაში შექმნილ სამართლებრივ ნორმებს. ისეთი საკითხები, როგორებიცაა პირადი ცხოვრების ხელშეუხებლობა, ინტელექტუალური საკუთრება, პლატფორმის პასუხისმგებლობა და მონაცემთა მმართველობა, განხილულია პროაქტიულად, ინოვაციებთან ერთად განვითარების უნარის მქონე, უფრო მოქნილი და პრინციპებზე დაფუძნებული რეგულირების შემუშავებისკენ მოწოდებით. აღსანიშნავია, რომ, აშშ-ის მარეგულირებელ გადაწყვეტილებებზე გავლენის გარდა, წიგნმა მნიშვნელოვანი გავლენა მოახდინა აკადემიურ და პოლიტიკურ დებატებზე დინამიური და ადაპტირებადი რეგულირების საჭიროების შესახებ. მართლაც, მიუხედავად იმისა, რომ საკანონმდებლო ტექსტებში პირდაპირ ციტირებული არ არის, ამ თეორიამ ხელი შეუწყო ევროკავშირის საკანონმდებლო არჩევნის ფორმირებას რისკზე დაფუძნებული და ტექნოლოგიურად ნეიტრალური მიდგომებისკენ, რაც აისახა “GDPR”-ში, ციფრული ბაზრების აქტსა და ხელოვნური ინტელექტის აქტში.

[23] იხ.: *Purdy J.S., Grewal D.S., Kapczynski A., Rahman S. K.,* Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis, 129 Yale L.J. 1784, 2020. ჩვენი აზრით, ეს არის ფუძემდებლური კვლევა, რადგან ის ე.წ. „სამართლისა და პოლიტიკური ეკონომიკის“ (“LPE”) მიდგომის თეორიულ ჩარჩოს ქმნის. იგი ეჭვქვეშ აყენებს გაბატონებულ მოსაზრებას, რომლის თანახმადაც, სამართალი

გარდა ამისა, „სამართლისა და ეკონომიკის“ პარადიგმებისა და მათი დოქტრინების მიღებამ, რომლებიც ათწლეულების განმავლობაში დომინირებდა ჩრდილოეთ ამერიკის დებატებში, თავად ნეოლიბერალიზმის საყრდენები ჩამოაყალიბა. ნეოლიბერალიზმი არ უნდა განვიხილოთ, როგორც ბაზრის ლოგიკის ბუნებრივი შედეგი, როგორც ამას ხშირად ამტკიცებენ ან ვარაუდობენ, არამედ როგორც სამართლის მიერ ფორმირებული ინსტიტუციური ძალა. აქ საკანონმდებლო და სასამართლო კომპონენტები ნეიტრალურ როლს არ ასრულებენ; ისინი აქტიურად მონაწილეობენ ბაზრების სტრუქტურირებაში, კერძო ძალაუფლების გაძლიერებასა და დემოკრატიულ შესაძლებლობებზე გავლენის მოხდენაში[24].

შემთხვევითი არ არის, რომ ამერიკის შეერთებულ შტატებში, სადაც მონაცემთა დაცვის ფედერალური რეგულაცია არ არსებობს, იურიდიული მეცნიერება კვლავ მიდრეკილია, პირადი ცხოვრების ხელშეუხებლობა განსაზღვროს, როგორც „მარტო ყოფნის უფლება“ და არა ისე, როგორც პერსონალური მონაცემების მიმოქცევასა და გამოყენებაზე კონტროლი. სხვა სიტყვებით რომ ვთქვათ, აშშ შორს რჩება მონაცემთა დაცვის, როგორც ფუნდამენტური უფლების, ევროპული პარადიგმისგან და კვლავაც ეჭიდება პირადი ცხოვრების ხელშეუხებლობის საკუთრებით გაგებასროგორც სხვების საკუთარ პირად საქმეებში ჩარევის აკრძალვის უფლებას ან საკუთარ მონაცემებზე საკუთრებით კონტროლს. ეს მიდგომა არ ითვალისწინებს, რომ მონაცემთა გამოყენებამ, მიუხედავად იმისა, რომ ის ინდივიდის დაცვას ისახავს მიზნად, უნდა დაუთმოს ადგილი კოლექტიურ ინტერესს, როდესაც ზოგად საზოგადოებრივი საკითხები წამოიჭრება[25].

ხელოვნური ინტელექტის სფეროში ამჟამად მიმდინარეობს ქაოტური დებატები მათ შორის, ვინც ნებისმიერ ახალ რეგულაციაზე სრული მორატორიუმის გამოცხადებას ემხრობა (და არსებული კანონების მომდევნო ათწლეულის განმავლობაში შეჩერებასაც კი გვთავაზობს), და მათ შორის, ვინც უფრო ფრთხილად მოითხოვს ახალი ტექნოლოგიების ფონზე მოქალაქეებისთვის უსაფრთხოების ზომებისა და დაცვის მექანიზმების

მხოლოდ ნეიტრალურ საბაზრო პირობებს უნდა უზრუნველყოფდეს და ეკონომიკურ აქტორებს სახელმწიფოს მხრიდან სტრუქტურული ჩარევის გარეშე თავისუფალი მოქმედების საშუალებას აძლევდეს. ეს შეხედულება არაადეკვატურია უთანასწორობის, ეკონომიკური ძალაუფლებისა და დემოკრატიული კრიზისის თანამედროვე დინამიკის გასააზრებლად. ავტორები ამტკიცებენ, რომ სამართალი არასდროს არის ნეიტრალური; პირიქით, ის ასრულებს კონსტიტუციურ როლს ეკონომიკის ორგანიზებასა და რესურსებისა თუ ძალაუფლების გადანაწილებაში. სტატია მოგვიწოდებს, გადავიაზროთ სამართლებრივი ინსტიტუტები, როგორც სოციალური ტრანსფორმაციის ინსტრუმენტები, რომლებიც ხელს უწყობენ ეკონომიკურ სამართლიანობას, ინკლუზიურობასა და არსებით დემოკრატიას. მან მნიშვნელოვანი გავლენა მოახდინა აკადემიურ დებატებზე, განსაკუთრებით ისეთ სფეროებში, როგორებიცაა ციფრული რეგულირება, შრომა, გარემოსდაცვითი სამართალი და რასობრივი თანასწორობა.

[24] Cf. *Kennedy D.*, Law-and-Economics from the Perspective of Critical Legal Studies, in *P. Newman (ed.),* The New Palgrave Dictionary of Economics and the Law, London, 2002, <duncankennedy.net/wp-content/uploads/2024/01/law-and-economics-from-the-perspective-of-cls.pdf>.

[25] A paradigmatic example is the undoubtedly valuable and scientifically rigorous work by *Richards N.,* Why Privacy Matters, Oxford University Press, 2021.

დაწესების აუცილებლობას. რისკი არის "laissez-faire"-ის ახალი ფაზა, რომელიც ამერიკულ კომპანიებს საშუალებას მისცემს, განიმტკიცონ (ან, უფრო სწორად, გააძლიერონ) თავიანთი ოლიგოპოლიური პოზიციები ბაზარზე, ტრანზაქციული ხარჯებისა და მარეგულირებელი ბარიერებისგან თავისუფლად. ეს სცენარი 1990-იანი წლების ბოლოსა და 2000-იანი წლების დასაწყისს — ინტერნეტის პირველ „სეზონს" — მოგვაგონებს.

აშშ-ის სამართლებრივი მოდელის ანალიზს ართულებს მისი ფედერალური ბუნება და შედეგად, შტატების დონეზე არსებული, ხშირად ურთიერთშეუსაბამო კანონების ერთობლიობა, რომლებიც ტექნოლოგიურ ინოვაციებს არეგულირებს.

თუმცა ორი მაგალითი პარადიგმატულია.

1996 წელს, კლინტონის ადმინისტრაციის დროს, მიიღეს *კომუნიკაციების ღირსების აქტი* ("CDA"), როგორც პასუხი ონლაინ ბავშვთა პორნოგრაფიის მზარდ პრობლემაზე[26]. სენატორი ექსონი, აქტის მთავარი ინიციატორი, მიზნად ისახავდა ონლაინ პორნოგრაფიის გავრცელების შეზღუდვას და, კერძოდ, არასრულწლოვანთა წვდომის შეზღუდვას ასეთ მასალაზე[27]. ინტერნეტისგან მომდინარე პოტენციურმა საფრთხემ — ერთგვარი „წითელი

[26] განსახილველი აქტის მიღების შემდეგ იურიდიული დოქტრინის ნაწილმა ონლაინ პორნოგრაფიის რეგულირებისთვის ალტერნატიული გადაწყვეტა შემოგვთავაზა, რომელიც ვებსაიტებისთვის მეორე დონის დომენის (მაგ., .sex ან .osc) მინიჭებას გულისხმობს, რათა *prima facie* მიუთითოს კონტენტის უხამს ბუნებაზე. See *Major A. M., Internet Red Light District:* A Domain Name Proposal for Regulatory Zoning of Obscene Content, in *Marshall J.* Computer & Info. 21, 1997.

[27] „საინფორმაციო სუპერმაგისტრალი არ უნდა იქცეს წითელი შუქნიშნების რაიონად. ეს კანონმდებლობა ამას აღკვეთს და წესიერების იმ სტანდარტებს, რომლებიც იცავდა სატელეფონო მომხმარებლებს, ახალ სატელეკომუნიკაციო მოწყობილობებზეც გაავრცელებს. მისი მიღების შემდეგ ჩვენი შვილები და ოჯახები უკეთ იქნებიან დაცული მათგან, ვინც ციფრულ სამყაროში ბავშვების არასათანადო კომუნიკაციებსა და ურთიერთობებში ჩასათრევად მოქმედებს. წესიერების აქტი ასევე დაიცავს მოქალაქეებს ელექტრონული თვალთვალისგან და დაიცავს სახლის ხელშეუხებლობას დაუპატიჟებელი უხამსობისგან", 141 Cong. Rec. S1953. იხილეთ აგრეთვე: „კომუნიკაციების წესიერების აქტის ფუნდამენტური მიზანია ბავშვების ესოდენ საჭირო დაცვის უზრუნველყოფა", 141 Cong. Rec. S8088. საკანონმდებლო წინადადება შთაგონებული იყო მ.რ. იმის (M.R. Imm) კვლევით, Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories, 83 Georgetown L.J. 1849 (1985), რომელშიც ნათქვამი იყო, რომ ონლაინ გავრცელებული კონტენტის 83.5% პორნოგრაფიული ხასიათის იყო. თუმცა კვლევამ მნიშვნელოვანი კითხვები გააჩინა როგორც აშშ-ის იურისტ-აკადემიკოსებში, ისე სისტემის ოპერატორებში. კრიტიკული მოსაზრებების მიმოხილვისთვის, იხილეთ *Cannon R.,* The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway, 49 Fed. Comm. L.J. 52 (1996). რაც შეეხება უხამსობას, წამყვანი პრეცედენტებია *Miller v. California*, 413 U.S. 15 (1973), რომელმაც დაადგინა უხამსობის შეფასების სტანდარტები (ე. წ. „უხამსობის ტესტი"), და *Paris Adult Theatre I v. Slaton*, 413 U.S. 49 (1973), რომელმაც აღიარა სახელმწიფოს ინტერესი, დაარეგულიროს უხამსი და პორნოგრაფიული მასალების კომერციული გავრცელება, ისევე, როგორც ამგვარი ხასიათის საჯარო ჩვენებები. საკანონმდებლო დონეზე, უხამსობა რეგულირდება ამერიკის შეერთებული შტატების კოდექსის მე-18 კარის 71-ე თავით, ხოლო 47-ე კარის § 223 ეხება „უხამს ან შევიწროების შემცველ სატელეფონო ზარებს". აღსანიშნავია, რომ უხამსობა ერთ-ერთია იმ იშვიათ გამონათქვამთაგან, რომელსაც პირველი შესწორება არ იცავს. ბუნებრივია, აკრძალულია ბავშვთა პორნოგრაფიის ფლობა და გავრცელებაც; იხილეთ 18 U.S.C. § 2251; *Osborne v. Ohio*, 495 U.S. 103 (1990). საბოლოოდ, 1998 წელს, ონლაინ სივრცეში ბავშვთა ექსპლუატაციასთან ბრძოლის მიზნით, მიღებულ იქნა „ბავშვთა სექსუალური მტაცებლებისგან დაცვის აქტი".

ფარნების უბნის“ სახით — საფუძველი დაუდო ამ აქტის შექმნას, რომელიც მეცნიერების მხრიდან მწვავე კრიტიკის საგანი გახდა, როგორც ინტერნეტის განვითარების წინააღმდეგ მიმართული, თავისუფლების შემზღუდველი ზომა (და რომელიც საბოლოოდ უზენაეს სასამართლოში გასაჩივრდა საქმეში “Reno v. ACLU“)[28].

ერთ-ერთი მთავარი დებულება იყო *Good Samaritan Clause* — § 230(c)(2)(A) — რომელიც იმუნიტეტს ანიჭებდა ინტერნეტ სერვისის პროვაიდერებს (“ISP”), რომლებიც კეთილსინდისიერად მოქმედებდნენ უხამსად, შეურაცხმყოფლად ან სხვაგვარად საზიანოდ მიჩნეულ მასალაზე წვდომის შეზღუდვის მიზნით, მაშინაც კი, როდესაც კონკრეტული კონსტიტუციური გარანტიები არ არსებობდა. დროთა განმავლობაში ამ პუნქტმა არა მხოლოდ გავლენა მოახდინა ცილისწამების სამართალზე, არამედ იქცა სამართლებრივ ფარად “ISP”-ებისთვის, რათა თავი აერიდებინათ მომხმარებლის მიერ გამოქვეყნებული კონტენტის წაშლის ვალდებულებისთვის.

რეტროსპექტივაში § 230-მა, მიუხედავად მისი გადაჭარბებებისა, ხელი შეუწყო იმ დროისთვის ახალი ინტერნეტ მოთამაშეების მიერ შეთავაზებული სერვისების გაფართოებას, რომლებმაც ისარგებლეს ერთგვარი იმუნიტეტით, რადგან არ მოეთხოვებოდათ მესამე მხარის კონტენტის წაშლა.

მეორე მნიშვნელოვანი მაგალითია 1998 წლის *ციფრული ათასწლეულის საავტორო უფლებების აქტი* (“DMCA”), რომელმაც შემოიღო დებულებები “ISP”-ების საავტორო უფლებების დარღვევის შესახებ სარჩელებისგან დასაცავად და დაამკვიდრა ტექნოლოგიური ნეიტრალიტეტის პრინციპი, რომელიც მოგვიანებით აისახა ევროკავშირის ელექტრონული კომერციის დირექტივაში (2000/31/EC) [29].

“DMCA”-ის წესებმა, რომლებიც შემდგომში ევროკავშირშიც გადმოიღეს, გაათავისუფლა “ISP”-ები პასუხისმგებლობისგან მომხმარებლების მიერ ატვირთული უკანონო მასალისთვის, იმ პირობით, რომ ასეთი მასალა დროულად წაიშლებოდა გაუქმების შესახებ ვალიდური მოთხოვნის მიღების შემდეგ. ამ გარანტიებმა უდავოდ შეუწყო ხელი ისეთი პლატფორმების აღზევებას, როგორებიცაა: “YouTube”, “Facebook” და სხვა ციფრული

[28] 521 U.S. 844 (1997). უზენაესმა სასამართლომ გააუქმა მხოლოდ კანონის §§ 223 (a) და (d) ნაწილები, რომლებიც კრძალავდა „უხამსი ან ბინძური შინაარსის შეტყობინებების გამიზნულ გადაცემას 18 წლამდე ასაკის ნებისმიერი მიმღებისთვის“ და „აშკარად შეურაცხმყოფელი შეტყობინებების გამიზნულ გაგზავნას ან ჩვენებას იმგვარად, რომ ის ხელმისაწვდომი გამხდარიყო 18 წლამდე ასაკის პირისთვის“. აგრეთვე უნდა აღინიშნოს, რომ 2001 წელს ძალაში შევიდა ბავშვთა ინტერნეტის დაცვის აქტი და სამეზობლო ინტერნეტის დაცვის აქტი. ეს კანონები ავალდებულებს ბიბლიოთეკების ოპერატორებს, დააყენონ ფილტრაციის პროგრამული უზრუნველყოფა თავიანთ კომპიუტერებზე, რომლებიც მომხმარებლებს ინტერნეტზე წვდომას აძლევს, რათა დაბლოკონ პორნოგრაფიული მასალის ჩვენება.

[29] იხ. *Verbiest T., Spindler G., Riccio G.M.,* Study on the Liability of Internet Intermediaries, European Commission, DG Internal Market, 22007, SSRN: <https://ssrn.com/abstract=2575069 or http://dx.doi.org/10.2139/ssrn.2575069>, 2002, და უახლესი: *Geiger C., Frosio G., Izyumenko E.,* The Oxford Handbook of Online Intermediary Liability, Oxford University Press, 2020.

შუამავლები, რადგან მათ საშუალება მისცა, უმასპინძლონ მომხმარებლის მიერ გენერირებული კონტენტის უზარმაზარ რაოდენობას წინასწარი კონტროლის გარეშე, რითაც საფუძველი ჩაუყარეს აშშ-ის „დიდი ტექნოლოგიური კომპანიების“ გლობალურ დომინირებას ციფრულ ეკონომიკაში.

დღეს, ხელოვნური ინტელექტის რეგულირებასთან დაკავშირებით, აშშ-ის კომპანიები კვლავ დომინანტურ პოზიციას იკავებენ ბაზარზე და პოლიტიკაც შესაბამისად რეაგირებს — მიდრეკილებით არარეგულირებისკენ და არა უბრალოდ დერეგულაციისკენ. ამის უახლესი მაგალითია შტატის ან ადგილობრივ დონეზე ხელოვნური ინტელექტის ნებისმიერ რეგულაციაზე ათწლიანი მორატორიუმის შემოღების მცდელობა, რომლის აშკარა მიზანი იყო ხელოვნური ინტელექტის განვითარებაზე შეზღუდვების თავიდან აცილება და ინდუსტრიისთვის გლობალურ კონკურენციაში მოქმედების სრული თავისუფლების მინიჭება — განსაკუთრებით ჩინეთის წინააღმდეგ, რომელიც ტრამპის ეპოქის პოლიტიკის საყვარელი სამიზნე იყო. ეს აკრძალვა შეტანილი იყო „დიდ ლამაზ კანონპროექტში“ (H.R.1), საგადასახადო და ინფრასტრუქტურული შეთანხმების კანონპროექტში და მას აქტიურად უჭერდნენ მხარს მსხვილი ტექნოლოგიური ფირმები, რომლებიც ამტკიცებდნენ, რომ ერთიანი ფედერალური ჩარჩო უფრო ეფექტიანი იქნებოდა, ვიდრე შტატების კანონების ფრაგმენტული ნაზავი[30].

ეს მორატორიუმი, რომელიც ვრცელდებოდა ხელოვნური ინტელექტის სისტემებზე, ალგორითმულ მოდელებსა და ავტომატიზებული გადაწყვეტილების მიღების ინსტრუმენტებზე, მიზნად ისახავდა არა მხოლოდ ახალი კანონების დაბლოკვას, არამედ არსებულის გაუქმებასაც, რითაც ფაქტობრივად მთელი მარეგულირებელი უფლებამოსილება კონგრესს გადაეცემოდა. მისი მომხრეების აზრით, ეს შეამცირებდა სამართლებრივ ფრაგმენტაციას ცალკეულ შტატებს შორის.

თუმცა სენატმა წინადადება უდიდესი უმრავლესობით, 99 ხმით 1-ის წინააღმდეგ, ორპარტიული კენჭისყრით უარყო. აღსანიშნავია, რომ ეს შედეგი ნაკლებად იყო განპირობებული ხელოვნური ინტელექტის დერეგულაციის პრინციპული უარყოფით და, უფრო მეტად, რესპუბლიკელთა მიდრეკილებით,

[30] კერძოდ, იხილეთ სემ ალტმანის განცხადებები, რომლებიც Tech Policy Press-მა გაავრცელა, *Transcript: Sam Altman Testifies at US Senate Hearing on AI Competitiveness*, https://www.techpolicy.press/transcript-sam-altman-testifies-at-us-senate-hearing-on-ai-competitiveness/. უფრო კონკრეტულად, მეწარმემ უარყო წინადადებები, რომლებიც დეველოპერებს ავალდებულებდა, ხელოვნური ინტელექტის სისტემების გამოშვებამდე მთავრობისგან ნებართვა მიეღოთ, და მათ სექტორისთვის „კატასტროფული“ უწოდა. მიუხედავად ამისა, მან ხაზგასმით აღნიშნა, რომ “NIST”-ის (სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტი) მიერ სტანდარტების დადგენა შეიძლება სასარგებლო იყოს იმ პირობით, რომ ეს პროგრესს არ შეანელებს. უფრო მეტიც, მიუხედავად იმისა, რომ მან აღიარა ამერიკის შეერთებული შტატების ტექნოლოგიური უპირატესობა ჩინეთთან შედარებით, ის ამტკიცებდა, რომ ამ ლიდერობის შეფასება სამომავლო პერსპექტივიდან რთულია. ამ მოსაზრების გასამყარებლად მან დაასკვნა, რომ ხელოვნური ინტელექტის მომავალი უნდა ემყარებოდეს „დემოკრატიულ ღირებულებებს, როგორებიცაა გამჭვირვალობა და თავისუფლება“, რითაც ის ავტორიტარულ მოდელებს უნდა გაემიჯნოს.

შეენარჩუნებინათ ცალკეული შტატების ავტონომია. სხვა სიტყვებით რომ ვთქვათ, უარყოფა ასახავდა შეშფოთებას ფედერალურ და შტატის დონეებს შორის ურთიერთობასა და ადმინისტრაციულ დისკრეციაზე და არა არარეგულირებული ხელოვნური ინტელექტის განვითარების თავიდან აცილების მცდელობას.

მიუხედავად ამისა, თუმცა ეს შემთხვევა არ აჩვენებს მკაფიო პოზიციას ხელოვნური ინტელექტის პოლიტიკასთან დაკავშირებით, ის გვიჩვენებს, რომ აშშ-ის რეგულირების მიმართულება შესაძლოა იცვლებოდეს.

როგორც ახლახან აღინიშნა, ბაიდენის ადმინისტრაციის სტრატეგია ორ ფაზად განვითარდა[31]. პირველი, უფრო პროგრამული ეტაპი მოიცავდა 2022 წელს „ხელოვნური ინტელექტის უფლებათა ბილის პროექტის“ გამოქვეყნებას — დოკუმენტის, რომელსაც სავალდებულო ძალა არ გააჩნია და რომელიც ხელოვნური ინტელექტის პასუხისმგებლიანი გამოყენების ძირითად პრინციპებს განსაზღვრავს: თვალთვალისგან დაცვას, ალგორითმულ გამჭვირვალობას, დისკრიმინაციის აკრძალვასა და ანგარიშვალდებულებას. მეორე, უფრო ოპერაციული ფაზა, 2023 წლის 30 ოქტომბრის[32] 14110-ე აღმასრულებელ ბრძანებასთან ერთად დადგა, რომელმაც სავალდებულო ვალდებულებები დააკისრა მოწინავე ხელოვნური ინტელექტის მოდელების, განსაკუთრებით კი ორმაგი დანიშნულების სისტემების, დეველოპერებს და დანერგა ჰოლისტური მიდგომა, რომელიც აერთიანებდა ეროვნულ უსაფრთხოებას, სამოქალაქო უფლებების დაცვასა და ინოვაციების ხელშეწყობას.

მიუხედავად იმისა, რომ ამ აღმასრულებელ ბრძანებას პირდაპირი ფედერალური კანონმდებლობა არ შეუქმნია, მან განსაზღვრა ვალდებულებების, სახელმძღვანელო პრინციპებისა და დირექტივების დეტალური ჩამონათვალი ფედერალური სააგენტოებისთვის, მიზნად ისახავდა რა ტექნოლოგიური ინოვაციების დაბალანსებას ეროვნულ უსაფრთხოებასა და სამოქალაქო თავისუფლებებთან. მისი რამდენიმე ძირითადი პრინციპი ემთხვეოდა ევროპის ხელოვნური ინტელექტის აქტის პრინციპებს. მაგალითად, ბრძანება ავალდებულებდა გამჭვირვალობას იმ კომპანიებისთვის, რომლებიც მაღალი გავლენის მქონე საბაზისო მოდელებს ქმნიდნენ, განსაკუთრებით მათ, რომლებიც აჭარბებდნენ გამოთვლითი სიმძლავრის გარკვეულ ზღვრულ მაჩვენებლებს ან იყენებდნენ არასაჯარო ინფორმაციის დიდ მონაცემთა ბაზებს. ეს ზღვრული მაჩვენებლები განისაზღვრა ვაჭრობის დეპარტამენტის მიერ, სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (“NIST”) მეშვეობით, სხვა ტექნიკურ და უსაფრთხოების სააგენტოებთან თანამშრომლობით.

[31] იხ. *Lubello V.,* From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer, in Bocconi Legal Studies Research Paper, 2025, SSRN: <https://ssrn.com/abstract=5302544>.

[32] აღმასრულებელი ბრძანება ხელოვნური ინტელექტის უსაფრთხო, დაცული და სანდო განვითარებისა და გამოყენების შესახებ.

დამატებით პარალელებს შორისაა გამჭვირვალობასა და „დიპფეიკებთან“ ბრძოლასთან დაკავშირებული ვალდებულებები, რომლებიც მოიცავს: ექსპერიმენტებს კონტენტის წყლის ნიშნებით მარკირებისა და მიკვლევადობის ტექნოლოგიებზე; ხელოვნური ინტელექტის მიერ გენერირებული კონტენტის საიდენტიფიკაციო ტექნიკური სტანდარტების შემუშავებას; და ციფრული ინფორმაციისადმი საზოგადოებრივი ნდობის გასაძლიერებლად წარმომავლობის პროტოკოლების შექმნას.

თუმცა 2025 წლის იანვარში, ტრამპის პრეზიდენტად დაბრუნებასთან ერთად, მარეგულირებელ მიმართულებაში არსებითი ცვლილება მოხდა. ეს დაიწყო 14179-ე აღმასრულებელი ბრძანებით, რომელმაც სრულად გააუქმა ბაიდენის ბრძანება და ფედერალურ სააგენტოებს დაავალა, გადაეხედათ და გაეუქმებინათ ის რეგულაციები, რომლებიც ხელს უშლიდა ხელოვნური ინტელექტის განვითარებას. ტრამპის მიდგომა, რომელიც აშკარად დერეგულაციის პრინციპებს ეფუძნება, მიზნად ისახავს აშშ-ის ტექნოლოგიური ლიდერობის კვლავ დამკვიდრებას იმ შეზღუდვების მოხსნით, რომლებიც იდეოლოგიურად ან ანტიინოვაციურად აღიქმება, განსაკუთრებით კი იმ შეზღუდვებისას, რომლებიც მიმართულია გენერაციული ხელოვნური ინტელექტის მოდელებში აღქმული „ვოუქ“ (“woke”) ან პოლიტიკურად მიკერძოებული კონტენტის წინააღმდეგ[33].

4. ევროკავშირის სამართლებრივი მოდელის შესაძლო სამომავლო გავრცელების შესახებ

ბოლო ათწლეულებში ჩვენ ვხედავთ სამართლის (განსაკუთრებით კერძო სამართლის) როლის ღრმა ტრანსფორმაციას სამართლებრივ სისტემაში, რაც მისი ცენტრალური როლის თანდათანობით დაკარგვით ხასიათდება მარეგულირებელი სამართლისა და ტექნიკური წესების სასარგებლოდ. ეს ცვლილება ასახავს არა მხოლოდ ნორმების შექმნის ფორმების ევოლუციას, არამედ თავად სამართლის კონცეფციის ცვლილებას, რომელიც სულ უფრო მეტად განიხილება, როგორც ეკონომიკის ფუნქციური ინსტრუმენტი და არა, როგორც ზოგადი და სტრუქტურული პრინციპების გამოხატულება, რომლებიც დროში მდგრადობისთვისაა შექმნილი.

კლასიკური კერძო სამართალი, რომელიც მე-19 საუკუნის სამოქალაქო კოდექსის მოდელს ეფუძნებოდა, აგებული იყო აბსტრაქტულ, სტაბილურ და მოქნილ კატეგორიებზე, რომლებიც მიზნად ისახავდა სამართლებრივი უსაფრთხოების უზრუნველყოფას და პირთა შორის ურთიერთობების სისტემური ლოგიკით მოწესრიგებას. თუმცა თანამედროვე ეპოქაში ეს ჩარჩო თანდათანობით დაჩრდილა მარეგულირებელმა სამართალმა, რომელიც

[33] აშშ-ის წარმომადგენელთა პალატა, *Censorship’s Next Frontier: The Federal Government’s Attempt to Control Artificial Intelligence to Suppress Free Speech*, შუალედური ანგარიში აშშ-ის წარმომადგენელთა პალატის იურიდიულ საკითხთა კომიტეტისა და ფედერალური მთავრობის იარაღად გამოყენების საკითხებზე მომუშავე შერჩეული ქვეკომიტეტისა, 2024 წლის 18 დეკემბერი.

გაგებულია, როგორც სექტორული წესების ერთობლიობა, ხშირად საჯარო სამართლის ბუნების, რომლის მიზანია ეკონომიკის კონკრეტული სფეროების (მაგ., ენერგეტიკა, ტელეკომუნიკაციები, ფინანსები, ჯანდაცვა, გარემოს დაცვა) რეგულირება მიზნობრივი, სიტუაციური და ხშირად ტექნოკრატიული ჩარევების გზით.

როგორც წამყვანი მეცნიერები აღნიშნავენ, „კერძო სამართალმა ადგილი დაუთმო ფუნქციურ სამართალს, რომელსაც დამოუკიდებელი უწყებები და ეფექტიანობის ლოგიკა მართავს და რომელიც ხშირად მოწყვეტილია ნებისმიერ სისტემურ მოწყობას“[34]. ამის შედეგია „ეპიზოდური“ კანონმდებლობის ფორმა, რომლის მიხედვითაც საერთო თანმიმდევრულობა ეწირება პოლიტიკური გადაუდებლობის, ბაზრის ზეწოლის ან მედიასთან დაკავშირებული გარემოებებს. კანონმდებლები უარს ამბობენ ხანგრძლივი, სტრუქტურული ნორმების შექმნაზე და სანაცვლოდ ქმნიან სამართლებრივ ტექსტებს, რომლებიც მიზნად ისახავს მყისიერი პრობლემების მოგვარებას, ყოველგვარი გრძელვადიანი ხედვის გარეშე.

როგორც მკაფიოდ არის აღნიშნული, მარეგულირებელი სამართალი წარმოადგენს ინსტრუმენტებით მმართველობის ტრიუმფს — საჯარო პოლიტიკის ფორმას, რომელიც ხორციელდება ტექნიკური ინსტრუმენტებით, პოლიტიკური განხილვისა და დემოკრატიული დებატების გვერდის ავლით[35]. ამ პროცესში სამართალი კარგავს თავის მომწესრიგებელ და პროგნოზირებად ფუნქციას და იქცევა სპეციალური, არაერთგვაროვანი წესების ნაზავად, რომელსაც ყოველგვარი სისტემური ხედვა აკლია. ხელოვნური ინტელექტის აქტი — მიუხედავად იმისა, რომ გარკვეულ პრინციპებს აწესებს — ამის მთავარი მაგალითია: სექტორული წესების რთული ქსელი, რომელსაც ხშირად ტექნიკური ექსპერტებიც კი შეუფერებლად მიიჩნევენ და რომელიც რთულად გასაგები (და გამოსაყენებელია) იურისტებისთვის.

ამ კონტექსტში თავად ნორმატიულ ენაზეც ახდენს გავლენას ტექნოკრატიული გადახრა: ნორმები ხშირად ჰიპერდეტალური ფორმით იწერება, მუდმივი მითითებებით იმპლემენტაციის რეგულაციებზე ან ტექნიკურ სტანდარტებზე, რაც მათ გაგებას ართულებს არა მხოლოდ რიგითი მოქალაქისთვის, არამედ იურისტ-პრაქტიკოსებისთვისაც. ეს ქმნის ხელმისაწვდომობის დეფიციტს და წყვეტს კავშირს სამართალსა და მის ადრესატებს შორის, რითაც ძირს უთხრის მატერიალური კანონიერების პრინციპს. ამის პარადიგმული მაგალითია ხელოვნური ინტელექტის აქტის მე-3 მუხლის 67-ე განმარტება, რომელიც „მცოცავწერტილიან ოპერაციას“ განმარტავს, როგორც „ნებისმიერი მათემატიკური ოპერაცია ან მინიჭება, რომელიც მოიცავს მცოცავწერტილიან რიცხვებს - ნამდვილ რიცხვთა ქვესიმრავლეს, რომლებიც კომპიუტერებში, როგორც წესი, წარმოდგენილია ფიქსირებული სიზუსტის მქონე მთელი რიცხვისა და მასშტაბირების

[34] *Alpa G.,* Diritto privato e tecnica legislativa, 2018, see also *Micklitz H. W.,* Introduction, in Costitutionalization of European Private Law, Oxford, 2014, 1.

[35] *Lascoumes P., Le Gales P.* (éds.), Gouverner par les instruments, Science Po, Paris, 2005.

ფაქტორის გამოყენებით, რომელიც, თავის მხრივ, ფიქსირებული ფუძის მთელი ხარისხია“.

ზოგიერთი მეცნიერი ამ ტრანსფორმაციას ნეოლიბერალური პარადიგმის აღზევებას უკავშირებს, რომელმაც შექმნა სამართლის, როგორც ბაზრის სამსახურში მყოფი ტექნიკური ინსტრუმენტის ხედვა, და არა, როგორც სამართლიანობის ან სოციალური ბალანსის აღდგენის საშუალებისა, რომლის მიხედვითაც სამართლის სავარაუდო „ტექნიკური ნეიტრალიტეტი“ მითია: ყოველი მარეგულირებელი არჩევანი გავლენას ახდენს ძალაუფლებრივ სტრუქტურებზე და ასახავს კონკრეტულ ინტერესებს და, შესაბამისად, წარმოადგენს არჩევანს, თუ რომელი ინტერესები უნდა იყოს დაცული სხვებზე მეტად[36].

თუმცა ეს არ არის „ბრიუსელის ეფექტის“ შესუსტების ერთადერთი მიზეზი. კიდევ ერთი მიზეზი არის საკანონმდებლო „წარღვნა“: ციფრული სერვისების აქტი, ციფრული ბაზრების აქტი, ხელოვნური ინტელექტის აქტი, კიბერმედეგობის აქტი, მონაცემთა აქტი, მონაცემთა მმართველობის აქტი — აღნიშნული მხოლოდ რამდენიმე მაგალითია. ეს მასიური წარმოება, რომელსაც ხშირად „რბილ სამართლად“ მოიხსენიებენ, მაგრამ პრაქტიკაში სავალდებულოა, მომდინარეობს როგორც ცენტრალური, ისე ეროვნული დონის ადმინისტრაციული ორგანოებისგან. ეს აძლიერებს სამართლებრივ ტექსტებს შორის შეუსაბამობების რისკს, რომლებიც ხშირად ლობისტური ზეწოლის შედეგია და, შესაბამისად, ცუდად არის კოორდინირებული ერთიან და თანმიმდევრულ საკანონმდებლო ხედვაში[37].

ნორმების ეს ჭარბწარმოება, რომელსაც არ ახლავს თანაბრად მძლავრი ტექნოლოგიური განვითარება ევროპულ დონეზე, ქმნის პარადოქსულ შედეგებს (მაგალითად, კომპანიები, რომლებსაც შეეხოთ პირველი აკრძალვები ხელოვნური ინტელექტის აქტის მე-5 მუხლით, რომელიც 2025 წლის თებერვლიდან მოქმედებს, არაევროპულია). ეს ასევე იწვევს დიფერენცირებულ ბიზნეს სტრატეგიებს, რომელთა შორისაა ზოგიერთი ამერიკული კომპანიის მიერ მიღებული გადაწყვეტილება, არ შესთავაზონ ხელოვნური ინტელექტის სერვისები ევროკავშირის ფარგლებში[38].

---

[36] *Purdy J.S., Grewal D.S., Kapczynski A., Sabeel Rahman K.,* note 23, 1791.

[37] Cf. *Padeiro P. J. F.*, Lobbying in the European Union's AI Act: the role of lobbying by the big five tech companies on the Council of EU's legislative process, Instituto Universitario de Lisboa, October 2024, 44; *Woll C., Artigas J.*, Big Tech's influence in the EU: Lobbying and digital governance, 61 European Journal of Political Research, 2022, 384; *Rozgonyi K.,* Digital giants and EU regulation: The lobbying strategies of Meta in Brussels, 19 Journal of Information Technology & Politics, 2022, 463.

[38] ასეთია, მაგალითად, "Apple"-ის შემთხვევა: Montgomery B., *Apple-ი ევროპაში ხელოვნურ ინტელექტზე დაფუძნებული ფუნქციების გაშვებას აჭიანურებს და მიზეზად ევროკავშირის რეგულაციებს ასახელებს.*, The Guardian, 2024 წლის 21 ივნისი. მწვავე დაძაბულობა ასევე წარმოიშვა იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ "OpenAI"-სთვის, "*ChatGPT*"-ის დეველოპერი კომპანიისთვის, საქმიანობის დროებითი შეჩერების დაწესებასთან დაკავშირებით. ამ საქმის შემდგომი ანალიზისთვის, იხ.: *Diurni A., Riccio G.M.,* ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, in 9 The Italian Law Journal, 2023, 474.

მეტიც, როგორც 2024 წლის ბოლოს ევროკომისიისთვის წარდგენილ *დრაგის ანგარიშშია* აღნიშნული, რომ ევროპამ ვერ შეძლო ადეკვატური ტექნოლოგიური შესაძლებლობების მქონე კომპანიების განვითარების ხელშეწყობა (და, შესაბამისად, აშშ-ისა და ჩინეთის „გიგანტებთან“[39] შესადარი კომპანიების შექმნა). ამის შედეგია ევროპის სრული დამოკიდებულება მესამე მხარის აქტორებზე.[40] ეს ჩამორჩენა კიდევ უფრო მძაფრდება გადაწყვეტილების მიღების ნელი პროცესებით, ფორმალისტური ვალდებულებებით (რაც შემთხვევითი არ არის, რომ იწვევს "GDPR“-ის გადახედვას, დაწყებული მცირე და საშუალო საწარმოებისთვის ჩანაწერების წარმოების ვალდებულების გაუქმებით)[41] და საუკეთესო პრაქტიკის მცირე ან ნაკლებად ტექნოლოგიურად განვითარებულ წევრ ქვეყნებში დანერგვის შეზღუდული უნარით.

დასასრულს, ძნელია იმის პროგნოზირება, შეძლებს თუ არა ევროკავშირი, დარჩეს ფუნდამენტური უფლებების დაცვის შუქურად ხელოვნური ინტელექტის განვითარების კონტექსტში.

ზოგიერთი ნიშანი მიუთითებს ამ გავლენის შემცირებასა და არაევროპული კომპანიების — არა მხოლოდ ამერიკულის — მზაობის შემცირებაზე, მოერგონ ევროპულ გადაწყვეტილებებს. მაგალითად, განვიხილოთ “DeepSeek”-ის სახელით ცნობილი დიდი ენობრივი მოდელის მმართველი ჩინური კომპანიების პასუხი, რომლებმაც არ უპასუხეს იტალიის მონაცემთა დაცვის ორგანოს მოთხოვნებს, გარდა იმისა, რომ განაცხადეს, ევროპული კონფიდენციალურობის რეგულაციები მათ საქმიანობაზე არ ვრცელდებოდა[42]. ეს აბსურდული პასუხია. აშკარაა, რომ ჩინური კომპანიების წარმომადგენელ იურისტებს არ შეიძლებოდა არ სცოდნოდათ “GDPR”-ის მოქმედების სფეროს შესახებ, მაგრამ ეს მაინც აჩვენებს ევროპული ბაზრის მიმზიდველობის შემცირებას არაევროპული ხელოვნური ინტელექტის კომპანიებისთვის.

და შესაძლოა, ეს არის ის საკითხი, რომელსაც უნდა დავუბრუნდეთ: ევროკავშირი ქმნის წესებს, მაგრამ კვლავაც დარწმუნებულნი ვართ, რომ „ინოვატორი“ ქვეყნები დაინტერესებულნი არიან მათი დაცვით?

[39] Cf. *Draghi M.,* The future of European competitiveness, European Commission, 2024.

[40] *დრაგის ანგარიშში* მოყვანილი ზოგიერთი მაგალითი, მათ შორის სტატიის ტექსტში ნახსენებიც, უკვე განხილული იყო, სხვათა შორის, შემდეგ ნაშრომში: *Renda A.,* Beyond the Brussels Effect. Leveraging Digital Regulation for Strategic Autonomy, FEPS – Foundation for European Progressive Studies, Brussels, 2022.

[41] საინფორმაციო სააგენტო, *“GDPR”-ის მიზნობრივი მოდიფიკაციები:* “EDPB და “EDPS” მიესალმებიან აღრიცხვის ვალდებულებების გამარტივებას და დამატებით განმარტებებს ითხოვენ, 2025 წლის 9 ივლისი.

[42] Garante per la protezione dei dati personali, Provv. January 30, 2025, doc. web n. 10098477.

ბიბლიოგრაფია:

1. *Almada M.*, *Petit N.,* the EU AI Act: A Medley of Product Safety and Fundamental Rights. European University Institute, RSCAS Working Paper 2023/59, 2023.
2. *Alpa G.,* Diritto privato e tecnica legislativa, 2018.
3. *Ancel M.*, Utilità e metodi del diritto comparato. Italian translation by P. Stanzione. Camerino, 1974.
4. *Ascarelli T.,* Premesse allo studio del diritto comparato, in Studi di diritto comparato e in tema di interpretazione, Milano, 1952.
5. *Bradford A.*, The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020.
6. *Calzada I.*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities 5: 1140, 2022
7. *Cannon R.,* The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway." Federal Communications Law Journal 49: 52, 1996.
8. *Costantinesco L.,* metodo comparative, Torino, 2000.
9. *Creemers R.,* China's Emerging Data Protection Framework, SSRN. https://ssrn.com/abstract=3964684, 2021.
10. *Creemers R., Webster G.,* (trans.), Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina, 2021. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.
11. *Diurni A., Riccio, G. M.,* ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, The Italian Law Journal 9: 474, 2023.
12. *Downes L.,* The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009.
13. *Draghi M.,* the Future of European Competitiveness. European Commission, 2024.
14. *Ferrajoli L.,* "Crisi del diritto e dei diritti nell'età della globalizzazione." Questione Giustizia. <https://www.questionegiustizia.it/articolo/crisi-del-diritto-e-dei-diritti-nell-eta-della-globalizzazione>, 2023.
15. *Geiger C., Frosio, G., Izyumenko E.,* the Oxford Handbook of Online Intermediary Liability. Oxford University Press, 2020.
16. *Gorla G.,* "Diritto comparato." Enciclopedia del diritto, XII, Milano, 1964.
17. *Grossi P.,* Aspetti giuridici della globalizzazione economica. In Atti della Accademia dei Georgofili, 2013.
18. *Hoecke M. Van*, ed. Epistemology and Methodology of Comparative Law. Hart Publishing, 2004.
19. *Imm M. R.,* Marketing Pornography on the Information Superhighway, Georgetown Law Journal 83: 1849, 1985.

20. *Kennedy D.,* Law-and-Economics from the Perspective of Critical Legal Studies. In The New Palgrave Dictionary of Economics and the Law, ed. *Newman P.,* London, <https://duncankennedy.net/wp-content/uploads/2024/01/law-and-economics-from-the-perspective-of-cls.pdf>, 2002.
21. *Lascoumes P*., *Le Galès P*., eds. Gouverner par les instruments. Sciences Po, Paris, 2005.
22. *Liz dos Santos A. L.,* Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais. Revista dos Tribunais 105, 2020.
23. *Lubello V.,* From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer, Bocconi Legal Studies Research Paper. SSRN: https://ssrn.com/abstract=5302544, 2025.
24. *Major A. M.,* Internet Red Light District: A Domain Name Proposal for Regulatory Zoning of Obscene Content, Marshall Journal of Computer & Information Law 21, 1997.
25. *Mattei U.,* Comparative Law and Economics. University of Michigan Press, 1997.
26. *Meier P., Métille S.,* Loi fédérale sur la protection des données. Helbing Lichtenhahn Verlag, 2023.
27. *Montgomery B.,* Apple Delays Launch of AI-powered Features in Europe, Blaming EU Rules. The Guardian, June 21, 2024.
28. *Moriconi C.,* Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China. Nordic Journal of Law and Social Research 9: 248, 2019.
29. *Pereira J. F.,* Lobbying in the European Union's AI Act: The Role of Lobbying by the Big Five Tech Companies. Instituto Universitário de Lisboa, 2024.
30. *Purdy J. S., Grewal D. S., Kapczynski A., Rahman S., K.,* Building a Law-and-Political-Economy Framework, Yale Law Journal 129: 1784, 2020.
31. *Renda A.* 2022. Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy. Foundation for European Progressive Studies (FEPS), Brussels.
32. *Richards N.,* Why Privacy Matters. Oxford University Press, 2021.
33. *Rozgonyi K.,* Digital Giants and EU Regulation: The Lobbying Strategies of Meta in Brussels, Journal of Information Technology & Politics 19: 463, 2022.
34. *Sacco R.,* Circolazione e mutazione dei modelli giuridici, In Digesto delle discipline privatistiche, sez. civ., II. Torino: UTET, 365, 1988.
35. *Sacco R.,* Introduzione al diritto comparato. Fifth ed., in Trattato di diritto comparato, Torino: UTET, 1992.
36. *Santoni G*., Personal Data as a Market Commodity: Legal Irritants from China's Experience, European Journal of Privacy Law and Technology 1, 2023.
37. *Stanzione P.,* Sui metodi del diritto comparato, Introduzione a *Ancel M.,* Utilità e metodi del diritto comparato, trad. it., Camerino, 1974.
38. United States Code, Title 18, Chapter 7, Title 47 § 223.

39. *Verbiest T., Spindler G., Riccio G. M.,* Study on the Liability of Internet Intermediaries. European Commission, DG Internal Market. SSRN: https://ssrn.com/abstract=2575069, 2002.
40. *Viola M., L. Heringer.,* Um olhar internacional: Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados, in Souza C.A., *Magrani E., Silva P.,* (eds.), Lei Geral de Proteção de Dados(LGPD): caderno especial, São Paulo, Thomson Reuter, 2019, 227.
41. *Voss W. G., Pernot-Leplay E.,* China Data Flows and Power in the Era of Chinese Big Tech, 44 Nw. J. Int'l L. & Bus. (2024) 1.
42. *Woll C., Artigas, J.* Big Tech's Influence in the EU: Lobbying and Digital Governance. European Journal of Political Research 61: 384, 2022.
43. *Zeno-Zencovich V.,* Comparison Involves Pluralism: A Rejected Viewpoint, Comparative Law Review 6, 2025.
44. *Zheng G.,* Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China, 43 Computer Law Security Rev. 105610, 2021.
45. Osborne v. Ohio, 495 U.S. 103, 1990.
46. Paris Adult Theatre I v. Slaton, 413 U.S. 49.

ენდრე გიოზო სზაბო*

მონაცემთა დაცვის საზედამხედველო ორგანოდან მონაცემთა დამუშავებისთვის პასუხისმგებელ პირამდე — გამოცდილება ევროსტატის ფარგლებში**

საზედამხედველო ორგანოს საქმიანობიდან მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის საკონსულტაციო საქმიანობაზე გადასვლა პასუხისმგებლობისა და პერსპექტივის შეცვლას გულისხმობს. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის კონსულტაციის გასაწევად, ზოგადი ცოდნის გარდა, სექტორული ცოდნაც საჭიროა. სხვა ექსპერტებთან ერთობლივი მუშაობა გადამწყვეტია მაღალი დონის კონსულტაციის გასაწევად, მაშინაც კი, თუ სავალდებულო არ არის, ექსპერტებს მნიშვნელოვანი როლი აკისრიათ ორგანიზაციაში მონაცემთა დაცვის კულტურის ჩამოყალიბების პროცესში, რომელიც მოიცავს მონაცემთა დაცვის შესახებ თანამშრომლების ცნობიერების ამაღლებას. ევროკავშირის მიერ 2024 წელს მნიშვნელოვანი ცვლილებები განხორციელდა ევროპული სტატისტიკის შესახებ რეგულაციაში. ბოლო წლებში აქცენტი გამოკითხვის მონაცემებიდან ადმინისტრაციულ მონაცემებსა და ახალ ტექნოლოგიებზე გადავიდა. ახალი ჩარჩოს თანახმად, კერძო მონაცემების მფლობელები ვალდებულნი არიან, უფასოდ მიაწოდონ მონაცემები ევროპული სტატისტიკის წარმოებისთვის. კერძო საკუთრებაში არსებული მონაცემების მოთხოვნისას სტატისტიკის ეროვნული ინსტიტუტებს და ევროსტატს შეუძლიათ პერსონალურ მონაცემებზე წვდომა მკაცრი პირობებით. ეს ზოგადი დებულება უნდა შეივსოს სექტორული საკანონმდებლო აქტით, რომელიც ჩამოთვლის პერსონალური მონაცემების

* სამართლის დოქტორი, სამართლებრივ საკითხთა და პოლიტიკის ოფიცერი და „ევროსტატის“ მონაცემთა დაცვის კოორდინატორი.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე“) წარდგენილი მოხსენების ტექსტს. სტატიაში გამოთქმული მოსაზრებები ეკუთვნის ავტორს და არ ასახავს ინსტიტუციის ოფიციალურ პოზიციას.

კატეგორიებს, რომლებზეც წვდომა შეიძლება. სტატისტიკური მიზნებისთვის პერსონალურ მონაცემებზე წვდომისა და დამუშავებისას როგორც "GDPR", ასევე "EU DPR" კვლავაც გამოიყენება. ნაშრომში ნათქვამია, რომ კონფიდენციალობის ექსპერტები მათი ორგანიზაციების განუყოფელი ნაწილია და ხელს უწყობენ მისიის წარმატებას. ისინი საჭიროების შემთხვევაში ოპტიმალურ, კანონიერ კორექტირებას გვთავაზობენ და ხელს უწყობენ მონაცემთა დაცვის კულტურის განვითარებას. ოფიციალური სტატისტიკის წარმოებისას შესაბამისობისა და ნდობის აღდგენის უზრუნველყოფა ფუნდამენტურია.

საკვანძო სიტყვები: *კონფიდენციალობის ექსპერტები, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო, სტატისტიკის ეროვნული ინსტიტუტები, სტატისტიკა, მონაცემთა დაცვის კულტურა, კერძო საკუთრებაში არსებული მონაცემები.*

1. შესავალი

ჩემთვის გაზაფხულის კონფერენცია არ არის მხოლოდ ღონისძიება მონაცემთა დაცვის შესახებ. მას განსაკუთრებული ადგილი უჭირავს ჩემს გულში, რადგან ყოველწლიურად ვესწრები შეხვედრებს. ასევე, მქონდა პატივი, ორჯერ მემასპინძლა გაზაფხულის კონფერენციისთვის ბუდაპეშტში, უნგრეთში: პირველად – 2016 წელს, შემდეგ კი – 2023 წელს. ეს უკანასკნელი მოვლენა ჩემი კარიერის პირველი ნახევრის დასასრულს მოხდა. 2023 წლის მაისში კვლავ ღონისძიების მასპინძელთა გუნდის წევრი ვიყავი, ხოლო იმავე წლის აგვისტოში ჩემი პროფესიული ცხოვრების ახალი თავი დავიწყე და შევუერთდი ევროკომისიას, კერძოდ კი, ევროკავშირის სტატისტიკის სამსახურს: ევროსტატს.[1]

მონაცემთა დაცვის საზედამხედველო ორგანოდან ("DPA")[2] მონაცემთა დამუშავებისთვის პასუხისმგებელ პირის პოზიციაზე გადასვლა არა მხოლოდ მნიშვნელოვანი წინგადადგმული ნაბიჯია ადამიანის კარიერაში, არამედ ღრმა გავლენას ახდენს მის ყოველდღიურ საქმიანობაზე. უფრო ზუსტად რომ

[1] „ევროსტატი" დაფუძნებულია ლუქსემბურგში, ის არის ევროკავშირის სტატისტიკის სამსახური და, ამავდროულად, ევროკომისიის გენერალური დირექტორატი. ლუქსემბურგის მონაცემთა დაცვის ეროვნულმა კომისიამ ("CNPD") გაზაფხულის კონფერენციას 2012 წელს უმასპინძლა.

[2] ავტორი თითქმის ოცი წლის განმავლობაში მუშაობდა უნგრეთის მონაცემთა დაცვის სამსახურში. 2006-2007 წლებში ის იყო პირველი მივლინებული ეროვნული ექსპერტი პერსონალურ მონაცემთა დაცვის ევროპელი ზედამხედველის ოფისში. 2012-2023 წლებში მას ეკავა უნგრეთის მონაცემთა დაცვისა და ინფორმაციის თავისუფლების უწყების ვიცე-პრეზიდენტის თანამდებობა.

ვთქვათ, ხედვა სრულიად იცვლება: საზედამხედველო ორგანო, როგორც წესი, მონაცემთა დამუშავების ოპერაციის კანონიერებას *ex post* აფასებს, მაშინ, როცა მონაცემთა დამმუშავებლის ორგანიზაციის შიგნით, პერსონალურ მონაცემთა დაცვის სპეციალისტი გადაწყვეტილების მიღების პროცესში მონაწილეობს დამუშავებისთვის პასუხისმგებელი პირისთვის რჩევის მიცემით. ეს პასუხისმგებლობის სრულიად განსხვავებული ფორმაა, რომელიც, მიუხედავად იმისა, რომ იმავე საფუძვლებს ეფუძნება, ფუნდამენტურად ცვლის საქმიანობის ლოგიკასა და დინამიკას.

ეს არის ჩემი პირადი გამოცდილება, რომელიც 2023 წლიდან გრძელდება. თბილისში, საქართველოში გამართულ გაზაფხულის კონფერენციას სწორედ ამ გამოცდილებით დავესწარი.

2. მზადება მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის რჩევის მისაცემად

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოში მუშაობა და ევროკავშირის "DPA"-ების (პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების) ქსელის წევრობა, ცხადია, შესანიშნავი გარემოა ექსპერტისთვის, სანამ ის მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთან დაიწყებს მუშაობას. მიუხედავად იმისა, რომ DPA-ში მომუშავე ექსპერტებს გააჩნიათ პერსონალურ მონაცემთა დაცვის შესახებ მყარი ჰორიზონტალური ცოდნა, ეს სულაც არ ნიშნავს, რომ მათ იცნობენ თითოეული კონკრეტული სფეროსთვის საჭირო სექტორულ სამართლებრივ ექსპერტიზას. აქედან გამომდინარე, აუცილებელია, გაეცნონ სექტორულ კანონმდებლობას და ასევე მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის „დნმ-ს". მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ფუნქციონირებისა და მახასიათებლების გაგების გარეშე მონაცემთა დაცვის ექსპერტი ვერ შეძლებს სასარგებლო რჩევების მიცემას კოლეგებისთვის, რომლებიც ხელმძღვანელობას საჭიროებენ.

სხვა კოლეგების მსგავსად, ჩემმა გამოცდილებამაც დაადასტურა, რამდენად მნიშვნელოვანია მსგავს სიტუაციაში მყოფი ექსპერტების ქსელის არსებობა. ეს მნიშვნელოვანია არა მხოლოდ მუშაობის პირველ ეტაპზე, არამედ მოგვიანებითაც, როდესაც საქმე რთულ შემთხვევებს ეხება, მაგალითად, ახალი ტექნოლოგიების გამოყენებას. კარგი ქსელი, რომელიც ექსპერტისთვის ხელმისაწვდომია, შეუცვლელია ყოველდღიური სამუშაოს ხარისხის უზრუნველსაყოფად.

3. თანამშრომლობა გუნდის წევრებთან მონაცემთა დაცვის კანონმდებლობის დასანერგად — მონაცემთა დაცვის კულტურის მშენებლობა

უმნიშვნელოვანესია, რომ თანამშრომლებმა კარგად იცოდნენ პერსონალურ მონაცემთა დაცვის წესები, რათა საჭირო დროს დროულად მიმართონ მონაცემთა დაცვის ექსპერტს რჩევისთვის. ჩემმა გამოცდილებამ ევროსტატთან დაადასტურა, რომ ეს სწორედ ასეა, რაც შემთხვევითი არ არის, რადგანაც სტატისტიკური კონფიდენციალობა სტატისტიკური სამსახურების ყოველდღიური მუშაობის ერთ-ერთი მთავარი პრინციპია. სტატისტიკური კონფიდენციალობა გულისხმობს სტატისტიკურ ერთეულებთან დაკავშირებული მონაცემების დაცვას, იქნება ეს კომპანიები თუ ფიზიკური პირები. შესაბამისად, მონაცემების დაცვა ზოგადად, სტატისტიკურ სამყაროში ბუნებრივი მოთხოვნაა. ჩემი გამოცდილებით, სტატისტიკის სფეროში მომუშავე კოლეგები ადვილად აიდენტიფიცირებენ მონაცემთა დაცვის თვალსაზრისით შესაბამის საკითხებსა და შეკითხვებს.[3]

სტატისტიკის სამსახურებში სიფრთხილის კულტურა ღრმადაა ფესვგადგმული, რადგანაც ისინი ყოველდღიურად აქვეყნებენ უზარმაზარ ინფორმაციას და კონფიდენციალური მონაცემების გამოქვეყნება ნებისმიერი გზით უნდა იქნას თავიდან აცილებული.

მონაცემთა დაცვის მოთხოვნების აღსრულება ყოველთვის პოპულარული არ არის, თუმცა, თუ კოლეგები კარგად არიან მომზადებულნი, ამ მოთხოვნებს კარგად იგებენ და ახორციელებენ. ასევე მნიშვნელოვანია, რომ მონაცემთა დაცვის კოორდინატორი ("DPC")[4] იყოს კონსტრუქციული, ეძებდეს ალტერნატივებსა და განხორციელებად გადაწყვეტილებებს. ეს როლი არ შეიძლება იყოს „ხელშეუხებელი სიმაღლიდან" მოქმედი პოზიცია, ვინაიდან DPC უფრო ფართო გუნდის ნაწილია და ორგანიზაციის წარმატებისთვის მუშაობს. ჩემთვის ბუდაპეშტის კონფერენციის ერთ-ერთი მთავარი გზავნილი იყო ანა პოლიუს ("EDPS"-ის 2024 წლის კანდიდატთა მოკლე სიაში შეყვანილი) ნათქვამი. ეს არ არის პირდაპირი ციტატა, თუმცა აზრს ზუსტად გადმოსცემს: პირადი ცხოვრების ხელშეუხებლობის სფეროში კარგ ექსპერტად გაქცევთ არა უარის თქმა, არამედ თქვენი უნარი, დაეხმაროთ ორგანიზაციას მიზნების მიღწევაში იმ გზით, რომელიც კანონიერი და პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობასთან თავსებადი იქნება.

კოლეგებთან რეგულარული თანამშრომლობა, ახალი თანამშრომლებისთვის ტრენინგების ჩატარება, მონაცემთა დამუშავებისთვის

[3] სტატისტიკური კონფიდენციალობა ნიშნავს „კონფიდენციალური მონაცემების დაცვას, რომლებიც ეხება ცალკეულ სტატისტიკურ ერთეულებს, მოპოვებულია უშუალოდ სტატისტიკური მიზნებისთვის ან არაპირდაპირი გზით ადმინისტრაციული თუ სხვა წყაროებიდან და გულისხმობს მოპოვებული მონაცემების არასტატისტიკური მიზნებისთვის გამოყენებისა და მათი უკანონო გამჟღავნების აკრძალვას" (Article 2 (1) e) რეგულაცია (EC) 223/2009 ევროპული სტატისტიკის შესახებ).

[4] ევროკომისიის ფარგლებში ყველა გენერალურ დირექტორატს ჰყავს მონაცემთა დაცვის კოორდინატორი ("DPC"), თავად კომისიას კი ჰყავს მონაცემთა დაცვის ოფიცერი ("DPO").

პასუხისმგებელი პირებისთვის დახმარების გაწევა მონაცემთა დაცვასთან დაკავშირებული საკითხების შეფასებისას – ეს ყველაფერი ხელს უწყობს ორგანიზაციაში მონაცემთა დაცვის კულტურის ჩამოყალიბებას. ეს კულტურა შეიძლება გარკვეული ხნით უხილავი იყოს, თუმცა კარგი მონაცემთა დაცვის კულტურის არსებობა აშკარად ხელშესახები გახდება შემთხვევებთან, განსაკუთრებით კი რთულ შემთხვევებთან მუშაობისას.

4. სტატისტიკის სამყარო — ძირითადი ცვლილებები ჩარჩო რეგულაციაში

ევროპული სტატისტიკის შესახებ ჩარჩო რეგულაციაში 2024 წელს მნიშვნელოვანი ცვლილება შევიდა. უპირველეს ყოვლისა, ცვლილების მთავარი მიზნებია სტატისტიკური მონაცემების წარმოების მისადაგება უახლეს მიღწევებთან და ახალი ტექნოლოგიებისა და მონაცემთა ახალი წყაროების კუთხით ხელმისაწვდომი რესურსების გამოყენება. ეს გულისხმობს ციფრული მონაცემების წყაროებისა და ახალი ტექნოლოგიების სრული პოტენციალის ათვისებას. გარდა ამისა, ცვლილებები მიზნად ისახავს სტატისტიკისა და ევროპული სტატისტიკური სისტემის[5] ფუნქციონირების გაუმჯობესებას, სხვა სიტყვებით რომ ვთქვათ, უფრო პროაქტიული და ეფექტიანი სტატისტიკის წარმოებას. დაბოლოს, ჩარჩო დაეხმარება სტატისტიკური პროდუქციის ინოვაციასა და ახალი სტატისტიკის შემუშავებას.

5. გადასვლა კვლევითი მონაცემებიდან ადმინისტრაციულ მონაცემთა წყაროებზე

ბოლო წლების განმავლობაში ჩვენ ვხედავთ აშკარა გადასვლას კვლევითი მონაცემებიდან სტატისტიკური პროდუქციისთვის გამოყენებულ ადმინისტრაციულ მონაცემებზე. შესაძლოა, ჯერ კიდევ შეგხვდეთ კვლევები, მაგალითად, შემოსავლისა და ცხოვრების პირობების სტატისტიკის (“SILC”) სფეროში, სადაც გამოიკითხებიან შერჩეული რესპონდენტები, მაგრამ სულ უფრო და უფრო მთავარი წყარო ხდება ადმინისტრაციული რეესტრები.

ტექნოლოგიური გარემოს ცვლილებისა და ინფორმაციის გაზიარების დაჩქარების გამო მუდმივად არსებობს სტატისტიკური წარმოების გამარტივების საჭიროება, რათა უზრუნველყოფილი იყოს უფრო დროული, უფრო ზუსტი და მაღალი ხარისხის სტატისტიკა.

[5] ევროპული სტატისტიკის შესახებ რეგულაციის (EC) 223/2009 მე-4 მუხლის თანახმად, „ევროპული სტატისტიკური სისტემა (ESS) არის პარტნიორობა თანამეგობრობის სტატისტიკურ ორგანოს, რომელიც არის კომისია (ევროსტატი), და ეროვნულ სტატისტიკურ ინსტიტუტებს (NSIs) და სხვა ეროვნულ ორგანოებს შორის, რომლებიც თითოეულ წევრ სახელმწიფოში პასუხისმგებელნი არიან ევროპული სტატისტიკის შემუშავებაზე, წარმოებასა და გავრცელებაზე.

6. კერძო საკუთრებაში არსებულ მონაცემებზე წვდომა

კერძო მონაცემთა მფლობელები ფლობენ განსაკუთრებით ღირებულ მონაცემთა ბაზებს, მაგალითად, მონაცემებს, რომლებიც ეხება საბანკო ბარათების გამოყენებას, სმარტ მრიცხველებს, მობილური ქსელის ოპერატორებს, ლოგისტიკურ კომპანიებს — და ეს მხოლოდ მცირე ჩამონათვალია.

შესწორებული ჩარჩო რეგულაციით, კერძო მონაცემთა მფლობელებს დაეკისრათ ახალი და ზოგადი ვალდებულება: მათ მოეთხოვებათ, უსასყიდლოდ გახადონ ხელმისაწვდომი მონაცემები და შესაბამისი მეტამონაცემები, თუ ეს მონაცემები აუცილებელია ევროპული სტატისტიკის შემუშავების, წარმოებისა და გავრცელებისთვის და მათი მოპოვება სხვა გზით შეუძლებელია, ან ალტერნატიულად, კერძო მფლობელობაში არსებული მონაცემების ხელახალი გამოყენება არსებითად შეამცირებს რესპონდენტთა ტვირთს.[6] ეს უზარმაზარი ცვლილებაა სტატისტიკურ წარმოებაში და დიდი ხნის ნანატრი შანსი, უკეთესად მოემსახურონ გადაწყვეტილების მიმღებ პირებს დროული და მაღალი ხარისხის სტატისტიკით, რაც ევროპული სტატისტიკისა და ზოგადად სტატისტიკის საბოლოო მიზანია.

7. პერსონალურ მონაცემებზე წვდომა (კერძო საკუთრებაში)

კანონმდებლებმა ეროვნული სტატისტიკური ინსტიტუტები და ევროსტატი აღჭურვეს ახალი და ძლიერი უფლებებით, რაც იმას ნიშნავს, რომ მათ მკაცრი პირობებით შეუძლიათ ჰქონდეთ წვდომა კერძო მფლობელობაში არსებულ მონაცემებს შორის არსებულ პერსონალურ მონაცემებზე. მონაცემების მოთხოვნისას ზოგადად მოქმედებს მონაცემთა მინიმიზაციისა და პროპორციულობის პრინციპი. ამ პრინციპების შესაბამისად, მონაცემებზე წვდომისას, როგორც მთავარი წესი, მხოლოდ არაპერსონალური მონაცემების მოთხოვნაა შესაძლებელი.

პერსონალური მონაცემების ჩამონათვალი გარკვეულ გარემოებებში შეიძლება დაზუსტდეს სექტორულ კანონმდებლობაში. ეს ნიშნავს, რომ ევროპული სტატისტიკის შესახებ შესწორებული ჩარჩო კანონმდებლობა

[6] ევროპული სტატისტიკის შესახებ (EC) 223/2009 რეგულაციის მე-17b მუხლის პირველი პუნქტის თანახმად, „...ეროვნული სტატისტიკის სამსახური (NSI) ან კომისია (ევროსტატი) უფლებამოსილია, კერძო მონაცემთა მფლობელისგან მოითხოვოს მონაცემებისა და შესაბამისი მეტამონაცემების უსასყიდლოდ ხელმისაწვდომობა, იმ შემთხვევაში, თუ მოთხოვნილი მონაცემები მკაცრად აუცილებელია ევროპული სტატისტიკის შემუშავების, წარმოებისა და გავრცელებისთვის და სხვა საშუალებებით მათი მოპოვება შეუძლებელია, ან თუ მათი ხელახალი გამოყენება მნიშვნელოვნად შეამცირებს საპასუხო ტვირთს მონაცემთა მფლობელებისა და სხვა ბიზნეს სუბიექტებისთვის. მონაცემთა ასეთი შეგროვება ან მონაცემებზე წვდომა კომისიამ შესაძლოა შეიტანოს ყოველწლიურ სამუშაო პროგრამაში“.

თავისთავად არ არის საკმარისი საფუძველი პერსონალური მონაცემების მოთხოვნისთვის. ის უნდა იყოს დამატებული და დაზუსტებული სხვა საკანონმდებლო აქტით.

ევროკავშირის შრომის ბაზრის სტატისტიკის შესახებ რეგულაცია ბიზნესის ჭრილში ("LMB")[7] არის პირველი სექტორული კანონმდებლობა, რომელიც ევროპული სტატისტიკის შესახებ რეგულაციის 2024 წელს შესწორების შემდეგ იქნა მიღებული. ეს რეგულაცია განსაზღვრავს, რომ ნებისმიერი ასეთი მოთხოვნა უნდა შემოიფარგლოს მხოლოდ იმ პერსონალური მონაცემების კატეგორიებით, რომლებიც აღნიშნულ რეგულაციაში მითითებულ სფეროებსა და თემებს განეკუთვნება.[8] ეს დებულება ასევე აწესებს პერსონალური მონაცემების ლიმიტებს, რომლებიც შეიძლება მოთხოვნილ იქნას კერძო მონაცემთა მფლობელებისგან.

ვინაიდან ეს წესები ჯერ კიდევ ახალია და, შესაბამისად, ამ ესეში არ არის წარმოდგენილი გამოყენების შემთხვევები, ჩვენ უნდა შემოვიფარგლოთ არსებული წესების ანალიზით და დაველოდოთ მათ სამომავლო იმპლემენტაციას. მონაცემებზე წვდომის შემთხვევაში, რა თქმა უნდა, მოქმედებს მთელი მონაცემთა დაცვის რეჟიმი: წევრ სახელმწიფოებში ეს არის "GDPR",[9] ხოლო ევროკავშირის დონეზე, ევროსტატისთვის, ეს არის ე.წ. "EUDPR".[10] თითოეული ეროვნული სტატისტიკური ინსტიტუტის მონაცემთა დაცვის ოფიცრები და ევროსტატის მონაცემთა დაცვის კოორდინატორი თვალს მიადევნებენ ამ მოთხოვნებს და საჭიროების შემთხვევაში ხელმისაწვდომი იქნებიან რჩევებისთვის თავიანთი შესაბამისი მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის.

მონაცემებზე წვდომა ყოველთვის ემყარებოდა სტატისტიკურ სამსახურებსა და მონაცემთა მფლობელებს შორის მჭიდრო თანამშრომლობას, რათა მაქსიმალურად შემცირებულიყო რესპონდენტთა ტვირთი. ეს მოსალოდნელია შესწორებული ჩარჩოს ფარგლებშიც და, მონაცემებსა და პერსონალურ მონაცემებზე წვდომის შეზღუდვების

[7] რეგულაცია (EU) 2025/941 ევროპარლამენტისა და საბჭოსი, რომელიც ეხება ევროკავშირის შრომის ბაზრის სტატისტიკას ბიზნესის ჭრილში, ამოქმედდება 2026 წლის პირველი იანვრიდან.

[8] უფრო კონკრეტულად, იმ მონაცემების ჩამონათვალი, რომელთა მოთხოვნაც შესაძლებელია, მოცემულია რეგულაციის მე-4 მუხლში. მე-3 მუხლის მე-3 პუნქტის თანახმად, „მოთხოვნა უნდა შემოიფარგლოს პერსონალური მონაცემების იმ კატეგორიებით, რომლებიც განეკუთვნება ამ რეგულაციის მე-4 მუხლში მითითებულ სფეროებსა და თემებს".

[9] რეგულაცია (EU) 2016/679 ევროპარლამენტისა და საბჭოსი, 2016 წლის 27 აპრილის, ფიზიკური პირების დაცვის შესახებ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით და ამგვარი მონაცემების თავისუფალი გადაადგილების შესახებ, რომლითაც უქმდება დირექტივა 95/46/EC (პერსონალურ მონაცემთა დაცვის ზოგადი რეგულაცია).

[10] რეგულაცია (EU) 2018/1725 ევროპარლამენტისა და საბჭოსი, 2018 წლის 23 ოქტომბრის, ფიზიკური პირების დაცვის შესახებ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით კავშირის ინსტიტუტების, ორგანოების, ოფისებისა და სააგენტოების მიერ და ამგვარი მონაცემების თავისუფალი გადაადგილების შესახებ, რომლითაც უქმდება რეგულაცია (EC) № 45/2001 და გადაწყვეტილება № 1247/2002/EC.

გამოყენების გარდა, მონაცემთა მფლობელებთან კარგი თანამშრომლობის შენარჩუნება ახალი წესების დანერგვის ქვაკუთხედად დარჩება.

სტატისტიკური ორგანოებისთვის სტატისტიკური კონფიდენციალურობა მხოლოდ შესაბამისობის ასპექტი არ არის. ისინი ახორციელებენ ყველა საჭირო ტექნიკურ და ადმინისტრაციულ ზომას კონფიდენციალური მონაცემების, მათ შორის პერსონალური მონაცემების, დაცვის უზრუნველსაყოფად. შესაბამისობის გარდა, ეს ასევე არის რესპონდენტების მიმართ ნდობის მშენებლობის ნაწილი.

ეს მოსაზრება მახსენებს ჯოვანი ბუტარელის, ევროპის მონაცემთა დაცვის გარდაცვლილ ზედამხედველს, და მის დასამახსოვრებელ განცხადებას. 2018 წელს ბრიუსელში, ევროპარლამენტის შენობაში, გამართულ გლობალური პირადი ცხოვრების ხელშეუხებლობის ასამბლეაზე ჯოვანი ბუტარელიმ თქვა: „ჩემთვის კანონთან შესაბამისობა საკმარისი არ არის".[11] ეს ძალიან ზუსტი და აქტუალურია ოფიციალური სტატისტიკის წარმოების კონტექსტში. შესაბამისობისა და შესაბამისობის დემონსტრირების გარდა, ნდობის მშენებლობა სტატისტიკური ინსტიტუტებისთვის მნიშვნელოვან ამოცანად რჩება.

8. დასკვნა

ზემოხსენებული ანალიზისა და ჩემს ახალ თანამდებობაზე მიღებული გამოცდილებიდან გამომდინარე, რამდენიმე დასკვნის გამოტანა შეიძლება. პირველ რიგში, პირადი ცხოვრების ხელშეუხებლობის პროფესიონალები გარეშე პირები კი არა, შიდა თანამშრომლები არიან. ისინი ორგანიზაციის განუყოფელ ნაწილს წარმოადგენენ და შეუძლიათ წვლილი შეიტანონ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების ძირითადი მისიის წარმატებაში.

მეორეც, პირადი ცხოვრების ხელშეუხებლობის პროფესიონალები ხელმისაწვდომნი უნდა იყვნენ, რათა საჭიროების შემთხვევაში შესთავაზონ ოპტიმალური და კანონიერი გადაწყვეტილებები, იმის ნაცვლად, რომ უბრალოდ არ ურჩიონ ან გამორიცხონ შესაძლო გადაწყვეტილებები. მათ შეძლებისდაგვარად კონსტრუქციული პოზიცია უნდა დაიკავონ, რათა დაეხმარონ თავიანთ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ძირითადი მიზნების მიღწევაში. წარმატების შემთხვევაში ეს სამუშაო ორგანიზაციაში მონაცემთა დაცვის კულტურის ჩამოყალიბებასთან ერთად წარიმართება.

დაბოლოს, პირადი ცხოვრების ხელშეუხებლობის სფეროს პროფესიონალებს შეუძლიათ, წვლილი შეიტანონ ნდობის მოპოვებაში შესაბამისობის უზრუნველყოფითა და დემონსტრირებით და, ამავდროულად,

[11] გამოსვლა ხელმისაწვდომია ონლაინ <https://www.youtube.com/watch?v=2gG1kY0L3a0>.

თავიანთი დამსაქმებლების ერთგვარ ელჩებად მოგვევლინონ გარე სამყაროსთან.

ბიბლიოგრაფია:

1. Regulation (EC) No 223/2009 on European Statistics “The European Statistical System (ESS)“.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
3. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
4. Regulation (EU) 2025/941 of the European Parliament and of the Council of 7 May 2025 on European Union labour market statistics on businesses is applicable from 1 January 2026.
5. Buttarelli G., Speech: Choose Humanity: Putting Dignity back into Digital, speech by Giovanni Buttarelli <https://www.youtube.com/watch?v=2gG1kY0L3a0>.

იულია სზიკლეი[*]

ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცე ("EHDS")[**]

„ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცის ("EHDS") შესახებ" რეგულაცია მიღებულია 2025 წლის 11 თებერვალს, სრულად კი 2031 წლის 26 მარტიდან ამოქმედდება. რეგულაციას ორმაგი მიზანი აქვს: პირველი, პაციენტებისთვის ჯანდაცვის კონტექსტში მათ პერსონალურ ჯანმრთელობასთან დაკავშირებულ ელექტრონულ მონაცემებზე წვდომისა და მათი კონტროლის გაუმჯობესება და მეორე, საზოგადოებისთვის სასარგებლო სხვა მიზნების უკეთ მიღწევა, როგორებიცაა: კვლევის, პაციენტთა უსაფრთხოების, პერსონალიზებული მედიცინის, ჯანმრთელობის საფრთხეების (მათ შორის, პანდემიების), ინოვაციების, პოლიტიკის შემუშავების, ოფიციალური სტატისტიკის ან მარეგულირებელი საქმიანობის მხარდაჭერა. "EHDS" არის ევროკავშირის პირველი საერთო მონაცემთა სივრცე, რომელიც მრავალ დაპირებას, მოლოდინსა და გამოწვევას გულისხმობს.

საკვანძო სიტყვები: *ჯანმრთელობასთან დაკავშირებული მონაცემთა ევროპული სივრცე, "EHDS", ჯანმრთელობასთან დაკავშირებული მონაცემები, მონაცემთა კანონი.*

1. შესავალი

ევროპარლამენტისა და ევროსაბჭოს 2025 წლის 11 თებერვლის რეგულაცია (EU) 2025/327 ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცის შესახებ, რომლითაც ცვლილება შედის 2011/24/EU

[*] უნგრეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ("NAIH") საერთაშორისო ურთიერთობების ვიცე-პრეზიდენტი.

[**] ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე") წარდგენილი მოხსენების ტექსტს.

დირექტივასა და (EU) 2024/2847 რეგულაციაში (“EHDS” რეგულაცია), მიზნად ისახავს ევროკავშირის ფარგლებში ჯანმრთელობის შესახებ ინფორმაციის გაცვლისა და მასზე ხელმისაწვდომობის ოპტიმიზაციას.

ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცე (“EHDS”) წარმოადგენს ევროკავშირის პირველ საერთო მონაცემთა სივრცის ინიციატივას, რომელიც ევროპული მონაცემთა სტრატეგიის ნაწილია და მიზნად ისახავს მონაცემებზე დაფუძნებული ეკონომიკის საჭიროებების დაკმაყოფილებას. მისი მიზანია მონაცემების უსაფრთხო და სანდო გამოყენებისა და გაზიარების ხელშეწყობა 14 ძირითად სექტორში, რომელთა შორისაა: სოფლის მეურნეობა, ენერგეტიკა, ტრანსპორტი და ფინანსები. ოფიციალური განცხადების თანახმად, *„ევროკავშირი გახდება მიმზიდველი, უსაფრთხო და დინამიკური მონაცემთა ეკონომიკა მონაცემებზე წვდომისა და მათი ხელახალი გამოყენების შესახებ მკაფიო და სამართლიანი წესების დადგენით; მონაცემების შესანახად და დასამუშავებლად შემდეგი თაობის ხელსაწყოებსა და ინფრასტრუქტურებში ინვესტირებით; ევროპული ღრუბლოვანი სიმძლავრეების გაერთიანებით; საკვანძო სექტორებში ევროპული მონაცემების საერთო და ურთიერთშეთავსებადი მონაცემთა სივრცეებში გაერთიანებით და მომხმარებლებისთვის მათი მონაცემების სრულად გასაკონტროლებლად უფლებების, ხელსაწყოებისა და უნარების მინიჭებით.“*[1]

საჯარო სექტორის სუბიექტების მიერ დამუშავებული (შენახული) პერსონალური მონაცემების (ხელახალი) გამოყენება დასაშვებია მხოლოდ ევროკავშირის მონაცემთა კანონმდებლობით დადგენილი მკაცრი გარანტიების პირობებში. აღნიშნული კანონმდებლობა მიჰყვება „წვდომაზე დაფუძნებულ“ მიდგომას, რომლის მაგალითებია ჰორიზონტალური რეგულაციები, როგორებიცაა: მონაცემთა მმართველობის აქტი (“DGA”), მონაცემთა აქტი (“DA”) და საჯარო სექტორის ინფორმაციის დირექტივა (“PSI”). ანონიმიზაცია არის ზოგადი წესი, ხოლო ხელახალი იდენტიფიცირება კანონით პირდაპირ აკრძალულია. გარდა ამისა, დაინერგა ახალი წესები, რომლებიც ეხება არაპერსონალურ მონაცემებს და იურიდიული პირების ინტერესების დაცვას. “DGA”-ის მიხედვით, მონაცემთა შუამავლობის ნეიტრალური სერვისები მიზნად ისახავს მონაცემთა სუბიექტებს, მონაცემთა მფლობელებსა და მომხმარებლებს (მოგებაზე ორიენტირებული) შორის კომერციული ურთიერთობების ხელშეწყობას. ამასთანავე, ალტრუისტული, მონაცემთა გაზიარების ორგანიზაციები, რომლებიც დანახარჯების ანაზღაურებისა და არაკომერციულობის პრინციპით მოქმედებენ, მხარს უჭერენ საჯარო ინტერესის მიზნებისთვის პერსონალური და არაპერსონალური მონაცემების ნებაყოფლობით, უსასყიდლო გაზიარებას.

[1] ევროკომისია, ევროპული მონაცემთა სტრატეგია, ევროკავშირის გადაქცევა მონაცემებით გაძლიერებული საზოგადოების სამაგალითო მოდელად, <commission.europa.eu/strategy-and-policy/priorities-2019-2024> [25.06.2025].

თუმცა, ევროკავშირის უკვე არსებული ჰორიზონტალური კანონმდებლობის დაცვით, "EHDS"-ი აწესებს ახალ, სექტორულ და *lex specialis* წესებს.

2. ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცე ("EHDS") ორმაგი მიზნები

1. პირველადი მონაცემების გამოყენება: პაციენტებს განუმტკიცდებათ მონაცემთა დაცვის უფლებები, კერძოდ, წვდომის, მონაცემთა პორტირების და მათ პერსონალურ ჯანმრთელობასთან დაკავშირებულ ელექტრონულ მონაცემებზე კონტროლის უფლება. ეს მოიცავს:

- ჯანმრთელობის შესახებ ინფორმაციის დამატებას;
- კონკრეტულ ნაწილებზე ან პირებზე წვდომის შეზღუდვას;
- წვდომის ისტორიის ნახვას;
- შეცდომების შემთხვევაში შესწორების მოთხოვნას;
- ჯანმრთელობის შესახებ მონაცემებზე სტანდარტიზებული ევროპული ფორმატით წვდომას.

2. მონაცემების მეორადი გამოყენება: ჯანმრთელობასთან დაკავშირებული ელექტრონული მონაცემები ასევე შეიძლება გამოყენებულ იქნას უფრო ფართო საზოგადოებრივი მიზნებისთვის, როგორებიცაა:

- კვლევა და ინოვაცია;
- პოლიტიკის შემუშავება;
- საზოგადოებრივი ჯანდაცვისთვის მზადყოფნა და რეაგირება (პანდემიების ჩათვლით);
- ოფიციალური სტატისტიკა;
- მარეგულირებელი საქმიანობა;
- პაციენტთა უსაფრთხოება;
- პერსონალიზებული მედიცინა.

3. განხორციელების ვადები

2027 წელი:

- წევრმა სახელმწიფოებმა უნდა შექმნან ციფრული ჯანმრთელობისა და ჯანმრთელობაზე წვდომის დაწესებულებები და ეროვნული საკონტაქტო პუნქტები.

2029 წელი:

- "EHDS"-ის ძირითადი სერვისები უნდა იყოს ოპერატიული;
- პაციენტებს უნდა ჰქონდეთ წვდომა მონაცემთა პირველ სამ კატეგორიაზე (სამედიცინო ისტორია, ელექტრონული რეცეპტები, ელექტრონული გაცემა).

- ელექტრონული ჯანმრთელობის ჩანაწერების ("EHR") სისტემები უნდა შეესაბამებოდეს "EHDS"-ის სპეციფიკაციებს;
- მომხმარებლებს შეუძლიათ გარკვეული კატეგორიებისთვის განაცხადების წარდგენა;
- მონაცემთა მფლობელებმა უნდა წარუდგინონ მონაცემთა ნაკრებების აღწერილობა წვდომის მიმნიჭებელ ორგანოს.

2031 წელი:

- "EHDS"-ის ყველა სერვისი სრულად ოპერატიული უნდა იყოს;
- პაციენტებს უნდა ჰქონდეთ წვდომა მათ ყველა მონაცემზე;
- ბაზარზე არსებული "EHR" სისტემები უნდა შეესაბამებოდეს "EHDS"-ის სპეციფიკაციებს ყველა კატეგორიაში;
- მონაცემთა მომხმარებლებს შეუძლიათ განაცხადი წარადგინონ მონაცემთა ყველა კატეგორიაზე;
- მონაცემთა მფლობელებმა უნდა უზრუნველყონ მონაცემთა ნაკრებების აღწერილობა.

4. ევროკავშირის არაწევრი ქვეყნები

პრეამბულის 35-ე პუნქტის თანახმად, ჯანმრთელობასთან დაკავშირებული მონაცემების ევროპული სივრცე ("EHDS") ასევე მხარს უჭერს ჯანმრთელობის შესახებ ელექტრონული მონაცემების გაცვლას შესაბამისი მესამე ქვეყნების ციფრული ჯანმრთელობის ეროვნულ საკონტაქტო პუნქტებსა და საერთაშორისო ორგანიზაციების მიერ საერთაშორისო დონეზე შექმნილ სისტემებთან, რათა ხელი შეეწყოს ჯანდაცვის უწყვეტობას. ეს განსაკუთრებით აქტუალურია იმ პირებისთვის, რომლებიც მეზობელ ევროკავშირის არაწევრ ქვეყნებში, კანდიდატ ქვეყნებსა და ასოცირებულ ზღვისიქითა ქვეყნებსა და ტერიტორიებზე მოგზაურობენ. მესამე ქვეყნების ციფრული ჯანდაცვის ასეთი ეროვნული საკონტაქტო პუნქტების "MyHealth@EU"-სთან დაკავშირება და საერთაშორისო ორგანიზაციების მიერ საერთაშორისო დონეზე შექმნილ ციფრულ სისტემებთან მათი ურთიერთთავსებადობა უნდა დაექვემდებაროს ევროკომისიის მიერ შესაბამისობის შემოწმებას, რომელიც უზრუნველყოფს აღნიშნული საკონტაქტო პუნქტებისა და ციფრული სისტემების შესაბამისობას "MyHealth@EU"-ს ტექნიკურ სპეციფიკაციებთან, მონაცემთა დაცვის წესებთან და სხვა მოთხოვნებთან. გარდა ამისა, იმის გათვალისწინებით, რომ "MyHealth@EU"-სთან დაკავშირება გულისხმობს პერსონალური ელექტრონული ჯანმრთელობის მონაცემების მესამე ქვეყნებში გადაცემას, მაგალითად, პაციენტის შემაჯამებელი დოკუმენტის გაზიარებას, როდესაც პაციენტი აღნიშნულ მესამე ქვეყანაში სამედიცინო დახმარებას ითხოვს, (EU)

2016/679 რეგულაციის V თავის შესაბამისად, უნდა დაინერგოს გადაცემის შესაბამისი ინსტრუმენტები. კომისია უფლებამოსილი უნდა იყოს, მიიღოს იმპლემენტაციის ხელშეწყობის მიზნით აქტები, რათა ხელი შეუწყოს ასეთი მესამე ქვეყნების ციფრული ჯანმრთელობის ეროვნული საკონტაქტო პუნქტებისა და საერთაშორისო ორგანიზაციების მიერ საერთაშორისო დონეზე შექმნილი სისტემების "MyHealth@EU"-სთან დაკავშირებას. აღნიშნული აქტების მომზადებისას კომისიამ უნდა გაითვალისწინოს წევრი სახელმწიფოების ეროვნული უსაფრთხოების ინტერესები.

მეორადი გამოყენებისთვის, "HealthData@EU"-ს შეფასებისა და მასთან შეერთების შემდეგ, წვდომა ხელმისაწვდომი იქნება მხოლოდ 2035 წლიდან.

5. მონაცემთა კატეგორიები და წყაროები

ჯანდაცვის სისტემიდან:

- მიღება-გაწერის დოკუმენტაცია, სამედიცინო ჩანაწერები, რეფერალები;
- ბიოლოგიური ნიმუშები, გამოსახულებები, სენსორული და მეტამონაცემები;
- რეცეპტები, პროგნოზული/პერსონალიზებული მედიცინის მონაცემები;
- მონიტორინგისა და კონტროლის მონაცემები.

მკვლევარებისა და ინდუსტრიისგან:

- მონაცემთა აგრეგირებული ბაზების ანალიზი;
- საძიებო მონაცემთა ნაკრებები;
- შემთხვევის კვლევები, ბიოლოგიური ნიმუშების ანალიზი.

6. უარის თქმის უფლებები

გარდა იმ შემთხვევებისა, როდესაც სასიცოცხლო ინტერესების დაცვაა საჭირო, წევრ სახელმწიფოებს შეუძლიათ პაციენტებს მისცენ უფლება, უარი თქვან მონაცემებზე წვდომაზე:

- ჯანდაცვის პროფესიონალების მიერ (პირველადი გამოყენება);
- ან მონაცემთა შემდგომ ხელახალ გამოყენებაზე (მეორადი გამოყენება).

თუმცა საზოგადოებრივი ინტერესების, პოლიტიკის შემუშავების, სტატისტიკური და კვლევითი მიზნებისთვის მონაცემებზე წვდომა გამორიცხულია უარის თქმის ოფციებიდან.

7. აკრძალული მეორადი გამოყენება

"EHDS" რეგულაციის 54-ე მუხლის თანახმად, ჯანმრთელობის მონაცემების მომხმარებლებს შეუძლიათ მონაცემების დამუშავება მხოლოდ იმ მიზნებისთვის, რომლებიც ავტორიზებულია:

- მონაცემთა დამუშავებაზე ნებართვის 68-ე მუხლის შესაბამისად;
- მონაცემთა დამტკიცებულ განაცხადში 69-ე მუხლის შესაბამისად;
- 67-ე მუხლის (3) პუნქტით გათვალისწინებულ კონკრეტულ შემთხვევებში ან 75-ე მუხლით გათვალისწინებული დამტკიცების საფუძველზე.

აკრძალულია მონაცემების გამოყენება:

- ელექტრონულ ჯანმრთელობის მონაცემებზე დაფუძნებული არახელსაყრელი გადაწყვეტილებების მისაღებად (მაგალითად, სამართლებრივი, ეკონომიკური ან სოციალური ზეგავლენით);
- დასაქმებასთან ან მომსახურებასთან დაკავშირებული დისკრიმინაციისთვის (მაგალითად, დაზღვევის, კრედიტის გამორიცხვები);
- რეკლამირებისა და მარკეტინგისთვის;
- მავნე ან დამოკიდებულების გამომწვევი პროდუქტების შესაქმნელად (მაგალითად, ნარკოტიკები, ალკოჰოლი, თამბაქო, იარაღი);
- ეროვნული კანონმდებლობით განსაზღვრული ეთიკური ნორმების დამრღვევი საქმიანობისთვის.

8. "EHDS"- ის მმართველობის სტრუქტურა

ინფრასტრუქტურა მოიცავს:

- უკვე არსებულ MyHealth@EU და HealthData@EU ინფრასტრუქტურებს;
- ეროვნულ საკონტაქტო პუნქტებს;
- ციფრული ჯანმრთელობის ორგანოებს;
- მონაცემებზე წვდომის მიმნიჭებელ ორგანოებს (წვდომის ავტორიზაციის, შესაბამისობის ზედამხედველობის, სანქციების დაწესების, ორწლიანი ანგარიშგების მიზნით);
- ბაზრის ზედამხედველობის ორგანოებს (ელექტრონული ჯანმრთელობის ჩანაწერების სისტემებზე ზედამხედველობის მიზნით);
- "EHDS" საბჭოს (რომელიც შედგება თითოეული წევრი სახელმწიფოს ორი წარმომადგენლისგან: ერთი წარმომადგენელი პირველადი გამოყენების მიზნებისთვის და ერთი მეორადი გამოყენების მიზნებისთვის, რომლებსაც ნიშნავს თითოეული წევრი სახელმწიფო. თითოეულ წევრ სახელმწიფოს აქვს ერთი ხმა);
- მონაცემთა მფლობელებსა და მომხმარებლებს.

9. მონაცემთა დაცვისა და დამუშავების პრინციპები

მონაცემთა დამუშავების სტანდარტების მიზანია ადამიანის ფუნდამენტური უფლებების დაცვა და არა სექტორის სპეციფიკური სამართლებრივი ან პროფესიული პრაქტიკის შეცვლა ან შეფერხება. დამუშავება უნდა აკმაყოფილებდეს აუცილებლობისა და პროპორციულობის სტანდარტებს. მიზანმა უნდა გაამართლოს პირადი ცხოვრების ხელშეუხებლობაში შეჭრა. „უფრო ეფექტიანი მედიკამენტი" არ ამართლებს „უფრო ინვაზიური განვითარების მეთოდებს:"

- რისკზე დაფუძნებული მიდგომა: დაცვის დონეები უნდა შეესაბამებოდეს ინდივიდებისთვის არსებულ რისკებს;
- შესაბამისობა: თუ ძირითადი პროცესი არ შეესაბამება კანონს, მონაცემთა დამუშავება ვერ იქნება კანონთან შესაბამისობაში;
- პირველადი დამუშავება, როგორც წესი, მოიცავს პერსონალურ და იდენტიფიცირებად მონაცემებს;
- მეორადი დამუშვება საჭიროებს წვდომის დამტკიცებას და, როგორც წესი, მოიცავს ანონიმიზებულ ან ფსევდონიმიზებულ მონაცემებს;
- ანონიმიზაცია განიხილება, როგორც დამუშავება (რომელიც საჭიროებს კანონიერ საფუძველს), მაგრამ მისი დასრულების შემდეგ მონაცემები აღარ ითვლება პერსონალურ მონაცემებად და გამოდის GDPR-ის ფარგლებიდან.

მონაცემთა დაცვის ორგანოები უნდა იყვნენ ინფორმირებული ჯანმრთელობის მონაცემთა ორგანოების მიერ დაწესებული სანქციების და მეორადი მონაცემების დამუშავებასთან დაკავშირებული საკითხების შესახებ და მათ უნდა გააზიარონ შესაბამისი ინფორმაცია წესების აღსრულების უზრუნველსაყოფად.

10. დასკვნა

ევროპის ჯანმრთელობის მონაცემთა სივრცე ("EHDS") პირებს საშუალებას აძლევს, საზღვრებს მიღმა მოიპოვონ წვდომა, განახორციელონ კონტროლი და გააზიარონ ელექტრონული ფორმით არსებული საკუთარ ჯანმრთელობასთან დაკავშირებული მონაცემები, რაც აუმჯობესებს ჯანდაცვის უსაფრთხოებასა და პაციენტთა კომფორტს. იგი ასევე იძლევა ჯანმრთელობის მონაცემების უსაფრთხო ხელახალი გამოყენების შესაძლებლობას კვლევის, ინოვაციების, პოლიტიკის შემუშავებისა და მარეგულირებელი საქმიანობისთვის. ევროკომისიის ცნობით, ამან მომდევნო ათწლეულში ევროკავშირში შესაძლოა 11 მილიარდ ევრომდე დაზოგვა განაპირობოს.[2] ამასთანავე, "EHDS"-ი ხელს

[2] ევროკომისია, კითხვები და პასუხები - ევროკავშირის ჯანდაცვა: ევროპის ჯანდაცვის მონაცემთა სივრცე (EHDS) <ec.europa.eu/commission/presscorner> [25.06.2025].

უწყობს უსაფრთხო ელექტრონული ჯანმრთელობის ჩანაწერების სისტემების ერთიანი ბაზრის განვითარებას, რომლებიც ემსახურება როგორც პირველად, ისე მეორად გამოყენებას.

მეორე მხრივ, მისი სირთულისა და ზომის გამო, ახალი ინფრასტრუქტურები მნიშვნელოვნად ზრდის მონაცემთა დაცვის რისკებს სხვადასხვა საფრთხის სახით, მათ შორის კიბერთავდასხმების, ინსაიდერული საფრთხეების და მონაცემთა დარღვევების ჩათვლით. ყველა ამ საფრთხემ და ზიანმა შეიძლება გამოიწვიოს არასანქცირებული წვდომა, კონტროლის დაკარგვა და დიდი პოტენციური ზიანი ინდივიდებისთვის. აღნიშნული რისკები კიდევ უფრო რთულდება, ჯანმრთელობის მონაცემების მგრძნობიარე ბუნებიდან გამომდინარე.

ბიბლიოგრაფია:

1. European Commission, European Data Strategy, Making the EU a Role Model for a Society Empowered by Data, <commission.europa.eu/strategy-and-policy/priorities-2019-2024> [25.06.2025].
2. European Commission, Questions and answers - EU Health: European Health Data Space (EHDS), <ec.europa.eu/commission/presscorner> [25.06.2025].

თამარ სამნიაშვილი*

მონაცემთა სუბიექტის თანხმობა, როგორც სამართლებრივი საფუძველი: თეორიული და პრაქტიკული ასპექტები

სტატიაში განხილულია მონაცემთა სუბიექტის თანხმობის ინსტიტუტი, როგორც პერსონალურ მონაცემთა დამუშავების სამართლებრივი საფუძველი. გაანალიზებულია თანხმობის კანონიერების კრიტერიუმები და მისი ფორმულირების თავისებურებები სამართლებრივ დოკუმენტებში, ხელშეკრულებებსა და ონლაინ სივრცეებში, გამჭვირვალობისა და ინფორმირებულობის პრინციპების დაცვის აუცილებლობის გათვალისწინებით.

სტატია ეფუძნება საქართველოს ეროვნული კანონმდებლობისა და საერთაშორისო სამართლის, განსაკუთრებით კი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”)[1] შედარებით ანალიზს. გამოკვეთილია თანხმობის ინსტიტუტის პრაქტიკაში რეალიზების ძირითადი გამოწვევები და რისკები. სტატიაში წარმოჩენილია თანხმობის ეფექტური გამოყენებისთვის საჭირო კრიტერიუმები, რომელთა პრაქტიკაში დანერგვა და რეალიზებაც ხელს უწყობს მონაცემთა დაცვის კულტურის განვითარებასა და საზოგადოების ნდობის გამყარებას როგორც კერძო, ისე საჯარო სექტორში.

საკვანძო სიტყვები: *პერსონალური მონაცემები, განსაკუთრებული კატეგორიის მონაცემები, არასრულწლოვნის პერსონალური მონაცემები, თანხმობა, არასრულწლოვნის თანხმობა, თანხმობის გამოხმობის უფლება, თანხმობა ხელშეკრულებაში, თანხმობა ონლაინ სივრცეში, მზა ჩანაწერები („cookie ფაილები“), „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”).*

---

* ილიას სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი, სსიპ - საქართველოს ეროვნული არქივის პერსონალურ მონაცემთა დაცვის ოფიცერი.

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

1. შესავალი

მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავების თაობაზე „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით გათვალისწინებულ ერთ-ერთ სამართლებრივ საფუძველს წარმოადგენს.[2] საკითხი, რომ მონაცემთა დამუშავებისათვის პასუხისმგებელ პირს მონაცემთა დამუშავებისათვის ესაჭიროება სამართლებრივი საფუძველი, სიახლეს არ წარმოადგენს. საზოგადოების სამართლებრივი ცნობიერების ზრდასთან ერთად, ერთი მხრივ, იზრდება მონაცემთა სუბიექტის მოლოდინები/მოთხოვნები და, მეორე მხრივ, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთა ვალდებულება, დაამუშაონ მონაცემები კანონშესაბამისად.

თანხმობა, როგორც პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი, პრაქტიკაში ერთ-ერთ ხშირად გამოყენებულ და აქტუალურ საკითხს წარმოადგენს. შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო თანხმობის საკითხზე მსჯელობისას აღნიშნავს, რომ ის, როგორც წესი, არც ყველაზე მარტივ და არც ყველაზე შესაბამის ალტერნატივას არ წარმოადგენს, მაგალითად, იმიტომ, რომ პირი, რომელიც თანხმობას გასცემს, უფლებამოსილია ნებისმიერ დროს გამოითხოვოს იგი.[3]

აღნიშნულ საფუძველს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები, უმეტეს შემთხვევაში, არსებული/დაგეგმილი პროცესების კანონთან შესაბამისობაში მოსაყვანად იყენებენ. კერძოდ, შემთხვევებში, როდესაც სახეზე არ არის მონაცემთა დამუშავების სხვა სამართლებრივი საფუძველი და, შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი პროცესისთვის საფუძვლის შექმნას თანხმობის მოპოვებით ახორციელებს. აღნიშნულ შემთხვევაში კი წარმოიქმნება რისკი, რომ თანხმობა იქცეს „უნივერსალურ ინსტრუმენტად", რომელიც პასუხისმგებელ პირებს საშუალებას მისცემს, პროცესები მხოლოდ ფორმალურად მოაქციოს სამართლებრივ ჩარჩოში. შესაბამისად, ყურადღების მიღმა არ უნდა დარჩეს ის რისკები, რომლებიც აღნიშნული საფუძვლის მოპოვებას და შემდგომში მის რეალიზებას შესაძლოა ახლდეს თან.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანო ("ICO") თანხმობის საკითხზე მსჯელობისას სარეკომენდაციო მითითებას იძლევა, რომლის თანახმადაც, კონკრეტულ პროცესში შერჩეულ უნდა იქნეს სამართლებრივი საფუძველი, რომელიც ყველაზე ზუსტად ასახავს დამუშავების მიზანსა და რეალურ ურთიერთობას სუბიექტთან. თუ თანხმობის მიღება რთულია, ხშირად ამის მიზეზი არის ის, რომ სხვა სამართლებრივი

[2] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", №3144-XIმს-Xმპ, 14/06/2023, მუხლი 5 (1) (ა).

[3] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 15, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

საფუძველი უფრო შესაფერისია და ამიტომ უნდა იქნეს განხილული ალტერნატივები.[4]

თანხმობის მნიშვნელობა კიდევ უფრო თვალსაჩინო ხდება თანამედროვე ციფრულ რეალობაში. ინტერნეტსერვისების, სოციალური ქსელების, მობილური აპლიკაციების და ციფრული მარკეტინგის ეპოქაში მონაცემთა დამუშავების უდიდესი ნაწილი სწორედ თანხმობის საფუძველს ეფუძნება. მომხმარებლები ყოველდღიურად აჭერენ ღილაკს „ვეთანხმები“, თუმცა რეალურად იშვიათად აქვთ დრო ან შესაძლებლობა, სრულად გაეცნონ, რას გულისხმობს ეს თანხმობა და რამდენად რეალურია მათი თავისუფალი არჩევანი. სწორედ ამიტომ ბოლო წლების განმავლობაში განსაკუთრებით გააქტიურდა დისკუსია „ფორმალური თანხმობის“ პრობლემასა და მის ეფექტიანობაზე.

პრაქტიკაში თანხმობის გამოყენება განსაკუთრებით აქტუალურია კერძო სექტორში, რომელშიც ის ხშირად დაკავშირებულია პირდაპირ მარკეტინგთან, დასაქმების პროცესებთან, სადაზღვევო და საბანკო მომსახურებასთან, განათლებისა და ჯანდაცვის სექტორში მონაცემთა დამუშავებასთან. საჯარო სექტორში თანხმობის გამოყენება შედარებით შეზღუდულია, ვინაიდან აღნიშნულ სექტორში მონაცემთა დამუშავება უმეტესად კანონით დადგენილ ვალდებულებებს ან საჯარო ინტერესს ეფუძნება. აღნიშნულ შემთხვევებში ნებაყოფლობითობის საკითხი განსაკუთრებით სენსიტიურია, რადგან მოქალაქე საჯარო უწყებასთან ურთიერთობისას ხშირად ვერ აღიქვამს თანხმობის თავისუფალ არჩევანს. სწორედ ამიტომ, უმრავლეს შემთხვევაში, „საჯარო დაწესებულებები ვერ დაეყრდნობიან მონაცემთა სუბიექტის თანხმობას, მონაცემთა სუბიექტსა და დამუშავებისთვის პასუხისმგებელ პირთა შორის ძალთა ბალანსის გათვალისწინებით.“[5]

სტატიის მიზანი არა მხოლოდ თანხმობის, როგორც მონაცემთა დამუშავების სამართლებრივი საფუძვლის, თეორიული ანალიზია, არამედ მისი პრაქტიკული მნიშვნელობის, მასთან დაკავშირებული რისკების და განვითარების პერსპექტივების გამოკვეთაა.

[4] *Information Commissioner's Office (ICO)* Guideline on *When is consent appropriate?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].

[5] პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა სუბიექტისგან თანხმობის მიღების“ შესახებ, 10.

2. პერსონალური მონაცემების დამუშავება თანხმობის საფუძველზე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ითვალისწინებს თანხმობის დეფინიციას და განსაზღვრავს მისი კანონიერად მიჩნევისთვის სავალდებულო კრიტერიუმებს:[6]

- **ინფორმაციის მიღების შემდეგ** - გაცემულ თანხმობას არ უნდა ჰქონდეს წინმსწრები ხასიათი, უნდა გაიცეს მას შემდეგ, რაც სუბიექტს მიეწოდა ინფორმაცია, თუ რის თაობაზე არის მოთხოვნილი თანხმობა. აღნიშნული, თავის მხრივ, უზრუნველყოფს რეალური არჩევანის შესაძლებლობას;
- **ინფორმირებულობა** - მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები უნდა დარწმუნდნენ, რომ იყენებენ გასაგებ და მარტივ ენას ინფორმირებისათვის. ტექსტი უნდა იყოს მარტივად გასაგები ნებისმიერი პირისათვის და არა მხოლოდ იურისტებისათვის, არ უნდა შეიცავდეს გრძელ, რთულად გასაგებ კონფიდენციალობის პოლიტიკებსა და წესებს, რომლებიც წარმოდგენილი იქნება მხოლოდ იურიდიული ტერმინებით;
- **კონკრეტული მიზანი** - აღნიშნული კრიტერიუმიც პირდაპირ უკავშირდება ინფორმირების მოთხოვნასთან. სუბიექტისათვის ცნობილი უნდა იყოს, კონკრეტულად რა მიზნით მუშავდება მისი მონაცემები და რაზე გასცემს შესაბამის თანხმობას;
- **აქტიური მოქმედება** - თანხმობა უნდა იყოს მონაცემთა სუბიექტის აქტიური ქმედებით დაფიქსირებული, რაც კონკრეტულ შემთხვევაში შესაძლოა გამოიხატოს თანხმობის თაობაზე წერილობითი ფორმის არსებობისას მონიშვნის გაკეთებით, ბმულზე გადასვლით, ზეპირი სახით თანხმობის განცხადებით ან სხვა შესაბამისი ფორმით;
- **თავისუფლება** - თანხმობის თავისუფალი ხასიათი გულისხმობს შესაძლებლობას, მონაცემთა სუბიექტმა დამოუკიდებლად, ზეწოლის გარეშე მიიღოს გადაწყვეტილება საკუთარი მონაცემების დამუშავების თაობაზე;
- **მკაფიოობა** - მონაცემთა სუბიექტის ნება კონკრეტული მონაცემების ასევე კონკრეტული დამუშავების თაობაზე უნდა იყოს მკაფიო და არ უნდა იწვევდეს ეჭვს მისი არსებობის საკითხი;
- **ფორმა** - წერილობით (მათ შორის ელექტრონულად) ან ზეპირად - ფორმის საკითხი ძირითადად დამოკიდებულია მონაცემთა კატეგორიაზე, რომლის დამუშავების შესახებაც გაიცემა შესაბამისი თანხმობა. კერძოდ, განსაკუთრებული კატეგორიის მონაცემთა შემთხვევაში მხოლოდ წერილობითი ფორმით არის შესაძლებელი

[6] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 3 (მ).

თანხმობის გაცხადება.[7] ასევე მსგავს, კონკრეტულ რეგულირებას ითვალისწინებს კანონი პირდაპირი მარკეტინგის განხორციელებისას სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მონაცემების გარდა სხვა მონაცემების დამუშავებისას.[8]

აღსანიშნავია, რომ თანხმობის მოთხოვნები ხშირად ქმნის მონაცემთა სუბიექტისთვის არჩევანის ილუზიას, მაშინ როდესაც სინამდვილეში ასეთი არჩევანის შესაძლებლობა არ არსებობს.[9] შესაბამისად, თანხმობის კანონიერების შეფასების ეტაპზე მნიშვნელოვანია, რომ ყველა ზემოთ ჩამოთვლილი კრიტერიუმი სრულად დაკმაყოფილდეს.

3. თანხმობა პრაქტიკაში

თანხმობა მონაცემთა დამუშავების საფუძვლად ძირითადად კერძო სექტორის შემთხვევაში გვხვდება. აღნიშნულის განმაპირობებელი ძირითადად ის ფაქტია, რომ, საჯარო სექტორის შემთხვევაში, მისი წარმომადგენლების მხრიდან მონაცემთა დამუშავებისას იშვიათ შემთხვევებში თუ არის შესაძლებელი წარმოვიდგინოთ კონკრეტული სიტუაცია, როდესაც თანხმობა მონაცემთა სუბიექტის მიერ არ აღიქმება იძულებითი ხასიათის მატარებლად როგორც პირდაპირი, ასევე ირიბი ხასიათის ზემოქმედებისა და მოსალოდნელი გავლენის გათვალისწინებით.

მსგავსი საფრთხე შესაძლოა არსებობდეს მონაცემთა სუბიექტის თანხმობის კანონიერებასთან დაკავშირებით, როდესაც სუბიექტი დასაქმებული პირია, ხოლო მონაცემთა დამუშავება დამსაქმებლის მიერ ხორციელდება. აღნიშნულ შემთხვევაშიც აშკარაა დაქვემდებარებული მდგომარეობა და, შესაბამისად, რეალური საფრთხე, რომ მონაცემთა სუბიექტის მიერ კონკრეტული პროცესი დაკავშირებული იქნება გარკვეულ ზეწოლასა და მის მიერ გაცხადებულ ნებაზე უარყოფით გავლენასა და დამოკიდებულებაზე.

თუმცა არ ნიშნავს, რომ დამსაქმებლები ვერასდროს დაეყრდნობიან თანხმობას, როგორც მონაცემთა დამუშავების სამართლებრივ საფუძველს. შესაძლოა არსებობდეს სიტუაციები, როდესაც დამსაქმებელი შეძლებს დაამტკიცოს, რომ თანხმობა მართლაც თავისუფლად არის გაცემული. დამსაქმებელსა და თანამშრომლებს შორის არსებული ძალაუფლების უთანასწორობის გამო, თანამშრომლები თავისუფალი ნების გამოვლენას მხოლოდ გამონაკლის შემთხვევებში შეძლებენ, მაშინ, როდესაც მათი

[7] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 6 (1)(ა).
[8] იქვე, მუხლი 12 (2).
[9] *Cate, F. H.* The Failure of Fair Information Practice Principles In *Consumer Protection in the Age of the Information Economy* 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].

თანხმობის გაცემა ან მასზე უარი ნამდვილად არ გამოიწვევს რაიმე უარყოფით შედეგს.[10]

დამუშავების საფუძვლად თანხმობის განსაზღვრისას მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს საკმაოდ მნიშვნელოვანი ბერკეტები აქვთ ხელთ, რომელთა კანონშეუსაბამო, ან „შეფარვითი“ ფორმულირებისასაც, შესაძლოა მოპოვებულ თანხმობას სამართლებრივი ძალა არ ჰქონდეს და შეფასებისას დადგინდეს, რომ დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა დამუშავების კონკრეტულ პროცესს რეალურად სამართლებრივი საფუძვლის გარეშე ახორციელებდა.

ასევე საყურადღებოა შემთხვევა, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი თანხმობას უთითებს დამუშავების საფუძვლად იმ კატეგორიის მონაცემებისათვის, რომლებიც ფაქტობრივად აუცილებელია გარიგების შესრულებისთვის. აღნიშნულ შემთხვევაში მიიჩნევა, რომ თანხმობა სწორი სამართლებრივი საფუძველი არ არის.[11]

რა თქმა უნდა, გამოირიცხება შემთხვევა, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტის თანხმობას მხოლოდ მოიაზრებს მის ისეთ ქმედებებში, როგორებიცაა: დუმილი, უმოქმედობა, წინასწარ განხორციელებული მონიშვნები, საწყისი პარამეტრებისა და წესებისა და პირობების ერთიანი მიღების შემთხვევები.

ხშირია მოსაზრება, რომ მონაცემთა დამუშავების სამართლებრივ საფუძვლად სუბიექტის თანხმობის მითითება საფრთხის შემცველი და რისკის მატარებელი შესაძლოა აღმოჩნდეს, აღნიშნული საფრთხეები კი შესაძლოა წარმოჩნდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ სრულყოფილი ინფორმირების მიუხედავად. ამერიკელი მონაცემთა დაცვის და კონფიდენციალობის ექსპერტი ფრედ ქეითი თავის ნაშრომში, „სამართლიანი ინფორმირების პრაქტიკული პრინციპების წარუმატებლობა“, ინფორმირების პრაქტიკაში რეალიზების სირთულეებს შორის გამოყოფს საზოგადოების მხრიდან იგნორს მიწოდებული კონფიდენციალობის პოლიტიკებისა და ინფორმაციის მიმართ.

ამასთან, მონაცემთა დაცვის რეგულაციების და მარეგულირებელი კანონმდებლობის კომპლექსურობის მატებასთან ერთად, რთულდება ასევე იმ შეტყობინებების შინაარსი, რომელთაც აღნიშნული რეგულირებები მოითხოვს.[12]

ასევე, მსგავს რისკებს განიხილავს მონაცემთა დაცვის ევროპული საბჭო (“EDPB”) სახელმძღვანელო რეკომენდაციაში თანხმობის შესახებ, რომელშიც

[10] *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018,7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].

[11] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 10, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[12] *Cate, F. H.* The Failure of Fair Information Practice Principles In *Consumer Protection in the Age of the Information Economy,* 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].

აღნიშნულია საფრთხის თაობაზე, როდესაც, მონაცემთა სუბიექტები მათი მხრიდან თანხმობის ხშირად გაცემის შედეგად, თანხმობის მოპოვების ფორმების გაცნობის გარეშე გამოხატავენ ნებას, როდესაც წარმოიქმნება რეალური რისკი მათთვის, რადგან, როგორც წესი, თანხმობა მოთხოვნილია ისეთი ქმედებებისთვის, რომლებიც შესაბამისი ნების გამოხატვის გარეშე კანონიერი არ იქნებოდა.[13]

აღნიშნული გარემოებები კი, თავის მხრივ, ზრდის თანხმობის კანონიერებასთან დაკავშირებულ რისკებს.

3.1. არასრულწლოვნის თანხმობა

არასრულწლოვნის მონაცემების კანონიერად დამუშავების საკითხის მნიშვნელობას მისი სპეციალური წესით რეგულირებაც მოწმობს. საქართველოს ეროვნული კანონმდებლობით, ისევე, როგორც საერთაშორისო სტანდარტებით, განსაკუთრებული ყურადღება ექცევა არასრულწლოვნის უფლებების დაცვას და მათი რეალიზების რეალური მექანიზმების დანერგვას. აღნიშნული კი, პირველ რიგში, თავად არასრულწლოვნის ბუნებრივი მახასიათებლებით არის განპირობებული. მათი მხრიდან საკითხის მნიშვნელობისა და რისკების შესაძლო არასრულყოფილი აღქმა, საუკეთესო ინტერესების სრულად შეუფასებლობა წარმოადგენს იმ გარემოებათა არასრულ ჩამონათვალს, რომლებიც განაპირობებს მათი უფლებების დაცვის მაღალ სტანდარტს.

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო ყურადღებას ამახვილებს ონლაინ სივრცეში არასრულწლოვანთა უფლებების დაცვის საკითხზე. ბავშვები და ახალგაზრდა პირები სწრაფად და პროფესიონალურად გადაადგილდებიან სხვადასხვა პლატფორმაზე, მაგრამ ეს ყოველთვის არ ნიშნავს, რომ ისინი აცნობიერებენ რისკებს ან სრულად ხვდებიან შედეგებს, რომლებიც შესაძლოა მომავალში გამოვლინდეს.[14]

არასრულწლოვნისგან თანხმობის მოპოვებისას მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს თანხმობის ტექსტის მარტივი, აღქმადი, ბავშვისთვის გასაგები ენით მიწოდება, საჭიროების შემთხვევაში დამატებითი ვიზუალური საშუალებების გამოყენებით.[15] აღნიშნული საშუალებების რამდენიმე მაგალითს განიხილავს ასევე მონაცემთა დაცვის კომისია (“Data Protection Commission”): ანიმაციები,

[13] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[14] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide,3, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

[15] *The Autoriteit Persoonsgegevens (AP)*, Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].

ვიდეოები, სურათები, გამოსახულებები, თამაშთან დაკავშირებული ნიშნები - მორგებული მომხმარებელთა ასაკობრივ ჯგუფზე, განხილულია არასრულწლოვანთათვის ინფორმირების ეფექტიან საშუალებად.[16]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ასევე განსაზღვრავს საკითხის რეგულირების სპეციალურ წესს, როდესაც საქმე ეხება არასრულწლოვნის განსაკუთრებული კატეგორიის მონაცემებს.[17] აღნიშნულ შემთხვევაში, გარდა არასრულწლოვანთან დაკავშირებული მაღალი რისკისა, დამატებით თავს იჩენს თავად მონაცემთა მახასიათებელი, რაც განაპირობებს დაცვის მაღალ სტანდარტს. კერძოდ, არასრულწლოვნის განსაკუთრებული კატეგორიის მონაცემთა დამუშავება კანონის შესაბამისად, შესაძლებელია მხოლოდ მისი მშობლის ან კანონიერი წარმომადგენლის წერილობითი თანხმობით, თუ კანონით სხვა რამ არ არის გათვალისწინებული.[18]

3.1.1. არასრულწლოვნის თანხმობა – საერთაშორისო და ეროვნული პრაქტიკა

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”), ისევე როგორც საქართველოს ეროვნული კანონმდებლობა, სპეციალურ რეგულირებას ითვალისწინებს არასრულწლოვნის მონაცემების დამუშავებისათვის. კერძოდ, განხილულ შემთხვევებში ზღვრულ ასაკად მიჩნეულია 16 წელი, როდესაც მონაცემთა სუბიექტს ენიჭება უფლება განკარგოს საკუთარი პერსონალური მონაცემები და დაეთანხმოს დამუშავების კონკრეტულ პროცესს.[19] საკითხის სრულყოფილი განხილვისთვის უნდა აღინიშნოს ხსენებული წესიდან გამონაკლისები, როდესაც კანონი პირდაპირ განსაზღვრავს რეგულირების განსხვავებულ წესს.[20]

დამატებით უნდა აღინიშნოს, რომ საქართველოს კანონმდებლობა არასრულწლოვანთა მონაცემების დამუშავებისას მონაცემთა სუბიექტის დაცვის მაღალი სტანდარტის უზრუნველსაყოფად მკაცრ მოთხოვნებს აწესებს და მინიმალურ ასაკს მონაცემთა დამუშავებაზე თანხმობის გაცემისათვის 16 წელს ითვალისწინებს,[21] მაშინ, როდესაც “GDPR”-ის მე-8 მუხლი იძლევა საშუალებას, წევრი სახელმწიფოების მიერ მინიმალური ასაკად არანაკლებ 13

[16] *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021, 29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].

[17] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 7 (3).

[18] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 7 (1).

[19] GDPR, Article 8 (1).

[20] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 7 (1).

[21] იქვე.

წელი განისაზღვროს.[22] აღნიშნული განსხვავება ასახავს საქართველოს კანონმდებლობის მიდრეკილებას არასრულწლოვანთა მონაცემთა დაცვის მიმართულებით უფრო მკაცრი სტანდარტის შენარჩუნებისკენ.

აღნიშნული მიდგომის საპირისპიროდ, ბრიტანეთის მონაცემთა დაცვის ზოგადი რეგულაცია (UK GDPR) იყენებს უფრო მოქნილ რეგულირებას და განსაზღვრავს, რომ არასრულწლოვნის მონაცემთა დამუშავებისას თანხმობის გაცემისთვის მინიმალური ასაკი 13 წელია.[23]

შვედეთის მონაცემთა დაცვის საზედამხედველო ორგანო გზამკვლევში „ციფრულ პლატფორმებზე ბავშვებისა და ახალგაზრდა პირების უფლებების შესახებ“ 13-დან 16 წლამდე პირების მიერ თანხმობის გაცემის საკითხზე მსჯელობისას აღნიშნავს, რომ თითოეულ კონკრეტულ შემთხვევაში უნდა შეფასდეს, შეუძლია თუ არა აღნიშნულ პირს, გააცნობიეროს თანხმობის შედეგები. ამ შეფასებაზე მოქმედებს რამდენიმე ფაქტორი, მათ შორის: რამდენად სენსიტიურია მოწოდებული პერსონალური მონაცემები, რამდენ ხანს ინახება ისინი, ასევე ბავშვის ასაკი და განვითარების დონე.[24]

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანო (“CNIL — Commission nationale de l'informatique et des libertés”) არასრულწლოვანთა მონაცემების დაცვის საკითხზე მსჯელობისას ასევე ყურადღებას ამახვილებს მშობელთა მხრიდან კონტროლის მექანიზმების მნიშვნელობაზე. „არასრულწლოვნები ყოველთვის ვერ ახერხებენ სრულად გააცნობიერონ ის რისკები, რომლებიც ონლაინ სივრცეში ემუქრებათ, და მიიღონ ინფორმირებული გადაწყვეტილებები. მშობლებს სჭირდებათ ეფექტიანი საშუალებები, რათა მხარი დაუჭირონ ბავშვებს მათ ონლაინ ცხოვრებაში.“[25]თუმცა აქვე არის აღნიშვნა საჭირო სიფრთხილესთან დაკავშირებით, რომ კონტროლის მექანიზმი არ იყოს განსაკუთრებით ჩამრევი ხასიათის, რათა მათი გამოყენება არ იწვევდეს არასრულწლოვანში მუდმივი მეთვაყურეობის ქვეშ ყოფნის განცდას.[26]

საფრანგეთის მონაცემთა დაცვის საზედამხედბელო ორგანოს (“CNIL”) რეკომენდაციაში ასევე განსაზღვრულია მშობელთა კონტროლის მექანიზმების მონაცემთა დაცვის რეგულაციებთან შესაბამისობის საჭიროებაც. კერძოდ, აღნიშნული მექანიზმების შეფასებისას სახეზე უნდა იყოს შემდეგი წინაპირობები:

- **პროპორციულობის პრინციპი**, რომელიც ითვალისწინებს ბავშვის საუკეთესო ინტერესებს, ასაკს, განვითარების დონესა და ისეთი

[22] GDPR, Article 8 (1).
[23] UK General Data Protection Regulation (UK GDPR), Article 8 (1).
[24] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide,20,< https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[25] *CNIL (Commission nationale de l'informatique et des libertés), Recommendation 5: Promote parental controls that respect the child's privacy and best interests,* 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
[26] იქვე.

ზედმეტად ჩამრევი ფუნქციების გამოყენების გამორიცხვას, მაგალითად, როგორიცაა მუდმივი თვალყურის დევნება;

- **გამჭვირვალობის პრინციპი** ბავშვის მიმართ, რომელიც მოიაზრებს კონტროლის მექანიზმების შესახებ ზუსტი ინფორმაციის მიწოდებას;
- **ბავშვის მონაცემთა უსაფრთხოების პრინციპი**, რათა მშობელმა უზრუნველყოს, რომ მესამე პირებს არ ჰქონდეთ წვდომა მოპოვებულ მონაცემებზე (მაგ: ბავშვის გეოლოკაციის მონაცემები).[27]

მშობელთა/კანონიერ წარმომადგენელთა მიერ არასრულწლოვანთა კონტროლის საკითხზე მსჯელობისას შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო აღნიშნავს, რომ ბავშვები არ უნდა დაექვემდებარონ მათი პირადი და ოჯახური ცხოვრებისთვის უკანონო და თვითნებურ შეზღუდვებს. კონტროლის განმახორციელებლებს ეკისრებათ პასუხისმგებლობა ბავშვის აღზრდასა და განვითარებაზე მათი საუკეთესო ინტერესების გათვალისწინებით, აღნიშნულ კონტექსტში კი განსაკუთრებით მნიშვნელოვანი ამოცანაა არსებული ინტერესების დაბალანსება და მისი მნიშვნელობის გაცნობიერება. ამასთან, რაც ასაკით უფროსია ბავშვი, მით მეტი ყურადღება უნდა ექცეოდეს მის თავისუფალ ნებასა და თანხმობის გამოხატვის უფლებას.[28]

3.2. თანხმობა დოკუმენტში, რომლითაც რამდენიმე საკითხი არის დარეგულირებული

მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს განსაკუთრებული სიფრთხილე მართებს, როდესაც თანხმობის ფორმულირება შემადგენელი ნაწილია დოკუმენტის, რომელიც თანხმობის საკითხთან ერთად არეგულირებს სხვა საკითხებსაც.

აღნიშნულ შემთხვევაში განსაკუთრებით მნიშვნელოვანია შესაბამის დოკუმენტში თანხმობის ტექსტი იყოს ჩამოყალიბებული მკაფიოდ, მარტივი და გასაგები ენით და ასევე გამოყოფილად დოკუმენტის სხვა ნაწილებისგან.[29]

მსგავს რეგულირებას ითვალისწინებს ასევე "GDPR"-ის დოკუმენტიც. მე-7 მუხლის მე-2 ნაწილის თანახმად, თუ მონაცემთა სუბიექტი თანხმობას გამოხატავს წერილობით დოკუმენტში, რომელიც სხვა საკითხებსაც არეგულირებს, თანხმობასთან დაკავშირებული ტექსტი/განცხადება უნდა

[27] იქვე.

[28] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 40, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

[29] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", №3144-XIმს-Xმპ, 14/06/2023, მუხლი 32 (1).

იყოს მოცემული იმგვარად, რომ ნათლად გამოირჩეოდეს სხვა საკითხებისაგან, იყოს გასაგები და იოლად აღქმადი, დაწერილი ნათელი და მარტივი ენით.[30]

განხილული მოთხოვნა ემყარება მონაცემთა დამუშავების პროცესში გამჭვირვალობის პრინციპის დაცვასა და რეალიზებას. მონაცემთა სუბიექტისთვის ნათელი უნდა იყოს, კონკრეტულად რომელ დამუშავების პროცესზე აცხადებს თანხმობას, რომელი მონაცემები დამუშავდება, რა მიზნითა და საფუძვლით. სავალდებულო წესით უნდა გამოირიცხოს თანხმობის ფორმათა ფორმულირება იმ წესით, როდესაც ის არ არის თვალსაჩინო, დოკუმენტის სრული ტექსტისგან გამოყოფილი და გონივრული შეფასებით არ აღიქმება, როგორც მონაცემთა სუბიექტისთვის მიცემული არჩევანი საკუთარი მონაცემების განკარგვასთან დაკავშირებით.

3.3. თანხმობა ხელშეკრულებაში

გამჭვირვალობის პრინციპის დაცვა განსაკუთრებით მნიშვნელოვანია როდესაც დოკუმენტი, რომლითაც მონაცემთა სუბიექტისგან თანხმობა არის მოპოვებული, წარმოადგენს ხელშეკრულებას.

აღნიშნულ შემთხვევაში თანხმობის ნებაყოფლობითობის საკითხი განსაკუთრებით სენსიტიურია, ვინაიდან ხელშეკრულების დოკუმენტში ფორმულირებული თანხმობა უნდა იძლეოდეს იმის საშუალებას, რომ მონაცემთა სუბიექტმა აღიქვას საკუთარი ნების ნებაყოფლობითად გამოხატვის თავისუფლება, რომ შეუძლია, თავისუფლად გააკეთოს არჩევანი და მის მიერ მიღებული გადაწყვეტილება არ იმოქმედებს ხელშეკრულების პირობებზე, მათ შორის ხელშეკრულების დადება/არდადების საკითხზეც.

„როდესაც მონაცემთა სუბიექტის თანხმობა გაცემულია ხელშეკრულების ან მომსახურების ფარგლებში, თანხმობის ნებაყოფლობითობის განსაზღვრისას, სხვა გარემოებებთან ერთად, უნდა შეფასდეს, თუ რამდენად არის თანხმობა ხელშეკრულების ან მომსახურების აუცილებელი წინაპირობა და თუ შეიძლება ამ თანხმობის გარეშე შესაბამისი მომსახურების მიღება/ხელშეკრულების დადება.”[31]

აღნიშნული რეგულირება შესაბამისია “GDPR”-ის მიდგომასთან, რომელიც ხაზს უსვამს მონაცემთა დამუშავებაზე თანხმობის გაცემისას სუბიექტის ნების ნათლად გამოვლენას, დამუშავდეს ის მონაცემებიც, რომლებიც არ არის აუცილებელი ხელშეკრულების შესრულებისთვის.[32]

[30] GDPR, Article 7 (2).
[31] პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა სუბიექტისგან თანხმობის მიღების“ შესახებ, 21.
[32] GDPR, Article 7 (4).

3.4. თანხმობა ონლაინ სივრცეში

დღევანდელი რეალობის გაციფრულებისა და ონლაინ სერვისების გამოყენების მზარდი ტენდენციების პარალელურად იზრდება ონლაინ პლატფორმებზე მონაცემთა სუბიექტისგან მონაცემთა დამუშავებაზე მოპოვებულ თანხმობასთან დაკავშირებული რისკების რაოდენობაც. ვებგვერდებზე, მობილურ აპლიკაციებსა და ონლაინ სერვისებით მოპოვებული თანხმობის კანონიერების საკითხი ერთ-ერთ აქტუალურ და პრობლემურ საკითხს წარმოადგენს.

მონაცემთა დაცვის ევროპული საბჭო (“EDPB”) თანხმობის შესახებ არსებულ რეკომენდაციაში განიხილავს ციფრულ გარემოსთან დაკავშირებულ სპეციფიკას და მასთან არსებულ რისკებს. კერძოდ, ონლაინ სივრცეებში მონაცემთა სუბიექტები ყოველდღიურად იღებენ თანხმობის მრავალ მოთხოვნას, რომლებიც გამოიხატება ღილაკების მონიშვნასა და ბმულის გადართვაში. აღნიშნული ქმედებების სიხშირე კი შესაძლოა განაპირობებდეს სუბიექტის დამოკიდებულებას, თანხმობის მექანიზმთან გადაჭარბებული ურთიერთობის შედეგად შემცირდეს მისი სიფრთხილე და ყურადღება.[33]

მიუხედავად იმისა, რომ ონლაინ სივრცეში მოპოვებული თანხმობის შემთხვევაშიც სავალდებულოა კანონით გათვალისწინებული კრიტერიუმებისა და მოთხოვნების დაცვა, პრაქტიკაში ხშირია შემთხვევები, როდესაც თანხმობის მოპოვების ფორმა მხოლოდ ფორმალობას წარმოადგენს. აღნიშნულ მავნე პრაქტიკას განსაკუთრებით ხშირად ვხვდებით ვებსაიტზე მზა-ჩანაწერების ე.წ. „cookie ფაილების“ საკითხის რეგულირებასთან დაკავშირებით. ვებსაიტზე შესვლისას ხშირად არის წარმოდგენილი არსებულ „cookie ფაილებზე“ ერთობლივი თანხმობის ფორმები, მაშინ, როდესაც მონაცემთა სუბიექტის უფლებაა გააკეთოს არჩევანი და დაეთანხმოს მისი მონაცემების დამუშავებას მხოლოდ იმ მზა ჩანაწერების ფარგლებში, რომლებიც მას სურს, ან რომლებიც წარმოადგენს ვებგვერდის ფუნქციონირებისა და უსაფრთხოებისთვის აუცილებელ ჩანაწერს და, შესაბამისად, მისი ფუნქციონირებაც სავალდებულო ხასიათის მატარებელია.

ამასთან, მნიშვნელოვანია, რომ: „თანხმობა მოპოვებულ იქნეს ვებსაიტზე შესვლისთანავე, სანამ ისინი მომხმარებლის მოწყობილობაზე განთავსდება, მაგალითად, “cookie” ბანერების მეშვეობით. მონაცემთა დამუშავების თითოეულ მიზანთან მიმართებით (რეკლამირების, ანალიტიკის და ა.შ.) თანხმობა განცალკევებული უნდა იყოს და სუბიექტმა ინდივიდუალურად უნდა განაცხადოს იგი.“[34]

[33] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[34] პერსონალურ მონაცემთა დაცვის სამსახურის გზამკვლევი „ვებსაიტის შექმნის მსურველთათვის“ 27.

საყურადღებოა, რომ თანხმობის კანონით განსაზღვრული კრიტერიუმები ონლაინ სივრცეშიც დიდ მნიშვნელობას იძენს, განსაკუთრებით კი გამჭვირვალობის და ინფორმირებულობის პრინციპი, რომლის შესაბამისადაც, მონაცემთა სუბიექტისათვის მიწოდებული ინფორმაცია უნდა იყოს გასაგები, აღქმადი და კონკრეტული.

ონლაინ სივრცეებში წინასწარ გაკეთებულ მონიშვნებთან დაკავშირებით საინტერესო მსჯელობას ვხვდებით ევროკავშირის მართლმსაჯულების სასამართლოს ("CJEU") ერთ-ერთ გადაწყვეტილებაში (საქმეზე Planet49 GmbH (C-673/17, 2019 წლის 1 ოქტომბერი), რომელშიც აღნიშნულია, რომ მსგავს შემთხვევებში: „შეუძლებელია ობიექტურად დადგინდეს, ნამდვილად გასცა თუ არა მომხმარებელმა ვებსაიტზე თანხმობა საკუთარი პერსონალური მონაცემების დამუშავებაზე იმით, რომ არ მოხსნა მონიშვნა წინასწარ გაკეთებული მონიშვნიდან, ან საერთოდ - იყო თუ არა ეს თანხმობა ინფორმირებული. არ არის გამორიცხული, რომ მომხმარებელს არც წაეკითხა წინასწარ მონიშვნასთან დაკავშირებული ინფორმაცია, ან საერთოდ ვერ შეემჩნია ის და ისე გაეგრძელებინა ვებსაიტზე თავისი საქმიანობა."[35]

ონლაინ სივრცეში მიღებული თანხმობაც თავისთავად ექვემდებარება მოთხოვნას, მოპოვებულ იქნეს აქტიური ქმედებით (ღილაკზე დაჭერა, მონიშვნა და სხვ.), რაც, თავის მხრივ, გამორიცხავს ავტომატურად მონიშნული ფორმებით მოპოვებული თანხმობის სამართლებრივ ძალას.

3.5. თანხმობის გამოხმობის უფლება

თანხმობის ნებაყოფლობითი ხასიათის ერთ-ერთ გარანტიას ასევე წარმოადგენს მისი თავისუფალი გამოხმობის შესაძლებლობა და მის შესახებ მონაცემთა სუბიექტების ინფორმირება. აღნიშნულ შემთხვევაშიც მსგავსად მონაცემთა დამუშავების თაობაზე ინფორმაციის მიწოდების წინსწრებითი ხასიათისა, თანხმობის გამოხმობაზე ინფორმირებაც წინასწარ უნდა განხორციელდეს, მანამ, სანამ სუბიექტი განაცხადებს თანხმობას.

თანხმობის გამოხმობის საკითხის რეგულირებას „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი რამდენიმე ნორმაში ითვალისწინებს.

პირდაპირი მარკეტინგი - „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-12 მუხლი,[36] რომლითაც განსაზღვრულია თანხმობის გამოხმობის შესახებ ინფორმაციის მიწოდების ვალდებულებისა და აღნიშნული უფლების რეალიზების გარანტიების თაობაზე, კერძოდ, მისი უსასყიდლო და შეუზღუდავი გამოყენების ჭრილში.

[35] მართლმსაჯულების ევროპული სასამართლო (European Court of Justice), CJEU, Case C-673/17, Planet49 GmbH [2019], §55, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].

[36] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", №3144-XIმს-Xმპ, 14/06/2023, მუხლი 12 (3).

მონაცემთა სუბიექტის უფლებების თავში - „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-20 მუხლი,[37] რომელშიც დეტალურად არის განმარტებული აღნიშნულის რეალიზებისათვის საჭირო წინაპირობები:

- **დროში შეუზღუდავად, ნებისმიერ დროს** - აღნიშნული გამოირიცხავს დამუშავებისთვის პასუხისმგებელი პირის შესაძლებლობას, თუნდაც საკუთარი კონკრეტული მიზნის მითითებითა და ამ გზით დასაბუთებით, დააწესოს რაიმე ვადა თანხმობის გამოხმობისათვის;
- **განმარტებისა და დასაბუთების გარეშე** - კანონის მიზნებისა და მონაცემთა სუბიექტის ძირითადი უფლებების რეალიზების ქმედითი ღონისძიებების დასანერგად მნიშვნელოვანია, რომ გარანტირებული იყოს საკუთარი მონაცემების თავისუფლად განკარგვის შესაძლებლობა, მათ შორის – გაცემული თანხმობის განმარტებისა და დასაბუთების გარეშე მისი გამოთხოვის უფლება;
- **იმავე ფორმით გამოხმობის შესაძლებლობა, რომლითაც თანხმობა განაცხადა** - ნებაყოფლობითობისა და თავისუფლად ნების გამოვლენის კრიტერიუმი, რა თქმა უნდა, მოიაზრებს, რომ გამოირიცხოს დამუშავებისთვის პასუხისმგებელი პირის მხრიდან ზემოქმედების, ზეწოლის, ხელშეშლის, უფლების რეალიზებისთვის ხელოვნურად შექმნილი წინააღმდეგობების გათვალისწინება. რაც, თავის მხრივ, მოიაზრებს პასუხისმგებელი პირის ვალდებულებას, არ გაითვალისწინოს მხოლოდ კონკრეტულ შემთხვევებში, პირობებსა და ფორმით თანხმობის გამოხმობის შესაძლებლობა.

ამასთან, თანხმობის გამოხმობის კანონიერების შემოწმებისას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მტკიცების ტვირთია, დაადასტუროს, რომ მონაცემთა სუბიექტებისათვის აღნიშნული უფლების რეალიზება არ არის დაკავშირებული გარკვეულ ხარჯებთან და, შესაბამისად, არ არის აშკარა უარყოფითი შედეგების საფრთხე.[38]

აღნიშნული უფლების თავისუფლად და ნებისმიერ დროს რეალიზების შესაძლებლობის შეფასებისას ასევე ყურადღება უნდა მიექცეს კონკრეტული პროცესის თავისებურებებსაც. კერძოდ, თუ მონაცემთა სუბიექტს შესაძლოა შეეზღუდოს თანხმობის გამოხმობის უფლება იმ საფუძვლით, რომ მისი რეალიზებით დამუშავების შესაბამისი პროცესი დაზიანდება, მაგალითად, კვლევის შედეგებს შეექმნება საფრთხე, რეკომენდებულია, მსგავსი პროცესი არ იყოს დაფუძნებული თანხმობის სამართლებრივ საფუძველზე. ვინაიდან

[37] იქვე, მუხლი 20.
[38] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 13, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

თანხმობის გამოხმობა ნებისმიერ დროს შეუზღუდავად უნდა იყოს შესაძლებელი.[39]

3.6. თანხმობის გამოხმობა ონლაინ სივრცეში

ონლაინ სივრცეში, გარდა თანხმობის მოპოვებასთან დაკავშირებული საკითხებისა, მნიშვნელოვანია, გათვალისწინებული და პრაქტიკაში რეალიზებული იყოს მისი გამოხმობის შესაძლებლობა და უფლება.

მონაცემთა სუბიექტის აღნიშნული უფლების სრულყოფილი რეალიზებისათვის კი აუცილებელია ციფრული გარემო და მისი სპეციფიკა პრაქტიკაში შესაბამისი იყოს კანონის მოთხოვნებთან. ვებგვერდზე თანხმობის გამოხმობისათვის რთული და მრავალსაფეხურიანი გზების დასახვა პირდაპირ მიანიშნებს მონაცემთა დამუშავებაზე პასუხისმგებელი პირის არაკეთილსინდისიერ დამოკიდებულებასა და მონაცემთა სუბიექტის უფლებებისადმი არაჯეროვანი პატივისცემის საკითხებზე.

თანხმობა მხოლოდ ტექნიკური ფორმულარით ან ღილაკზე დაჭერით არ უნდა შემოიფარგლოს — ის უნდა იყოს რეალური ნების გამოხატულება, გამჭვირვალობისა და ინფორმირებულობის პრინციპსა და თავისუფალ არჩევანზე დაფუძნებული.

4. საერთაშორისო პრაქტიკა და გამოწვევები

მონაცემთა დამუშავების საფუძვლად თანხმობის განხილვის საკითხი, ისევე როგორც მისი კანონშესაბამისობა და მასთან დაკავშირებული უფლებების ქმედითობა, საერთაშორისო სამართლის ერთ-ერთ აქტუალურ საკითხს წარმოადგენს. პრაქტიკის ანალიზით ნათელია, რომ ნებაყოფლობითობის, ინფორმირებულობისა და გამჭვირვალობის პრინციპებს განსაკუთრებით დიდი მნიშვნელობა ენიჭება.

ამასთან, საერთაშორისო პრაქტიკის ანალიზი უზრუნველყოფს შესაძლებლობას, შეფასდეს ეროვნული კანონმდებლობის შესაბამისობა საერთაშორისო სტანდარტებთან, იდენტიფიცირდეს არსებული გამოწვევები და რისკები შედარებითი განხილვის საფუძველზე.

4.1. „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”)

საერთაშორისო პრაქტიკის დამკვიდრებაში მნიშვნელოვანი ადგილი უკავია ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციას“ (“General Data Protection Regulation – GDPR”),[40] რომელიც განსაზღვრავს მონაცემთა

[39] *Information Commissioner’s Office (ICO),* “What is Valid Consent?”, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016

დამუშავების პრინციპებს, უფლებებსა და ვალდებულებებს, რომლებიც მიმართულია ფიზიკური პირების მონაცემების დაცვისკენ.

"GDPR" განსაკუთრებულ მნიშვნელობას ანიჭებს და ნათლად გამოყოფს თანხმობის შემდეგ სავალდებულო მახასიათებლებს:

- ნათლად გამოხატული მოქმედება;
- ნებაყოფლობითობა;
- კონკრეტულობა;
- ინფორმირებულობა;
- მკაფიოობა.[41]

გარდა აღნიშნულისა, "GDPR" განსაზღვრავს მითითებას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მტკიცების ტვირთზე, შეძლოს მონაცემთა სუბიექტის მიერ დამუშავების პროცესზე გაცემული თანხმობის დემონსტრირება.[42] ასევე, ნათლად არის წარმოჩენილი საფრთხეები, როდესაც დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის აშკარა უთანასწორო ვითარებაა, განსაკუთრებით კი იმ შემთხვევაში, როდესაც დამუშავებისთვის პასუხისმგებელი პირი სახელმწიფო უწყებას წარმოადგენს.[43]

"GDPR"-ით გათვალისწინებული თანხმობის რეგულირების საკითხის ანალიზისას ცხადი ხდება მისი და საქართველოს კანონმდებლობის ერთმანეთთან შესაბამისობა და საკითხის მსგავსად რეგულირების პრაქტიკა. კერძოდ, განხილულ შემთხვევებში ვხვდებით რეგულირების ერთიან მიდგომას თანხმობის წერილობით დოკუმენტში გამოხატვის მიმართ, როდესაც დოკუმენტით ასევე სხვა საკითხებიც რეგულირდება. საკითხზე მსჯელობისას მკაფიოდ არის განსაზღვრული როგორც ეროვნული, ასევე საერთაშორისო კანონმდებლობის შესაბამისად, რომ თანხმობის ტექსტი/განცხადება გამორჩეულად/გამოყოფილად იყოს გათვალისწინებული სხვა საკითხებისგან, ნათლად და იოლად გასაგები ენით გადმოცემული.

ასევე პირდაპირი შესაბამისობაა საქართველოს ეროვნულ კანონმდებლობასა და "GDPR" ნორმებს შორის თანხმობის გამოთხოვის საკითხთან დაკავშირებითაც. ორივე განხილულ შემთხვევაში თანხმობის თავისუფლად, შეუზღუდავად გამოხმობის შესაძლებლობა, თავად თანხმობის სწორი ფორმულირების და მისი, როგორც სამართლებრივად გამართული საფუძვლის, რეალიზების წინაპირობად არის განხილული.[44]

საერთაშორისო პრაქტიკა, განსაკუთრებით "GDPR"-ის დებულებები, წარმოადგენს მნიშვნელოვან სტანდარტს, რომლის საფუძველზეც საქართველოს კანონმდებლობა და მასზე დაფუძნებული პრაქტიკა სახელმძღვანელო მითითებებს იღებს. საერთაშორისო რეგულაციები გვიჩვენებს, როგორ უნდა იყოს ფორმულირებული თანხმობის მოთხოვნის

[41] იქვე, Recital 32.
[42] იქვე, Article 7(1).
[43] GDPR, Recital 43.
[44] იქვე, Article 7(3).

ტექსტი, რათა რეალიზებულ იქნეს ნებაყოფლობითობის, ინფორმირებულობისა და გამჭვირვალობის პრინციპები.

შესაბამისად, "GDPR" მონაცემთა დაცვის სფეროში, მათ შორის დამუშავების პროცესების კანონიერების განსაზღვრების ეტაპზე, არა მხოლოდ საგანმანათლებლო და სახელმძღვანელო ინსტრუმენტს წარმოადგენს, არამედ მნიშვნელოვან სტანდარტადაც აღიქმება, რომელიც უზრუნველყოფს ეროვნული კანონმდებლობის განვითარებას ისევე, როგორც არსებული პრაქტიკისა და საზოგადოების სამართლებრივი ცნობიერების ამაღლებას.

5. დასკვნა

მონაცემთა დამუშავების საფუძვლად სუბიექტის თანხმობის გათვალისწინების საკითხის განხილვისას მასთან დაკავშირებული კანონისმიერი მოთხოვნებისა და კრიტერიუმების შეფასებისას ცხადი ხდება, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ დამუშავების პროცესისთვის, ერთი შეხედვით ყველაზე მარტივად მოსაძებნი და მისასადაგებელი საფუძველი, საკმარისად კომპლექსური და მრავლისმომცველია, ხოლო მასთან დაკავშირებული დამცველობითი ბერკეტები კი მნიშვნელოვნად გამორიცხავს თანხმობის მხოლოდ ფორმალურად არსებობის შესაძლებლობას.

თანხმობის ინსტიტუტის ეფექტიანად ფუნქციონირებისთვის გადამწყვეტია რამდენიმე ფაქტორის ერთობლიობა — გამჭვირვალობა, ინფორმირებულობა, ნებაყოფლობითობა და პასუხისმგებელი პირის კეთილსინდისიერება. აღნიშნული კრიტერიუმების ერთიანი სახით წარმოდგენის შემთხვევაში არის შესაძლებელი დავასკვნათ, რომ სუბიექტის თანხმობა რეალურად წარმოადგენს ნების თავისუფალ გამოვლინებას და არა მხოლოდ ფორმალობას.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანო ("ICO") თანხმობის სამართლებრივ საფუძველთან დაკავშირებით ზოგად პრინციპს აყალიბებს, რომლის თანახმადაც, როდესაც რთულდება თანხმობის სტანდარტის შესრულება, სახეზეა ნიშანი, რომ ის არ წარმოადგენს შესაფერის საფუძველს მონაცემთა დამუშავებისათვის.[45]

თანამედროვე ციფრულ გარემოში, სადაც მონაცემთა დამუშავების მოცულობა და სიხშირე უპრეცედენტოა, განსაკუთრებული მნიშვნელობა ენიჭება თანხმობის გაცემისა და გამოხმობის პრაქტიკულ უზრუნველყოფას — სუბიექტს უნდა ჰქონდეს შესაძლებლობა, გააცნობიეროს, რაზე ეთანხმება და სურვილის არსებობისას გამოითხოვოს იგი უკან.

გრძელვადიან პერსპექტივაში მნიშვნელოვანია, რომ თანხმობის ინსტიტუტი არ იქცეს ფორმალურ მექანიზმად, არამედ იყოს რეალური

[45] *Information Commissioner's Office (ICO)* Guideline on *When is consent appropriate?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/

გარანტი პირის ინფორმირებულობისა და არჩევნის თავისუფლებისათვის. სწორედ აღნიშნული მიდგომის დამკვიდრება უზრუნველყოფს მონაცემთა დაცვის კულტურის განვითარებას, კანონმდებლობის ეფექტიან გამოყენებას და საზოგადოების ნდობის განმტკიცებას როგორც საჯარო, ასევე კერძო სექტორის მიმართ.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14.06.2023.
2. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა სუბიექტისგან თანხმობის მიღების“ შესახებ, 10, 21.
3. პერსონალურ მონაცემთა დაცვის სამსახურის გზამკვლევი „ვებსაიტის შექმნის მსურველთათვის“, 27.
4. EU, 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).
5. UK General Data Protection Regulation (UK GDPR), <https://www.legislation.gov.uk/ukpga/2018/12/contents> [27.11.2025].
6. *The Autoriteit Persoonsgegevens (AP),* Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].
7. *Cate, F. H.* The Failure of Fair Information Practice Principles In Consumer Protection in the Age of the Information Economy 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].
8. *CNIL (Commission nationale de l'informatique et des libertés),* Recommendation 5: Promote parental controls that respect the child's privacy and best interests, 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
9. *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021, 29. <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].
10. *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018, 7,

<https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].

11. *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 10, 13, 19. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].
12. *Information Commissioner's Office (ICO)* Guideline on What is valid consent? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].
13. *Information Commissioner's Office (ICO)* Guideline on What is consent appropriate? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].
14. *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 3, 15, 20, 40. <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
15. მართლმსაჯულების ევროპული სასამართლო (European Court of Justice), CJEU, Case C-673/17, Planet49 GmbH [2019], §55 <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].

ჯინევრა სერინა ფერონი*

ხელოვნური ინტელექტის მართვა მონაცემთა დაცვის მეშვეობით: დამოუკიდებელი უწყებების სტრატეგიული როლი ალგორითმული ძალაუფლების ეპოქაში**

ხელოვნური ინტელექტი ("AI") მხოლოდ ტექნოლოგიურ ცვლილებას არ წარმოადგენს, ის ასევე კონსტიტუციური გამოწვევაა. ვინაიდან ხელოვნური ინტელექტის სისტემები უფრო აქტიურად ერთვებიან სოციალურ, ეკონომიკურ და სამართლებრივ გადაწყვეტილებებში, იზრდება მონაცემთა დაცვის საზედამხედველო ორგანოების ("DPAs") როლის მნიშვნელობა. წინამდებარე მოკლე ესე, რომელიც ეფუძნება იტალიის პერსონალურ მონაცემთა დაცვის სამსახურის ვიცე-პრეზიდენტის, პროფესორ ჩერინა ფერონის მიერ პერსონალურ მონაცემთა დაცვის ორგანოების 33-ე ევროპულ კონფერენციაზე წარმოთქმულ სიტყვას, განიხილავს ხელოვნურ ინტელექტსა და პერსონალურ მონაცემებს შორის არსებულ სტრუქტურულ ურთიერთდამოკიდებულებას და პერსონალურ მონაცემთა დაცვას ხელოვნური ინტელექტის მართვის ცენტრში ათავსებს. იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოს გამოცდილებისა და შედარებითი საერთაშორისო მაგალითების საფუძველზე, ის აანალიზებს ოთხ კრიტიკულ სფეროს: კანონიერ საფუძვლებს, მონაცემთა გადაცემას, ავტომატიზებული გადაწყვეტილებების მიღებას და მოწყვლადი პირების დაცვას, რომელთა მიმართებით მონაცემთა დაცვის საზედამხედველო ორგანოები ადგენენ ხელოვნური ინტელექტის სისტემების ნორმატიულ საზღვრებს. უფრო მეტიც, მასში საუბარია

* იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ვიცე-პრეზიდენტი; იტალიის და შედარებითი კონსტიტუციური სამართლის სრული პროფესორი ფლორენციის უნივერსიტეტის იურიდიულ ფაკულტეტზე; უნივერსიტეტის პროფესორთა სპეციალურ რეესტრში რეგისტრირებული იურისტი; იტალიის შედარებითი საჯარო სამართლის ასოციაციის საბჭოს წევრი; იტალიის კონსტიტუციონალისტთა ასოციაციის საბჭოს წევრი.

** ნაშრომი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მასპინძლობით ქ. ბათუმში გამართულ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა 33-ე ევროპულ კონფერენციაზე („საგაზაფხულო კონფერენციაზე") წარდგენილი მოხსენების ტექსტს.

იმაზე, რომ მონაცემთა დაცვის საზედამხედველო ორგანოების როლს სარგებელი შეიძლება მოუტანოს რეაქტიული აღმსრულებლებიდან პროაქტიულ ინსტიტუციურ აქტორებად ევოლუციამ, რომლებიც ჩართულნი იქნებიან სისტემების დიზაინში, აუდიტსა და რისკების კლასიფიკაციაში. ესეში გამოთქმულია მოსაზრება, რომ ხელოვნური ინტელექტის მმართველობის ლეგიტიმურობას, სამართლებრივ სტაბილურობასა და დემოკრატიულ ანგარიშვალდებულებას საუკეთესოდ ემსახურება დამოუკიდებელი საზედამხედველო ორგანოების ცენტრალური ჩართულობა.

საკვანძო სიტყვები: ხელოვნური ინტელექტი, მონაცემთა დაცვა, დამოუკიდებელი ორგანოები, “GDPR”, ხელოვნური ინტელექტის მართვა, ალგორითმული ანგარიშვალდებულება.

1. შესავალი

სამართლიანია ითქვას, რომ ხელოვნური ინტელექტის (AI) სფერო მნიშვნელოვან გავლენას ახდენს მმართველობაზე, ინსტიტუციურ ანგარიშვალდებულებასა და ფუნდამენტური უფლებების დაცვაზე. ეს არ არის თვითკმარი მოვლენა, არამედ ტრანსფორმაცია, რომელიც საჯარო ადმინისტრირების, კერძო ბაზრებისა და ყოველდღიური სოციალური ინტერაქციების ფარგლებში შეინიშნება. საინტერესოა, რომ ხელოვნური ინტელექტის, როგორც განმასხვავებელი მახასიათებელი წინა ტექნოლოგიური მიღწევებთან შედარებით, არის მისი უნარი, მიიღოს ან მოახდინოს გავლენა გადაწყვეტილებებზე დამოუკიდებლად. გადაწყვეტილებები, რომლებიც ერთ დროს ექსკლუზიურად ადამიანის განსჯისა და ინსტიტუციური პროცედურების სფეროს განეკუთვნებოდა, ახლა ხელოვნური ინტელექტის გავლენას განიცდის. გადაწყვეტილების მიღების უფლებამოსილების ამგვარმა გადანაწილებამ ადამიანიდან მანქანაზე შესაძლოა მნიშვნელოვანი ცვლილებები გამოიწვიოს ანგარიშვალდებულების, გამჭვირვალობისა და უფლებების განხორციელების კუთხით.

როგორც უკვე აღინიშნა, ხელოვნური ინტელექტის ზოგადი დანიშნულება გულისხმობს მის შესაძლებლობას, გავლენა მოახდინოს მარეგულირებელი სფეროების ფართო სპექტრზე, მათ შორის, მომხმარებელთა დაცვაზე, შრომის სამართალზე, მედიის სამართალზე, სისხლის სამართლის მართლმსაჯულებასა და ჯანდაცვის მმართველობაზე. მნიშვნელოვანია აღინიშნოს, რომ სამართლებრივი რეჟიმების ურთიერთკვეთა ქმნის ნორმატიული გაურკვევლობის სფეროებს, რამაც შეიძლება გაართულოს

საკანონმდებლო ლანდშაფტი. ასეთ გარემოში შესაძლოა, პერსონალურ მონაცემთა დაცვის სექტორულ საკითხად განხილვა უკვე აღარ იყოს საკმარისი. წინააღმდეგ შემთხვევაში, ის უნდა განიხილებოდეს, როგორც დემოკრატიული საზოგადოებების სექტორთაშორისი სტრუქტურული გარანტია.

იმის გათვალისწინებით, რომ ხელოვნური ინტელექტი ოპტიმიზაციის ინსტრუმენტიდან გადაწყვეტილების მიღების არქიტექტურად გარდაიქმნება, სასარგებლო იქნებოდა, დავფიქრდეთ, თუ ვინ უნდა განსაზღვროს მისი ფარგლები. საინტერესო იქნებოდა იმის ცოდნაც, თუ ვინ არის პასუხისმგებელი მისი ანგარიშვალდებულების უზრუნველყოფაზე და ვინ იცავს პირებს, როდესაც ალგორითმული სისტემების გავლენა მათ ცხოვრებაზე ყოველთვის მკაფიო არ არის.

ევროპულ სამართლებრივ ტრადიციაში მიიჩნევა, რომ ტექნოლოგიური საზღვრების გადალახვისგან ფუნდამენტური უფლებების დაცვას საუკეთესოდ ემსახურება ინსტიტუციური უფლებებზე დაფუძნებული მექანიზმები. მათ შორის, მონაცემთა დაცვის საზედამხედველო ორგანოებს (“DPAs”) უნიკალური პოზიცია უკავიათ. ისინი აღჭურვილნი არიან საგამოძიებო, მაკორექტირებელი და საკონსულტაციო მანდატით და უფლებამოსილნი არიან დაიცვან რეგულაცია (EU) 679/2016-ით (“GDPR”) გათვალისწინებული უფლებები.

თუმცა მნიშვნელოვანია აღინიშნოს, რომ ხელოვნური ინტელექტის სისტემების მმართველობაში მათი როლი ჯერ კიდევ განვითარების პროცესშია და ზოგჯერ სადავოა. წინამდებარე ნაშრომი მიზნად ისახავს, ნათელი მოჰფინოს მონაცემთა დაცვის საზედამხედველო ორგანოების (“DPAs”) მნიშვნელობას კანონიერი და უფლებებთან თავსებადი ხელოვნური ინტელექტის ჩამოყალიბებაში.

აღსრულების პრაქტიკულ გამოცდილებაზე, სამართლებრივ დოქტრინასა და ზედამხედველობის შედარებით პრაქტიკებზე დაყრდნობით, ნაშრომის მომდევნო ნაწილებში მოკრძალებულად არის შემოთავაზებული პერსონალურ მონაცემთა დაცვის პროაქტიული, ინტერდისციპლინური და წინმსწრები მოდელი ხელოვნური ინტელექტის ეპოქაში.

2. ხელოვნური ინტელექტი და მონაცემთა დაცვის აუცილებლობა

ხელოვნურ ინტელექტსა (AI) და პერსონალურ მონაცემებს შორის ურთიერთობა შემთხვევითი არ არის, არამედ კონსტიტუციურია. სამართლიანია იმის თქმა, რომ ხელოვნური ინტელექტის ყველაზე მოწინავე მოდელები, გენერაციული სისტემებიდან დაწყებული პროგნოზულ ანალიტიკამდე, იწვრთნება, იხვეწება და გამოიყენება იმ მონაცემების მეშვეობით, რომლებიც აღწერს ან უკავშირდება პირებს. არ აქვს მნიშვნელობა, რა ფორმას იღებს ეს მონაცემები, იქნება ეს მომხმარებლის მიერ შეყვანილი ინფორმაცია, სენსორების მონაცემები თუ ქცევითი პროფილები, გასათვალისწინებელია მნიშვნელოვანი სამართლებრივი შედეგები.

"GDPR"-ის თანახმად, პერსონალური მონაცემების დამუშავება დასაშვებია მხოლოდ კონკრეტული კანონიერი საფუძვლების არსებობისას.[1] ხელოვნური ინტელექტის კონტექსტში, განსაკუთრებით მოდელის წვრთნის სფეროში, ყველაზე ხშირად გამოყენებული საფუძვლებია თანხმობა და ლეგიტიმური ინტერესი. თუმცა მნიშვნელოვანია აღინიშნოს, რომ ორივე ამ მიდგომას აქვს თავისი გამოწვევები.

იმისთვის, რომ თანხმობა ნამდვილი იყოს, ის უნდა იყოს ინფორმირებული, კონკრეტული, ნებაყოფლობითი და უნდა არსებობდეს მისი გამოხმობის შესაძლებლობა. გაუმჭვირვალე და ფართომასშტაბიანი სწავლების ოპერაციებისას ამ კრიტერიუმების დაკმაყოფილება ზოგჯერ შესაძლოა, გამოწვევას წარმოადგენდეს.

მეორე მხრივ, ლეგიტიმური ინტერესი მოითხოვს ინტერესთა დაბალანსების ტესტს, რომელიც გულისხმობს იმის შეფასებას, თუ რამდენად აღემატება დამუშავებისთვის პასუხისმგებელი პირის ინტერესები მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს. ხელოვნური ინტელექტის სფეროში, სადაც რისკები შეიძლება იყოს რთული, კუმულაციური და რთულად პროგნოზირებადი, ასეთი შეფასებები განსაკუთრებული გულმოდგინებით შესწავლას საჭიროებს.

უფრო მეტიც, მონაცემთა საზღვრებს მიღმა ნაკადები დამატებით გამოწვევებს წარმოშობს. მნიშვნელოვანია აღინიშნოს, რომ ხელოვნური ინტელექტის შემქმნელები ხშირად ანაწილებენ გამოთვლით დავალებებს სხვადასხვა იურისდიქციაში, ზოგჯერ ისეთ მესამე ქვეყნებში, სადაც არ არსებობს დაცვის ადეკვატური სამართლებრივი გარანტიები. მიუხედავად იმისა, რომ "GDPR"-ის V თავი ასეთი გადაცემებისთვის მკაცრ პირობებს აწესებს, აღსრულების პროცესს შეიძლება ხელი შეუშალოს გამჭვირვალობის ნაკლებობამ. სინამდვილეში, ბევრი დეველოპერი არ ამჟღავნებს მონაცემთა დამუშავების ან შენახვის ადგილს, რის მიზეზადაც ხშირად ასახელებს კომერციულ საიდუმლოებას ან ტექნოლოგიურ სირთულეს.

დაბოლოს, "GDPR"-ის 22-ე მუხლის მიზანია, უზრუნველყოს, რომ მხოლოდ ავტომატიზებული დამუშავების საფუძველზე მიღებულმა გადაწყვეტილებებმა არ გამოიწვიოს იურიდიული ან მსგავსი მნიშვნელოვანი შედეგები. გამონაკლისები არსებობს, მაგრამ ისინი ექვემდებარება პროცედურულ გარანტიებს, მათ შორის, აზრობრივი ინფორმაციის მიწოდებას, გასაჩივრების უფლებას და ადამიანის მხრიდან ზედამხედველობის ჩართვას.[2]

---

[1] იხილეთ, კერძოდ, "GDPR"-ის მე-6 და მე-9 მუხლები. მაშინ, როდესაც მე-6 მუხლი აყალიბებს ნებისმიერი პერსონალური მონაცემის დამუშავების ზოგად კანონიერ საფუძვლებს, მე-9 მუხლი კონკრეტულად ფოკუსირებულია პერსონალურ მონაცემთა სპეციალური კატეგორიების დამუშავებაზე, რაც უფრო შეზღუდულია.

[2] "GDPR"-ის 22-ე მუხლი:

„1. მონაცემთა სუბიექტს უფლება აქვს, არ დაექვემდებაროს გადაწყვეტილებას, რომელიც მთლიანად ავტომატიზებული დამუშავების, მათ შორის პროფილის შედგენის საფუძველზეა მიღებული და რომელიც იწვევს მისთვის სამართლებრივ შედეგებს ან ანალოგიურად მნიშვნელოვან გავლენას ახდენს მასზე.

2. პირველი პუნქტი არ გამოიყენება, თუ გადაწყვეტილება:

ამ კონტექსტით მონაცემთა დაცვის საზედამხედველო ორგანოებმა დაიწყეს ინსპექტირება და ადმინისტრაციული წარმოება, რომლებიც, ზოგიერთ შემთხვევაში, ჯარიმების განსაზღვრით დასრულდა. იტალიაში პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“Garante”) მიერ “Replika”-სა და “ChatGPT”-ის წინააღმდეგ განხორციელებულმა აღსრულების ღონისძიებებმა ხაზი გაუსვა გადაუდებელი ზომების მიღების აუცილებლობას, განსაკუთრებით კანონიერი საფუძვლების არარსებობის, უფრო მეტი გამჭვირვალობის საჭიროებისა და არასრულწლოვანთა დაცვის გადამწყვეტი მნიშვნელობის გათვალისწინებით. კანადის[3], სამხრეთ კორეისა[4] და იაპონიის[5] მსგავსი ინტერვენციები ადასტურებს აღნიშნული პრობლემების გლობალურ აქტუალობას.

ა) აუცილებელია მონაცემთა სუბიექტსა და მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შორის ხელშეკრულების დასადებად ან შესასრულებლად;
ბ) უფლებამოსილია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით, რომელსაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ექვემდებარება და რომელიც ასევე ითვალისწინებს შესაბამის ზომებს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების, აგრეთვე მისი ლეგიტიმური ინტერესების დასაცავად; ან
გ) ეფუძნება მონაცემთა სუბიექტის მკაფიო თანხმობას.
3. მე-2 პუნქტის „ა“ და „გ“ ქვეპუნქტებით გათვალისწინებულ შემთხვევებში, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს შესაბამის ზომებს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების, აგრეთვე მისი ლეგიტიმური ინტერესების დასაცავად, რაც, სულ მცირე, გულისხმობს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მხრიდან ადამიანის ჩარევის, საკუთარი აზრის გამოხატვისა და გადაწყვეტილების გასაჩივრების უფლების უზრუნველყოფას.“

[3] 2023 წლის 4 აპრილს კანადის კონფიდენციალურობის კომისრის ოფისმა (“OPC”) გამოაცხადა “OpenAI”-ის წინააღმდეგ ინსპექტირების დაწყების შესახებ. ამას საფუძვლად დაედო საჩივარი, რომელიც უკავშირდებოდა პერსონალური მონაცემების შეგროვებასა და გამჟღავნებას თანხმობის გარეშე. მეტი ინფორმაციისთვის იხილეთ: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/>.

[4] 2025 წლის 17 თებერვალს სამხრეთ კორეის პერსონალური ინფორმაციის დაცვის კომისიამ (“PIPC”) განაცხადა, რომ “DeepSeek”-მა შეაჩერა თავისი აპლიკაციაზე დაფუძნებული სერვისი კორეაში, რათა დაცული ყოფილიყო პერსონალური ინფორმაციის დაცვის აქტი (“PIPA”). ამას წინ უძღოდა “PIPC”-ის მიერ ჩატარებული მოკვლევა და ტექნიკური შეფასება, რომელმაც გამოავლინა “DeepSeek”-ის კონფიდენციალურობის პოლიტიკის გამჭვირვალობის ნაკლებობა და მესამე მხარისთვის მონაცემების შესახებ არაინფორმირებული გადაცემები. მეტი ინფორმაციისთვის იხილეთ: https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2784#none.

[5] 2025 წლის 3 თებერვალს, იაპონიის პერსონალური ინფორმაციის დაცვის კომისიამ (“PPC”) გამოაქვეყნა დეტალური ინფორმაცია “Hangzhou DeepSeek Artificial Intelligence”-ის კონფიდენციალურობის პოლიტიკის შესახებ, რითაც ნათელი მოჰფინა, თუ როგორ აგროვებს, ამუშავებს და იცავს კომპანია მომხმარებლის მონაცემებს. მეტი ინფორმაციისთვის იხილეთ:https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/.

3. დამოუკიდებელი ზედამხედველობის დემოკრატიული ღირებულება

ხელოვნური ინტელექტის მართვა არ არის ნეიტრალური, ტექნოკრატიული პროცესი, არამედ ძალაუფლების დაპირისპირების სფერო. ხელოვნური ინტელექტის სისტემები გავლენას ახდენს ქცევაზე, აყალიბებს ნარატივებს, ქმნის ცოდნას და, უფრო მეტიც, ზოგიერთ შემთხვევაში, აქვს პოტენციალი, გადაწყვიტოს, გარანტირებული იქნება თუ არა წვდომა მთელ რიგ სერვისებზე, მათ შორის: კრედიტზე, დასაქმებაზე, ჯანმრთელობასა და საჯარო სერვისებზე. ამ თვალსაზრისით, მათი ოპერირებისა და ფუნქციონირების მარეგულირებელი წესები თავიანთი არსით პოლიტიკურია.

ამ მიზეზით, მონაცემთა დაცვის საზედამხედველო ორგანოების როლი არ არის მხოლოდ კანონთან შესაბამისობის უზრუნველყოფა. ისინი არიან კონსტიტუციური ინსტიტუტები, რომლებსაც აქვთ სამართლებრივი უფლებამოსილებები, ტექნიკური კომპეტენცია და დამოუკიდებლობა.

როგორც ითქვა, ამ პირობებში მონაცემთა დაცვის საზედამხედველო ორგანოების (“DPAs”) ინსტიტუციური დამოუკიდებლობა დემოკრატიულ გარანტიად განიხილება. “GDPR”-ის 52-ე მუხლი ადგენს, რომ მონაცემთა დაცვის საზედამხედველო ორგანოებმა უნდა იმოქმედონ სრული ავტონომიითა და დამოუკიდებლობით, გარე გავლენისგან თავისუფლად. ამ დამოუკიდებლობამ მათ საშუალება უნდა მისცეს, წინააღმდეგობა გაუწიონ პოლიტიკურ და ეკონომიკურ ზეწოლას, განსაკუთრებით იმ შემთხვევებში, რომლებიც მოიცავს გავლენიან მულტინაციონალურ ტექნოლოგიურ პროვაიდერებს.

ამ მოდელის ღირებულება გამოცდილებით დადასტურდა. იტალიის მონაცემთა დაცვის ორგანოს (“Garante”) მიერ “ChatGPT6”-ის გამოძიება, რომელმაც მონაცემთა დამუშავების დროებითი შეზღუდვა, რამდენიმე მაკორექტირებელი ღონისძიება და ჯარიმა გამოიწვია, განხორციელდა დამოუკიდებლად, მაგრამ ევროპელ კოლეგებთან და სამოქალაქო საზოგადოებასთან დიალოგში. მან აჩვენა, რომ ფუნდამენტური უფლებების დაცვა შესაძლებელია იმ შემთხვევებშიც კი, როდესაც სწრაფად ვითარდებოდა და დიდ ყურადღებას იქცევდა.

თუმცა უზრუნველყოფილი უნდა იყოს, რომ ინსტიტუციური დამოუკიდებლობა თანაზომიერი იყოს ინსტიტუციურ შესაძლებლობებთან. ეფექტიანი ზედამხედველობა მოითხოვს სამართლებრივ გარკვეულობას,

[6] იტალიის მონაცემთა დაცვის ორგანოს („Garante“) გამოძიებამ გამოავლინა “OpenAI”-ის მიერ “GDPR”-ის რამდენიმე დარღვევა, რომლებიც ეხებოდა მომხმარებლის პერსონალური მონაცემების დამუშავებას. აღნიშნული დარღვევები მოიცავდა: გამჭვირვალობის უზრუნველყოფისა და მომხმარებლებისთვის საჭირო ინფორმაციის მიწოდების ვალდებულების შეუსრულებლობას, ასაკის ვერიფიკაციის ადეკვატური მექანიზმების დანერგვის ვალდებულების შეუსრულებლობას, 13 წლამდე არასრულწლოვნების შეუსაბამო მასალების გამჟღავნების პოტენციურ რისკს, კიბერუსაფრთხოების ინციდენტის შესახებ შესაბამისი მხარეების ინფორმირების ვალდებულების შეუსრულებლობას და გადაუდებელი საინფორმაციო კამპანიის ჩატარების შესახებ წინა დავალების უგულებელყოფას. მეტი ინფორმაციისთვის იხილეთ: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432>.

ტექნიკურ ექსპერტიზასა და ოპერაციულ რესურსებს. ფაქტობრივად, პერსონალურ მონაცემთა დაცვის უწყების (“DPA”) თანამშრომლებს უნდა შეეძლოთ არა მხოლოდ საჩივრებზე რეაგირება, არამედ ინსპექტირების ჩატარება, რთული ალგორითმული სისტემების განმარტება და სტრატეგიული პროგნოზირების განხორციელება. ასეთი ინსტიტუციური შესაძლებლობები, დამოუკიდებლობის მოთხოვნასთან ერთად, მიზნად ისახავს იმის უზრუნველყოფას, რომ “DPA”-ებს შეეძლოთ ტექნოლოგიური ტენდენციების წინასწარ განჭვრეტა ან მათ განვითარებაში დროული ჩარევა.

4. *“Ex Post”*– იდან “*Ex Ante”*– მდე: ზედამხედველობის მოდელის გარდაქმნა

სრულიად ნათელია, რომ ტრადიციული მარეგულირებელი მოდელი, რომელიც *ex post* აღსრულებას ეფუძნება, ყოველთვის არ არის შესაფერისი, როდესაც საქმე გვაქვს ხელოვნური ინტელექტის სწრაფ ტემპთან, უზარმაზარ მასშტაბსა და რთულ ბუნებასთან. მიზანშეწონილია ჩარევა ზიანის დადგომამდე, რადგან ეს ზედამხედველობას უფრო ეფექტიანს გახდის. უნდა განვიხილოთ ზედამხედველობის ახალი პარადიგმა, კერძოდ, პარადიგმა, რომელიც აერთიანებს *ex post* უფლებამოსილებებს *ex ante* ჩართულობასთან.

ეს ცვლილება ნიშნავს, რომ უწყებებმა უნდა განახორციელონ უფრო აქტიური როლი ხელოვნური ინტელექტის სისტემების შემუშავებასა და გამოყენებაში. მაგალითად, ისეთი ინსტრუმენტი, როგორიცაა მარეგულირებელი სანდბოქსები (“regulatory sandboxes”), ეხმარება მონაცემთა დაცვის საზედამხედველო ორგანოებსა და დეველოპერებს, ერთად იმუშაონ რისკების გამოსავლენად და შესამცირებლად კონტროლირებად გარემოში. ადრეულ დიალოგს აქვს პოტენციალი, შეამციროს გაურკვევლობა და ხელი შეუწყოს შესაბამისობას დიზაინის ეტაპზევე (“compliance by design”). [7]

ასევე სასიცოცხლოდ მნიშვნელოვანია, რომ მონაცემთა დაცვის საზედამხედველო ორგანოებმა (“DPAs”) წვლილი შეიტანონ რისკების კლასიფიკაციის სისტემების განსაზღვრაში. ეს აუცილებელია იმისათვის, რომ მონაცემთა დაცვის პრინციპები ხელოვნური ინტელექტის რეგულირების არქიტექტურაში იყოს ინტეგრირებული. გარდა ამისა, მონაცემთა დაცვის საზედამხედველო ორგანოებს, როდესაც ეს შესაძლებელია, წვდომა უნდა ჰქონდეთ ხელოვნური ინტელექტის ტექნიკურ საფუძვლებზე:

[7] ამ მიზეზით, 2021 წლიდან, იტალიის მონაცემთა დაცვის ორგანო არის ფინანსთა და ეკონომიკის სამინისტროს მიერ დაარსებული “FinTech” საკოორდინაციო კომიტეტის მუდმივი წევრი. კომიტეტი ზედამხედველობას უწევს მარეგულირებელი „სანდბოქსის“ ინიციატივებს, რომლებიც შექმნილია ინოვაციური ფინანსური გადაწყვეტილებების შესამოწმებლად, მათ შორის, ხელოვნურ ინტელექტსა და მონაცემებზე ორიენტირებულ ტექნოლოგიებზე დაფუძნებულ გადაწყვეტილებებს. „სანდბოქსის“ ინიციატივამ განაცხადების პირველი ფანჯრის გახსნის შემდეგ 53 განაცხადი მიიღო. მათგან 13 დამტკიცდა. მეტი ინფორმაციისთვის იხილეთ: <https://www.dt.mef.gov.it/it/attivita_istituzionali/sistema_bancario_finanziario/fintech/index_bak.html>.

დოკუმენტაციაზე, საწვრთნელ მონაცემებსა და ალგორითმულ ლოგიკაზე, რადგან ოპერაციული გამჭვირვალობა ამ პროცესის არსებითი კომპონენტია.

ამ ფენებზე წვდომის გარეშე აღსრულება სრულ პოტენციალს ვერ მიაღწევს.

ამ თვალსაზრისით, ალგორითმული ინსპექტირება, რომლიც ინტერდისციპლინური გუნდების მიერ ხორციელდება, საკვანძო ინსტრუმენტს წარმოადგენს. შესაძლებელია, რომ ამ შესწავლამ გამოავლინოს არა მხოლოდ კანონთან შეუსაბამობა, არამედ სტრუქტურული რისკებიც, როგორებიცაა: მიკერძოება, დისკრიმინაცია ან გასაჩივრების ნაკლებობა. ასეთი პრაქტიკების ინტეგრაციას ხელოვნური ინტელექტის მმართველობის სისტემების ფარგლებში აქვს პოტენციალი, უზრუნველყოს კანონთან შესაბამისობის გადამოწმება. მიზანი არ არის გადაჭარბებული რეგულირების დაწესება, არამედ სამართლებრივი სიცხადის უზრუნველყოფა. პასუხისმგებლიანი ინოვაცია უფრო მარტივი მისაღწევია, როდესაც მოლოდინები წინასწარ არის ცნობილი. იმისათვის, რომ უზრუნველყოფილ იქნას აღსრულებისა და ზედამხედველობის ამგვარი მექანიზმების ეფექტიანობა, ისინი უნდა იყოს ინტეგრირებული ხელოვნური ინტელექტის მართვის უფრო ფართო, კოორდინირებულ მიდგომაში.

5. კოორდინირებული მმართველობა და უფლებებზე დაფუძნებული კონვერგენცია

ხელოვნური ინტელექტის მართვაში ჩართულნი არიან სხვადასხვა დაინტერესებული მხარეები, როგორიცაა: მარეგულირებელი ორგანოები, კონკურენციისა და მომხმარებელთა დაცვის ორგანოები და, რა თქმა უნდა, მონაცემთა დაცვის საზედამხედველო ორგანოები (“DPAs”). ეს განპირობებულია ხელოვნური ინტელექტის რთული ბუნებით, რომელსაც გავლენა აქვს მრავალ სფეროზე. ამან შეიძლება წარმოშვას გამოწვევები, როგორებიცაა: შეუსაბამობა, ფრაგმენტაციის პოტენციური რისკები და იურისდიქციული კონფლიქტი.

ამიტომ კონსტრუქციული დიალოგის სულისკვეთებით ძალისხმევა უნდა მიიმართოს ეფექტიანი და უფლებებზე დაფუძნებული კოორდინაციის უზრუნველსაყოფად, რათა თავიდან იქნას აცილებული შედეგები, რომლებიც შეიძლება საზიანო იყოს ყველასთვის.

ეს პროცესი მოითხოვს ინსტიტუციათაშორისი თანამშრომლობის ფორმალური მექანიზმების არსებობას. მაგალითად, მუდმივი საკოორდინაციო პლატფორმები, ერთობლივი სამუშაო ჯგუფები და საერთო რისკების რეესტრები შეიძლება იყოს მარეგულირებელი სტრატეგიების შესაბამისობაში მოყვანის საშუალება. შესაძლოა, ღირდეს იმის განხილვა, უნდა ჰქონდეთ თუ არა მონაცემთა დაცვის საზედამხედველო ორგანოების (“DPA”) წევრებს ამ პლატფორმებზე უფრო ცენტრალური როლი, ნაცვლად პერიფერიული კონსულტანტების როლისა.

საერთაშორისო დონეზე, კონვერგენციის ინიციატივები, როგორებიცაა: „მონაცემთა დაცვის საზედამხედველო ორგანოების საგაზაფხულო კონფერენცია“, “G7”, “OECD” („ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია“) და ევროპის საბჭო, გვთავაზობს პერსპექტიულ ჩარჩოებს, რომლებსაც აქვთ პოტენციალი, წვლილი შეიტანონ საერთო სტანდარტებისა და ზედამხედველობის პრიორიტეტების ჩამოყალიბებაში.

6. დასკვნა

ხელოვნურ ინტელექტს (“AI”) გავლენა აქვს ინდივიდებს, ინსტიტუტებსა და ბაზრებს შორის ძალაუფლების ურთიერთობებზე. მას აქვს პოტენციალი, მოახდინოს გავლენა იმ ფორმაზე, თუ როგორ მიიღება გადაწყვეტილებები, ცირკულირებს ინფორმაცია და ხორციელდება ან უარყოფილია უფლებები. ამ კონტექსტში, ხელოვნური ინტელექტის მართვა შეიძლება განიმარტოს, როგორც ძალაუფლების მართვის საშუალება.

მონაცემთა დაცვის საზედამხედველო ორგანოებს (“DPAs”) უნიკალური როლი აქვთ მმართველობის კანონიერების, პროპორციულობისა და ანგარიშვალდებულების უზრუნველყოფაში. ისინი აერთიანებენ სამართლებრივ უფლებამოსილებას, ტექნიკურ ექსპერტიზას და ინსტიტუციურ დამოუკიდებლობას.

მათი როლი არ არის ინოვაციის შეფერხება, არამედ მისი წარმართვა დემოკრატიული პრინციპების ფარგლებში. ამის გამო ისინი არა მხოლოდ მარეგულირებელი ორგანოები, არამედ ფუნდამენტური უფლებების კონსტიტუციური გარანტორებიც არიან.

ამ პოტენციალის მისაღწევად აუცილებელია, რომ მონაცემთა დაცვის საზედამხედველო ორგანოები სრულად იყვნენ ინტეგრირებული ხელოვნური ინტელექტის მმართველობით ჩარჩოებში, განიხილონ თავიანთი მანდატის გაფართოება რეაქტიული აღსრულებიდან პროაქტიულ ჩართულობამდე და აღიჭურვონ ადეკვატური რესურსებითა და სამართლებრივი ინსტრუმენტებით.

ბიბლიოგრაფია:

1. Italian Data Protection Authority, Comunicato Stampa - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro, 2023. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432>.
2. Ministero dell'Economia e delle Finanze. Sistema bancario finanziario <https://www.dt.mef.gov.it/it/attivita_istituzionali/sistema_bancario_finanziario/fintech/index_bak.htm>l.
3. Office of the Privacy Commissioner of Canada, OPC launches investigation into ChatGPT, 2023. <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/>.
4. Personal Information Protection Commission, Japan, Hangzhou DeepSeek Artificial Intelligence's privacy policy, 2025. <https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/>.
5. 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 [2016] OJ L119.

ოთარ ჩახუნაშვილი[*]
სალომე სიგუა[**]

ხელოვნური ინტელექტისა და პერსონალურ მონაცემთა დაცვის რეგულირების სამართლებრივი ასპექტები: ეროვნული და საერთაშორისო პრაქტიკის მიმოხილვა[***]

ინფორმაციული ტექნოლოგიების სწრაფმა განვითარებამ და ხელოვნური ინტელექტის (AI) ინტეგრაციამ საზოგადოებრივ და კერძო სექტორებში მკვეთრად გააფართოვა მონაცემთა დამუშავების პროცესები. აღნიშნულ პროცესს თან ახლავს მონაცემთა დაცვის მნიშვნელოვანი სამართლებრივი და ეთიკური გამოწვევები. სტატია მიზნად ისახავს ხელოვნური ინტელექტის სისტემების მიერ პერსონალური მონაცემების დამუშავების სამართლებრივი ჩარჩოს ანალიზს როგორც საერთაშორისო, ისე ეროვნულ კანონმდებლობაში.

შესწავლილია არსებული რეგულაციები, მათი ეფექტიანობა და შესაბამისობა თანამედროვე ტექნოლოგიურ რეალობასთან. აქცენტი კეთდება იმაზე, თუ რამდენად ადეკვატურად პასუხობს მოქმედი სამართლებრივი ნორმები AI-ის უნიკალურ შესაძლებლობებსა და რისკებს, მათ შორის, ალგორითმული მიკერძოების, გამჭვირვალობის და მომხმარებელთა უფლებების დაცვის კუთხით.

საკვანძო სიტყვები: *ხელოვნური ინტელექტი, პერსონალურ მონაცემთა დაცვა, ალგორითმული მიკერძოება, მომხმარებელთა უფლებების დაცვა.*

---

[*] სამართლის დოქტორი, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასისტენტ-პროფესორი, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის პირველი მოადგილე.

[**] ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის მოწვეული ლექტორი.

[***] სტატია მომზადებულია საქართველოს შოთა რუსთაველის ეროვნული სამეცნიერო ფონდის ახალგაზრდა მეცნიერთა გრანტით დაფინანსების კონკურსის (YS-23-3460) ფარგლებში.

1. შესავალი

ტექნოლოგიური პროგრესის პროცესში წამოიჭრება არაერთი მნიშვნელოვანი საკითხი, რომელთა შესრულებაც აუცილებელ პირობად მიიჩნევა დემოკრატიულ საზოგადოებაში. პერსონალურ მონაცემთა დაცვა ერთ-ერთი იმ უფლებათაგანია, რომელზეც ყურადღება გამახვილდა სოციალური ურთიერთობებისა და საამისო საშუალებათა განვითარების პარალელურად. პერსონალური მონაცემის დაცვის უფლება მოიაზრება თავად პერსონალური მონაცემების უფლების ან კონფიდენციალობის (“Privacy”) უფლების ქვეშ. ერთი შეხედვით, აღნიშნული ორი უფლება ერთმანეთის ანალოგია და შეიძლება სინონიმებად გამოვიყენოთ. ევროპის მასშტაბით, აღნიშნული უფლებები მდგრადი დემოკრატიის სასიცოცხლო კომპონენტებად მიიჩნევა.

უდავოა, რომ ხელოვნური ინტელექტი კაცობრიობის ტექნოლოგიური განვითარების ერთ-ერთი ბოლო სამეცნიერო მიღწევაა, რომელიც უახლოეს მომავალში ბევრ სფეროში იქნება გამოყენებული და „დაიპყრობს“ კიდეც მას. მეოთხე ინდუსტრიული რევოლუცია თავისი არსით შეიძლება დავახასიათოთ ისეთი ახალი ტექნოლოგიების განვითარებით, როგორებიც არის: ხელოვნური ინტელექტი, რობოტიკა, ნანოტექნიკა, კვანტური გამოთვლა, ბიოტექნოლოგია, ნივთების ინტერნეტი (IoT) და ბლოკჩეინი, რომლებიც შეცვლის საზოგადოების ცხოვრებისა და მუშაობის სტილს.

ხელოვნური ინტელექტის გარშემო არსებობს მრავალი კითხვა, თუმცა დღესდღეობით ყველაზე აქტუალური საკითხი ხელოვნური ინტელექტის მიერ პერსონალური მონაცემების დამუშავებას უკავშირდება. აღნიშნული ტექნოლოგია არის სწრაფად განვითარებადი და მონაცემები, რომლებსაც ის ამუშავებს, არის სხვადასხვა მოცულობისა და შინაარსის. ხელოვნური ინტელექტი მრავალი წყაროდან მოპოვებული ინფორმაციის საფუძველზე სწავლობს და წინასწარ შედგენილი ალგორითმის მიხედვით ამუშავებს დიდი რაოდენობით მონაცემებს. აღნიშნულიდან გამომდინარე, შეიძლება ითქვას, რომ მონაცემები გახდა ხელოვნური ინტელექტის ერთადერთი „საკვები“.

2. პერსონალური მონაცემების მომწესრიგებელი ეროვნული და საერთაშორისო საკანონმდებლო აქტების ანალიზი

პერსონალურია მონაცემი ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. აგრეთვე, პერსონალურ მონაცემებს წარმოადგენს სხვადასხვა ინფორმაციის ერთობლიობა, რომელთა დამუშავება პირის იდენტიფიცირების საშუალებას იძლევა.[1] ევროკავშირისა და ევროპის საბჭოს კანონმდებლობა „პერსონალურ

[1] European Commission, What is personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> [17.01.2024].

მონაცემებს“ განმარტავს, როგორც ინფორმაციას იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირის შესახებ,[2] რომლის ვინაობა ცნობილია ან შეიძლება დადგინდეს დამატებითი ინფორმაციის საფუძველზე. არის თუ არა პირი იდენტიფიცირებადი, ამის დასადგენად მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ან სხვა სუბიექტმა უნდა გაითვალისწინოს ყველა გონივრული საშუალება, რომელთა გამოყენებაც შესაძლებელია პირის პირდაპირი ან ირიბი იდენტიფიცირებისათვის.[3]

სამართლებრივი სახელმწიფოს პრინციპი დემოკრატიული სახელმწიფოს ერთ-ერთი უმნიშვნელოვანესი წინაპირობაა.[4] სამართლებრივ სახელმწიფოში უმაღლეს სოციალურ ღირებულებებად მიჩნეულია ადამიანი, მისი ღირსება, უფლებები და თავისუფლებები. შესაბამისად, სახელმწიფო ემსახურება ადამიანებს, რომლებიც თავად არიან სახელმწიფო ხელისუფლების წყარო.[5]

მას შემდეგ, რაც სოციალური და ეკონომიკური აქტივობების უმრავლესობა ონლაინ ხორციელდება, უფრო მეტი მნიშვნელობა მიენიჭა პერსონალური მონაცემებისა და კონფიდენციალობის უფლების დაცვას. უახლესი ინფორმაციით, მსოფლიოს 194 ქვეყნიდან 137 ქვეყანას აქვს მიღებული პერსონალურ მონაცემთა დაცვის მომწესრიგებელი საკანონმდებლო აქტები, რაც მსოფლიოს ქვეყნების 71%-ს შეადგენს. აღსანიშნავია, რომ 9% (დაახლოებით 17 სახელმწიფო) საკანონმდებლო აქტის შემუშავების პროცესშია, 15%-ს (დაახლოებით 30 სახელმწიფო) არ აქვს მიღებული საკანონმდებლო აქტი, ხოლო 5%-ზე (დაახლოებით 9 სახელმწიფო) ინფორმაცია არ იძებნება.[6] საგულისხმოა, რომ ქვეყნების უმრავლესობა, რომლებსაც არ აქვს მიღებული პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკანონმდებლო აქტები, არის აფრიკის კონტინენტის, ხოლო ქვეყნები, რომლებზეც ინფორმაცია არ იძებნება, არის როგორც აფრიკის, აგრეთვე ინდონეზიის ქვეყნები.

პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საერთაშორისო სამართლებრივი აქტების მიღება დაიწყო 1970-იან წლებში[7], როდესაც ინფორმაციული ტექნოლოგიები ინტენსიურ გამოყენებას დაექვემდებარა და რამდენიმე სახელმწიფომ მიიღო კანონმდებლობა საჯარო ხელისუფლებისა და მსხვილი კომპანიების მიერ პერსონალური ინფორმაციის დამუშავების გასაკონტროლებლად. შედეგად, ევროპის მასშტაბით შეიქმნა მონაცემთა

[2] მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 4 (1); ევროპის საბჭოს კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ("კონვენცია 108+“), მუხლი 2 (ა).

[3] მონაცემთა დაცვის ძირითადი რეგულაცია, პრეამბულა, პუნქტი 26.

[4] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 მარტის N1/4/757 გადაწყვეტილება საქმეზე „საქართველოს მოქალაქე გიორგი კრავეიშვილი საქართველოს მთავრობის წინააღმდეგ“, II-4.

[5] სამეცნიერო ჟურნალი “ახალგაზრდა ადვოკატები“ N5, „ახალგაზრდა ადვოკატებისა“ და „ადვოკატთა საგანმანათლებლო ცენტრის“ ერთობლივი გამოცემა, თბილისი, 2016, 34.

[6] UN Trade&Development, Data Protection and Privacy Legislation, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> [17.01.2024].

[7] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, 2018, გვ. 22.

დაცვის ინსტრუმენტები[8] და წლების განმავლობაში მონაცემთა დაცვა დამოუკიდებელ ღირებულებად ჩამოყალიბდა, რომელიც არ განიხილება პირადი ცხოვრების პატივისცემის უფლების ქვეშ. ევროკავშირის სამართლის სისტემაში მონაცემთა დაცვა ფუნდამენტურ უფლებად არის აღიარებული პირადი ცხოვრების პატივისცემის უფლებისგან განცალკევებულად.

გაეროს სამართლებრივი ჩარჩო პერსონალურ მონაცემთა დაცვას ფუნდამენტურ უფლებად არ მიიჩნევს, მიუხედავად იმისა, რომ პირადი ცხოვრების დაცვა საერთაშორისო სამართლის სისტემამ დიდი ხნის წინ აღიარა ფუნდამენტურ უფლებად, კერძოდ, ადამიანის უფლებათა საყოველთაო დეკლარაციის ("UDHD") მე-12 მუხლი ეხება პირადი და ოჯახური ცხოვრების პატივისცემას.[9] აღნიშნული კონვენცია პირველი საერთაშორისო ინსტრუმენტია, რომლითაც დადგინდა, რომ ადამიანს აქვს უფლება, საკუთარი პირადი სივრცე დაიცვას სხვისი, განსაკუთრებით კი სახელმწიფოს ჩარევისგან. "UDHD"-ს სავალდებულო იურიდიული ძალა არ გააჩნია, თუმცა აქვს ადამიანის უფლებათა საერთაშორისო სამართლის ფუძემდებლური ინსტრუმენტის მნიშვნელოვანი სტატუსი და გავლენა მოახდინა ევროპაში ადამიანის უფლებათა ინსტრუმენტების შექმნაზე. დეკლარაცია ერთმანეთისგან მიჯნავს პირად ცხოვრებაში ჩარევის დაუშვებლობას, როგორც სახელმწიფო ორგანოების, ასევე კერძო პირების (მეზობელი, დამსაქმებელი და ა. შ.) მხრიდან.[10]

ადამიანის უფლებათა საყოველთაო დეკლარაციის გარდა, გაეროს სხვადასხვა საერთაშორისო აქტით დადგენილია საერთაშორისო სტანდარტები კონფიდენციალობისა და პირადი ცხოვრების დაცვის შესახებ. დეკლარაციის შემდეგ პირველი ასეთი აქტი იყო საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ ("ICCPR"), რომელიც ძალაში 1976 წელს შევიდა და განამტკიცებს, რომ „არავინ უნდა დაექვემდებაროს მის პირად და ოჯახურ ცხოვრებაში საცხოვრებლის ან კორესპონდენციის ხელშეუხებლობაში თვითნებურ ან უკანონო ჩარევას ან ღირსებისა და რეპუტაციის უკანონო ხელყოფას"[11]. "ICCPR" არის საერთაშორისო ხელშეკრულება, რომელიც ხელმომწერ მხარეებს ავალდებულებს სამოქალაქო უფლებების, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის უზრუნველყოფასა და დაცვას. 1989 წელს გენერალურმა ასამბლეამ მიიღო საერთაშორისო კონვენცია ყველა მიგრანტი მუშაკისა და მათი ოჯახის წევრების დაცვის შესახებ, რომლის მიხედვითაც, დაუშვებელია მიგრანტი მუშაკისა და მისი ოჯახის წევრების მიმართ თვითნებური ან უკანონო ჩარევა კონფიდენციალობის, სახლის, ოჯახის, პირადი მიმოწერისა და სხვა

[8] ევროკავშირმა მონაცემთა დაცვის პირველი ყოვლისმომცველი ინსტრუმენტი 1995 წელს შეიმუშავა: ეს იყო დირექტივა 95/46/EC, რომელიც შეეხება ფიზიკური პირების დაცვას პერსონალურ მონაცემთა დამუშავებისა და თავისუფალი მიმოცვლისას.

[9] ადამიანის უფლებათა საყოვეთაო დეკლარაციის მე-12 მუხლი.

[10] *Alfredsson G., Eide Asbjorn,* The Universal Declaration of Human Rights A Common Standard of Achievement, Hague, Kluwer Law International, 1999, 257-258.

[11] საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ (ICCPR) 1976, მუხლი 17.

სახით.[12] 2006 წელს პირადი ცხოვრების ხელშეუხებლობისა და კონფიდენციალობის უფლება შეზღუდული შესაძლებლობის მქონე პირებისთვის განსაზღვრა კონვენციამ[13] შეზღუდული შესაძლებლობების პირთა უფლებების შესახებ, რომლის შესრულებაც სავალდებულოა ხელმომწერი მხარეების მიერ.

ადამიანის უფლებათა საყოველთაო დეკლარაციის მიღებიდან მალევე პირადი ცხოვრების პატივისცემის უფლება აღიარა ევროპამაც, კერძოდ, 1950 წელს შეიქმნა ადამიანის უფლებათა ევროპული კონვენცია ("ECHR"), რომელიც ითვალისწინებს პიირადი ცხოვრების ხელშეუხებლობის ფუნდამენტურ უფლებას.[14] "ECHR"-ის მე-8 მუხლის თანახმად, ყველას აქვს უფლება, პატივი სცეს მის პირად და ოჯახურ ცხოვრებას, საცხოვრებელსა და მიმოწერას; დაუშვებელია ამ უფლების განხორციელებაში საჯარო ხელისუფლების ჩარევა, გარდა ისეთი შემთხვევებისა, როდესაც ასეთი ჩარევა ხორციელდება კანონის შესაბამისად, მნიშვნელოვანი და ლეგიტიმური საჯარო ინტერესების დასაცავად და აუცილებელია დემოკრატიულ საზოგადოებაში.

პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საერთაშირისო სამართლებრივი აქტების მიღება ძირითადად დაიწყო მე-20 საუკუნის 60-იანი და 80-იანი წლების პერიოდში. კერძოდ, ჯერ კიდევ 1960-იან წლებში ინფორმაციული ტექნოლოგიების გამოჩენასთან ერთად, გაჩნდა მზარდი მოთხოვნა პერსონალურ მონაცემთა დაცვის დეტალურ წესებზე. 70-იანი წლების შუა პერიოდისთვის ევროპის საბჭოს მინისტრთა კომიტეტმა არაერთი რეზოლუცია მიიღო პერსონალურ მონაცემთა დაცვის შესახებ, რომლებიც ევროპული კონვენციის მე-8 მუხლზე მიუთითებდა.[15] პირველი საერთაშორისო ინსტრუმენტი, რომელიც ეხება პერსონალური მონაცემების დაცვას, არის ევროპის საბჭოს კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ"[16], რომელსაც ევროპის საბჭოს 108-ე კონვენციასაც უწოდებენ. კონვენცია მიღებული არის 1981 წელს, ხოლო საქართველოს პარლამენტმა მისი რატიფიცირება მოახდინა 2005 წელს.[17] აღნიშნული კონვენცია იყო და დღემდე რჩება სავალდებულო იურიდიული ძალის მქონე ერთადერთ საერთაშორისო ინსტრუმენტად მონაცემთა დაცვის სფეროში. იგი იცავს ფიზიკური პირის უფლებას, იცოდეს, თუ რა ინფორმაცია ინახება მასზე და, საჭიროების შემთხვევაში, მოითხოვოს

[12] ყველა მიგრანტი მუშაკისა და მათი ოჯახის წევრების დაცვის შესახებ კონვენცია, მუხლი 14.
[13] შეზღუდული შესაძლებლობების მქონე პირთა უფლებების კონვენცია, მუხლი 22.
[14] ადამიანის უფლებათა ევროპული კონვენცია, 1950, მუხლი 8.
[15] ევროპის საბჭოს მინისტრთა კომიტეტი (1973), რეზოლუცია (73) 22 კერძო სექტორში მონაცემთა ელექტრონული ბანკის პირისპირ ფიზიკურ პირთა პირადი ცხოვრების დაცვის შესახებ, 1973 წლის 26 სექტემბერი; ევროპის საბჭოს მინისტრთა კომიტეტი (1974), რეზოლუცია (74) 29 საჯარო სექტორში მონაცემთა ელექტრონული ბანკის პირისპირ ფიზიკურ პირთა პირადი ცხოვრების დაცვის შესახებ, 1974 წლის 20 სექტემბერი.
[16] ევროპის საბჭო, კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ CETS No. 108, 1981.
[17] EU Treaty Office, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108> [20.01.2024].

მისი შესწორება. კონვენციით გათვალისწინებული უფლებების შეზღუდვა ნებადართულია მხოლოდ მაშინ, როცა არსებობს აღმატებული ინტერესები, როგორებიცაა სახელმწიფო უსაფრთხოება ან თავდაცვა. ამასთან, კონვენცია ადგენს პერსონალურ მონაცემთა თავისუფალ გადაცემას ხელშემკვრელ მხარეებს შორის და გარკვეულ შეზღუდვებს იმ სახელმწიფოებისთვის, რომლებშიც სამართლებრივი რეგულაციები არ უზრუნველყოფს მონაცემთა სათანადო დაცვას.

2001 წელს მიიღეს 108-ე კონვენციის დამატებითი ოქმი, რომელიც მოიცავს დებულებებს მონაცემთა საერთაშორისო გადაცემაზე იმ სახელმწიფოებისათვის, რომლებიც კონვენციის მხარეები არ არიან (ე. წ. „მესამე ქვეყნები“), ასევე, სავალდებულო მოთხოვნას შიდასახელმწიფოებრივ დონეზე მონაცემთა დაცვის საზედამხედველო ორგანოს შექმნის შესახებ და, რაც ყველაზე მნიშვნელოვანია, დამატებითი ოქმით გაზრდილი არის კონვენციის მოქმედების სფერო.[18]

1995 წლიდან 2018 წლის მაისამდე ევროკავშირის მონაცემთა დაცვის მთავარი სამართლებრივი ინსტრუმენტი იყო ევროპის პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, რომელიც შეეხებოდა პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვას და ამგვარი მონაცემების თავისუფალ მიმოცვლას (მონაცემთა დაცვის დირექტივა).[19] დირექტივა მიღებულია 1995 წელს. ამ დროისათვის ევროკავშირის რამდენიმე წევრ სახელმწიფოში უკვე მოქმედებდა კანონები მონაცემთა დაცვის შესახებ და საჭირო იყო მათი ჰარმონიზება, რათა უზრუნველყოფილიყო პერსონალურ მონაცემთა მაღალი სტანდარტებით დაცვა და მათი თავისუფალი გადაცემა სხვადასხვა წევრ სახელმწიფოს შორის. შიდა ბაზარზე საქონლის, კაპიტალის, მომსახურებისა და ადამიანების თავისუფალი გადაადგილება მოითხოვდა მონაცემთა თავისუფალ მოძრაობასაც, რაც შეუძლებელი იქნებოდა წევრ ქვეყნებში მონაცემთა დაცვის თანაბრად მაღალი სტანდარტის გარეშე.

მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”) ევროპის კავშირმა მიიღო 2016 წელს, რათა ჩაენაცვლებინა მანამდე მოქმედი დირექტივა, რომელიც მიღებული იყო ჯერ კიდევ ინტერნეტის ახლად შემქნის დროს, 1995 წელს. რეგულაციამდე არსებული დირექტივა ვერ პასუხობდა თანამედროვე ტექნოლოგიებისა და ინტერნეტით გამოწვეულ გამოწვევებს, ამიტომ საჭირო გახდა რეფორმის განხორციელება და 1995 წლის დირექტივის ახლით ჩანაცვლება.[20] მონაცემთა დაცვის ძირითადი რეგულაციის რეგულაციას აქვს პირდაპირი მოქმედების იურიდიული ძალა, თუმცა მასთან სრული

[18] ევროპის საბჭო, კონვენციის დამატებითი ოქმი, რომელიც შეეხება ფიზიკური პირების დაცვას პერსონალურ მონაცემთა ავტომატური დამუშავებისას, საზედამხედველო ორგანოებსა და მონაცემთა საზღვართშორის მიმოცვლასთან დაკავშირებით, CETS No. 181, 2001.

[19] ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 1995 L 281.

[20] EDPS, The History of the General Data Protection Regulation, <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [15.01.2024].

შესაბამისობისათვის წევრმა სახელმწიფოებმა განაახლეს მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონმდებლობა.

საქართველოს კონსტიტუცია განამტკიცებს ადამიანის პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის, ინფორმაციული თვითგამორკვევის უფლებებს; ამასთან, ადგენს, რომ ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, ფინანსებსა თუ სხვა პირად საკითხებთან, არავისთვის უნდა იყოს ხელმისაწვდომი მისი თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობისა თუ სხვათა უფლებების დასაცავად. აღნიშნული პერსონალური მონაცემების დაცვის კონსტიტუციურ საფუძვლად უნდა იქნას მიჩნეული, რომელთა რეალიზების გარანტიები სხვადასხვა საკანონმდებლო აქტით, მათ შორის, საქართველოს კანონით „პერსონალურ მონაცემთა დაცვის შესახებ“, არის დადგენილი.

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ საბაზისო ნორმატიული აქტია პერსონალურ მონაცემთა დაცვის სფეროში, რომლის პირველადი რედაქციაც ამოქმედდა 2014 წლის 1 ნოემბერს. მომდევნო წლებში საერთაშორისო სტანდარტებთან დაახლოების მიზნით მასში რამდენიმე მნიშვნელოვანი ცვლილება განხორციელდა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის მიღებით პერსონალურ მონაცემთა დაცვის სფეროს მარეგულირებელი ეროვნული კანონმდებლობა არსებითად დაუახლოვდა ევროპულ სტანდარტს, რაც, თავის მხრივ, ქვეყანაში მონაცემთა დაცვის მიმართულებით საერთაშორისოდ აღიარებული პრინციპებისა და საუკეთესო პრაქტიკის დამკვიდრებას უზრუნველყოფს. ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციისა და მოდერნიზებული 108-ე კონვენციის მიღების შემდეგ საჭირო გახდა ეროვნული კანონმდებლობის უფრო მეტად დაახლოება ევროპულ სტანდარტებთან. შესაბამისად, 2023 წელს საქართველოს პარლამენტმა მიიღო ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომელიც ამოქმედდა 2024 წლის 1 მარტს.[21]

ახალი კანონით გათვალისწინებული სიახლეებიდან დამუშავებისთვის პასუხისმგებელი პირებისთვის დაკისრებულ ვალდებულებათაგან, ტექნოლოგიური პროგრესით გამოწვეული რისკების მართვის თვალსაზრისით, მნიშვნელოვანი ინსტიტუტებია მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების და მონაცემთა მეტად დაფარვის პრიორიტეტის (ე. წ. “Privacy by Design/by Default”) გათვალისწინება. აღნიშნული პერსონალურ მონაცემთა დაცვის ქართული კანონმდებლობისთვის სიახლეს წარმოადგენს და, ახალი ტექნოლოგიების უსწრაფესი ტემპით განვითარების პირობებში, ადამიანის

[21] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 14/06/2023

უფლებების დარღვევის მომეტებული საფრთხეების წინსწრებით შეფასებას და მათ შემცირებას ისახავს მიზნად.

საქართველოს მოქმედი კანონმდებლობა, კერძოდ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი წარმოადგენს ძირითად საკანონმდებლო ჩარჩოს, რომელიც არეგულირებს მონაცემთა დამუშავების ძირითად პრინციპებს, აგრეთვე, მონაცემთა ავტომატიზებული დამუშავების (როგორიცაა, მათ შორის, AI სისტემები) სამართლებრივ ასპექტებს. კანონის თანახმად, მონაცემთა დამუშავება უნდა ეფუძნებოდეს ლეგიტიმურ მიზანს, კანონსაწინააღმდეგო ჩარევისგან დაცვის პრინციპს და იცავდეს მონაცემთა სუბიექტის უფლებებს, მათ შორის: ინფორმირების, წვდომის, ჩასწორების, წაშლისა და წინააღმდეგობის უფლებას.

3. ხელოვნური ინტელექტის მომწესრიგებელი ეროვნული და საერთაშორისო აქტების ანალიზი

უდავოა, რომ ხელოვნური ინტელექტი წარმოადგენს კაცობრიობის ტექნოლოგიური პროგრესის ერთ-ერთ უმნიშვნელოვანეს და თანამედროვე სამეცნიერო მიღწევას, რომელიც უახლოეს პერიოდში მრავალი სფეროს განვითარებას მნიშვნელოვნად შეცვლის და მასში მყარად მკვიდრდება. მეოთხე ინდუსტრიული რევოლუცია კი, თავის არსით, დაკავშირებულია ინოვაციური ტექნოლოგიების, მათ შორის, ხელოვნური ინტელექტის, რობოტიკის, ნანოტექნოლოგიების, კვანტური გამოთვლების, ბიოტექნოლოგიების, ნივთების ინტერნეტის (IoT) და ბლოკჩეინის განვითარებასთან – ტექნოლოგიებთან, რომლებიც მნიშვნელოვნად გარდაქმნის როგორც ჩვენს ყოველდღიურ ცხოვრებას, ასევე – შრომისა და საქმიანობის მოდელს.[22]

ხელოვნური ინტელექტი (AI) გულისხმობს კომპიუტერული მანქანების ინტელექტს, რომლებიც „ჭკვიანი აგენტებივით“ იქცევიან. ტერმინი AI გამოიყენება მაშინ, როდესაც კომპიუტერული მანქანა მიმართავს „კოგნიტური“ ფუნქციების იმიტაციას.[23]

პერსონალურ მონაცემთა დაცვის ძირითადი პრობლემები უკავშირდება, ერთი მხრივ, დამუშავებული პერსონალური მონაცემების მოცულობასა და ფართო სპექტრს, ხოლო, მეორე მხრივ, დამუშავებასა და მის შედეგებს. კომპლექსური ალგორითმებისა და კომპიუტერული პროგრამების დანერგვა, რათა მასობრივი მონაცემები გარდაიქმნას გადაწყვეტილების მიღების რესურსად, გავლენას ახდენს მონაცემთა სუბიექტის სხვადასხვა ჯგუფზე,

[22] *გაბისონია ზ.,* ინტერნეტ სამართალი და ხელოვნური ინტელექტი, „იურისტების სამყარო“, თბილისი 2022, 513.

[23] *Stuart Russel and Peter Norvig*, Artificial Intelligence: A Modern Approach (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, 27, 32–58, 968–972; *Stuart Russel and Peter Norvig*, Artificial Intelligence: A Modern Approach (3rd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, 2.

განსაკუთრებით, პროფილირებისა და დისკრიმინაციული მიდგომებისას და, საბოლოო ჯამში, წარმოქმნის მონაცემთა დაცვასთან დაკავშირებულ პრობლემებს.[24]

ხელოვნური ინტელექტის რეგულირება კომპლექსურ გამოწვევას წარმოადგენს მსოფლიოსთვის, რადგან იგი მოიცავს ეთიკურ, სამართლებრივ და ტექნიკურ ასპექტებს. ხელოვნური ინტელექტის სწრაფი განვითარებიდან გამომდინარე, სხვადასხვა სახელმწიფოსთვის გამოწვევად რჩება მისი სამართლებრივი მოწესრიგება. ამიტომ ძირითადად პოლიტიკის დოკუმენტების ან ეროვნული სტრატეგიების დონეზე ხორციელდება მისი რეგულირება. თავისთავად ხელოვნური ინტელექტის განვითარების სამოქმედო გეგმისა და ჩარჩო-დოკუმენტების დოკუმენტის მიღება პანაცეა არ არის. ამას ზოგიერთი ქვეყნის მიერ მიღებული დოკუმენტის არაპრაქტიკულობაც მოწმობს. თავად სიტყვა „სტრატეგია“ ერთ-ერთი ყველაზე ხშირად გამოყენებადი სიტყვაა თანამედროვე პოლიტოლოგიასა თუ მენეჯმენტში. მიუხედავად ამისა, მისი შეთანხმებული და ერთიანი დეფინიცია არ არსებობს. სტრატეგიაზე საუბრისას, პირველ რიგში, ასოცირება ხდება სტრატეგიულ გეგმასთან, რომელიც ხშირად დაწერილ დოკუმენტს წარმოადგენს.

ხელოვნური ინტელექტის განვითარების სახელმწიფო სტრატეგია 2017 წელს პირველად მიიღო კანადამ, ხოლო შემდეგ მას იაპონია და ჩინეთიც შეუერთდა. იმავე წელს ხელოვნური ინტელექტის სტრატეგია დაამტკიცა სინგაპურმა და ფინეთმაც. 2018 წლიდან ამ მიმართულებით პრაქტიკულად ბუმი დაიწყო. ამავე წელს მსგავსი შინაარსის სტრატეგიები მიიღო ამერიკის შეერთებულმა შტატებმა, ტაივანმა, იტალიამ, დიდმა ბრიტანეთმა, შვედეთმა, მექსიკამ, დანიამ, საფრანგეთმა, ავსტრალიამ, სამხრეთ კორეამ, გერმანიამ და ინდოეთმა.[25] 2018 წელს ხელოვნური ინტელექტის განვითარების სტრატეგია დაამტკიცა ევროკავშირმაც.

2024 წლის 13 მარტს ევროპარლამენტმა პლენარულ სესიაზე მხარი დაუჭირა ევროკომისიის წინადადებას ხელოვნური ინტელექტის შესახებ ჰარმონიზებული წესების (“AI Act”) განმსაზღვრელი რეგულაციის მიღების თაობაზე (523 -მხარდამჭერი; 46 - მოწინააღმდეგე; 49- მ შეიკავა).[26]„ხელოვნური ინტელექტის აქტი" (“AI Act”) ევროკავშირის წევრი სახელმწიფოებისთვის სავალდებულო ძალის მქონე დოკუმენტია, რომლის მიზანია, სამართლებრივი მოწესრიგების ფარგლებში მოაქციოს ხელოვნური ინტელექტის სისტემების შექმნის, განვითარებისა და გამოყენების პროცესი. აქტის მოქმედება ვრცელდება წევრ ქვეყნებზე ევროკავშირის მასშტაბით და მოიცავს როგორც

[24] ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2.

[25] *Dutton T.,* An Overview of National AI Strategies, Politics + AI 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> [10.03.2024].

[26] OneTrust DataGuidence, <https://www.dataguidance.com/news/eueuropean-parliament-adopts-ai-act> [12.03.2024].

საჯარო, ისე კერძო სექტორს. თუმცა არსებობს გამონაკლისებიც, კერძოდ, ხელოვნური ინტელექტის აქტი არ ვრცელდება სამხედრო, თავდაცვითი, ეროვნული უსაფრთხოების, კვლევისა და განვითარებისთვის შექმნილ ხელოვნური ინტელექტის სისტემებზე.[27] აქტით განსაზღვრულია სხვადასხვა ვალდებულება ხელოვნური ინტელექტის სისტემების პოტენციური რისკებისა და ზემოქმედების დონის მიხედვით. მასში კლასიფიცირებულია "AI" სისტემების სამი ძირითადი ჯგუფი, რომელთა მიმართაც განსხვავებული მოთხოვნები და ვალდებულებებია დადგენილი ("unacceptable-risk, high-risk, limited risk").

ევროპის საბჭოს ჩარჩო კონვენცია ხელოვნურ ინტელექტზე ადამიანის უფლებების, დემოკრატიისა და სამართლის უზენაესობის დაცვის მიზნით წარმოადგენს ერთ-ერთ პირველ საერთაშორისო იურიდიულ დოკუმენტს, რომელიც მიზნად ისახავს ხელოვნური ინტელექტის განვითარებისა და გამოყენების სტანდარტების დადგენას, რომლებიც სრულად პასუხობს ადამიანის ღირსების, პირადი თავისუფლებებისა და თანასწორობის პრინციპებს. კონვენცია ხაზს უსვამს იმას, რომ ტექნოლოგიური პროგრესი არ უნდა იყოს ხელის შეშლა ადამიანის უფლებების დაცვისა და დემოკრატიული ღირებულებების განმტკიცებისათვის. ის ყურადღებას ამახვილებს გამჭვირვალობაზე, ანგარიშვალდებულებასა და უსაფრთხოებაზე, რაც აუცილებელია ისეთი სისტემების შესაქმნელად, რომლებიც პატივს სცემენ პიროვნების ავტონომიას და უზრუნველყოფენ მონაცემთა დაცვას. სახელმწიფომ და კერძო სექტორმა უნდა მიიღონ შესაბამისი ზომები ზიანის თავიდან ასაცილებლად და უნდა უზრუნველყონ ადამიანის უფლებების რეალური დაცვა, მათ შორის რისკების შეფასება, ზედამხედველობა და კომპენსაციის მექანიზმები. ამ კონვენციით გათვალისწინებული მიდგომა ეწინააღმდეგება დისკრიმინაციას და ხელს უწყობს სამართლიან და პასუხისმგებელ გამოყენებას, რაც უზრუნველყოფს არა მხოლოდ ტექნოლოგიის განვითარებას, არამედ საზოგადოების ნდობას და დემოკრატიული სამართლის საფუძვლების შენარჩუნებას.

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ ("OECD") რეკომენდაცია ხელოვნურ ინტელექტთან დაკავშირებით პირველად 2019 წელს შეიმუშავა. რეკომენდაცია მიზნად ისახავდა ინოვაციებისა და ნდობის ამაღლების ხელშეწყობას ხელოვნური ინტელექტის სისტემების მიმართ, რა თქმა უნდა, ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის უზრუნველყოფით. 2023 წელს განახლდა არსებული რეკომენდაციები, უფრო მკაფიოდ განისაზღვრა ხელოვნური ინტელექტის სისტემის დეფინიცია, რაც გამოწვეული იყო ხელოვნური ინტელექტის სწრაფი ტექნოლოგიური განვითარებით. საერთო ჯამში, "OECD" რეკომენდაცია შეიცავს ხუთ მაღალი დონის ღირებულებებზე დაფუძნებულ პრინციპს და ხუთ რეკომენდაციას ეროვნული პოლიტიკისა და საერთაშორისო

[27]ევროკავშირის „ხელოვნური ინტელექტის შესახებ" აქტი, პრეამბულა, პუნქტი 24.

თანამშრომლობის მიმართულებით. სამწუხაროდ, "OECD" რეკომენდაციები მხოლოდ რეკომენდაცია არის და არ აქვს შემზღუდველი ეფექტი.[28]

ამერიკის შეერთებულ შტატებში 2022 წლის 4 ოქტომბერს თეთრი სახლის მეცნიერებისა და ტექნოლოგიების პოლიტიკის ოფისმა გამოაქვეყნა ავტომატური სისტემების განვითარებისა და გამოყენების გეგმა, რომელიც არ არის სავალდებულო და შეიცავს მხოლოდ ხუთ პრინციპს, რომლებიც მიზნად ისახავს ხელოვნური ინტელექტის სისტემის გამოყენების შედეგად მიყენებული ზიანის მინიმუმამდე დაყვანას. 2022 წლის 18 აგვისტოს სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა ("NIST") გამოაქვეყნა AI რისკის მართვის ჩარჩოს მეორე პროექტი. ხელოვნური ინტელექტის რისკების მართვის ჩარჩო მიზნად ისახავს დაეხმაროს კომპანიებს, რომლებიც შეიმუშავებენ ან განათავსებენ AI სისტემებს, შეაფასონ და მართონ ამ ტექნოლოგიებთან დაკავშირებული რისკები. იგი შედგება ნებაყოფლობითი გაიდლაინებისა და რეკომენდაციებისგან, ამიტომ ის ასევე არასავალდებულოა და აშკარად არ უნდა იქნას გაგებული, როგორც რეგულაცია.[29]

2017 წელს ჩინეთის[30] სახელმწიფო საბჭომ პირველად დაადგინა „მომავალი თაობის ხელოვნური ინტელექტის განვითარების გეგმა". 2021 წელს გამოქვეყნდა ხელოვნური ინტელექტის მართვის ეთიკური სახელმძღვანელო პრინციპები. შემდეგ, 2022 წლის იანვარში, ჩინეთმა გამოაქვეყნა ორი კანონი, რომლებიც ეხება კონკრეტულ AI აპლიკაციებს. მიუხედავად იმისა, რომ დებულებები ინტერნეტ-საინფორმაციო სერვისების ალგორითმული რეკომენდაციების მართვის შესახებ ("Algorithm Provisions") ძალაშია 2023 წლის მარტიდან, დებულებები ინტერნეტ საინფორმაციო სერვისების ღრმა სინთეზის მართვის შესახებ ("Draft Deep Synthesis Provisions") ჯერ კიდევ პროექტის ეტაპზეა.

იაპონიას[31] აქვს მეორე უდიდესი IT სექტორი "OECD"-ის ქვეყნებში და აქვს დიდი ინვესტიციები კვლევასა და განვითარებაში. ამასთან, ის იყო რიგით მეორე ქვეყანა, რომელმაც ხელოვნური ინტელექტის სტრატეგია შეიმუშავა. „ხელოვნური ინტელექტის ტექნოლოგიის სტრატეგია" გამოქვეყნდა 2017 წლის მარტში. სტრატეგიაში აღსანიშნავია ინდუსტრიალიზაციის საგზაო რუკა, რომელიც ითვალისწინებს ხელოვნური ინტელექტის სერვისების განვითარებას და ორგანიზებას უწევს ხელოვნური ინტელექტის განვითარების

[28] OECD Recommendation of the Council on Artificial Intelligence, 2024

[29] *Kohn B., Pieper F.U.,* AI Regulation Around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[30] *Klimentov M.,* From China to Brazil, here's how AI regulated around the world, September 2023, <https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/?trk=article-ssr-frontendpulse_little-text-block> [25.03.202].

[31] *Habuka Hiroki*, Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency, Report 2023, <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7 presidency#:~:text=As%20mentioned%20above%2C%20there%20are,occurs%20due%20to%20AI%20systems?trk=article-ssr-frontend-pulse_little-text-block> [30.03.2024].

სამ ფაზას: 1. ხელოვნური ინტელექტისთვის საჭირო მონაცემების დამუშავება, 2. ხელოვნური ინტელექტის საჯარო გამოყენება, და 3. ხელოვნური ინტელექტის ეკოსისტემების შექმნა.

ხელოვნური ინტელექტის მომწესრიგებელი სტრატეგიები და რეგულაციები მჭიდროდ უკავშირდება მთავარ პროექტს „საზოგადოება 5.0“. „ადამიანზე ორიენტირებული ხელოვნური ინტელექტის შესახებ სოციალური პრინციპები“, რომლებიც შემუშავებულია ინტეგრირებული ინოვაციების სტრატეგიის ხელშეწყობის საბჭოს მიერ, იაპონიის მთავრობამ 2019 წლის მარტში გამოაქვეყნა. აღნიშნული დოკუმენტი ასახავს იმ ძირეულ პრინციპებს, რომლებიც უნდა წარმართავდეს ხელოვნური ინტელექტის უნარიანი საზოგადოების ჩამოყალიბებასა და განვითარებას. პირველი ნაწილი შეიცავს შვიდ სოციალურ პრინციპს, რომლებსაც საზოგადოებამ და სახელმწიფომ უნდა სცეს პატივი ხელოვნურ ინტელექტუალურ კავშირთან ურთიერთობისას: (1) ადამიანზე ორიენტაცია, (2) განათლების უზრუნველყოფა და წიგნიერება, (3) მონაცემთა დაცვა, (4) უსაფრთხოების უზრუნველყოფა, (5) სამართლიანი კონკურენცია, (6) სამართლიანობა, ანგარიშვალდებულება და გამჭვირვალობა და (7) ინოვაცია. არც ერთი აღნიშნული მარეგულირებელი ღონისძიება არ არის იურიდიულად სავალდებულო.

ბრაზილია[32] მუშაობს კანონზე, რომელიც არეგულირებს ხელოვნურ ინტელექტს. 2022 წლის 1 დეკემბერს ბრაზილიის სენატის არამუდმივმა იურისპრუდენციის კომისიამ წარმოადგინა მოხსენება AI-ის რეგულირების შესახებ, რომელიც, მათ შორის, AI-ს რეგულირების პროექტს წარმოადგენდა. კომიტეტის მომხსენებლის თქმით, ხელოვნური ინტელექტის რეგულირება დაფუძნებულია სამ ცენტრალურ საყრდენზე: AI სისტემით დაზარალებული ადამიანების უფლებების უზრუნველყოფა, რისკის დონის კლასიფიკაცია და მართვის ღონისძიებების პროგნოზირება კომპანიებისთვის, რომლებიც უზრუნველყოფენ ან ამუშავებენ AI სისტემას.

პროექტი მონაცემთა სუბიექტს ანიჭებს უფლებას ხელოვნური ინტელექტის სისტემის პროვაიდერებისგან მოითხოვონ და მიიღონ ინფორმაცია, რა მოცულობით და რა მიზნით ხორციელდება მათი პერსონალური მონაცემების დამუშავება.

კანადა[33] იყო ერთ-ერთი პირველი ქვეყანა მსოფლიოში, რომელმაც მიიღო ხელოვნური ინტელექტის სტრატეგია. 2017 წელს კანადამ მიიღო ხუთწლიანი „პან-კანადური ხელოვნური ინტელექტის სტრატეგია“, რომელიც ორიენტირებული იყო ხელოვნური ინტელექტის კვლევებსა და ახალი ტალანტების აღმოჩენაზე. კანადის სტრატეგია განსხვავდება სხვა ქვეყნების სტრატეგიისგან იმით, რომ ის ძირითადად კონცენტრირებულია კვლევებისა

[32] *Kohn B., Pieper F.U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[33] *გაბისონია ზ.,* ინტერნეტ სამართალი და ხელოვნური ინტელექტი, „იურისტების სამყარო“, თბილისი 2022, 526.

და ახალი ტალანტების აღმოჩენაზე და ორიენტირებულია ამ სფეროს ცოდნის მაქსიმალურ დაგროვებაზე.

2022 წლის 16 ივნისს კანადის ფედერალურმა მთავრობამ წარადგინა კანონის პროექტი C-27, რომელიც ასევე ცნობილია, როგორც ციფრული ქარტიის განხორციელების აქტი. ხელოვნური ინტელექტისა და მონაცემთა აქტი ("AIDA") არეგულირებს საერთაშორისო და პროვინციულ ვაჭრობას ხელოვნური ინტელექტის სისტემებში. აქტის მიზანია, შეამცირონ ის შესაძლო რისკები და მიკერძოებული შედეგები, რომლებიც დაკავშირებულია მაღალი ხარისხის ხელოვნური ინტელექტის სისტემებთან. ამასთან, კანონი საშუალებას აძლევს სახელმწიფოს, შეზღუდოს ხელოვნური ინტელექტის სისტემის გამოყენება, თუ ეს უკანასკნელი მნიშვნელოვან ზიანს აყენებს ინდივიდების კანონიერ უფლებებსა და ინტერესებს.[34]

ევროკავშირისგან განსხვავებით, შვეიცარიაში ხელოვნური ინტელექტის რეგულირებისთვის ცალკე კანონის მიღების აუცილებლობას ვერ ხედავენ. შვეიცარიის მთავრობა ფიქრობს,[35] რომ ახალი კანონის შემუშავება არ არის საჭირო, რადგან შესაძლებელია არსებული საკანონმდებლო რეგულაციები შესაბამისობაში მოვიდეს და ადაპტირდეს ხელოვნურ ინტელექტთან. მაგალითად, მონაცემთა დაცვის კანონით გათვალისწინებულ იქნა დებულება ხელოვნური ინტელექტის გამჭვირვალობის შესახებ, მათ შორის, კონკურენციის კანონს, პროდუქტის პასუხისმგებლობის შესახებ კანონსა და სამოქალაქო კოდექსს დაემატა შესაბამისი რეგულაციები ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებით.

გაერთიანებული სამეფოს[36] მთავრობამ ჯერ კიდევ 2018 წელს დაიწყო ხელოვნური ინტელექტის სექტორული ანგარიშის გამოქვეყნება, რაც სახელმწიფოს დიდი ინდუსტრიული სტრატეგიის ნაწილი იყო. მოგვიანებით, 2023 წლის 29 მარტს, მთავრობამ გამოაქვეყნა AI „თეთრი წიგნი", რომელშიც მოცემულია წინადადებები გაერთიანებულ სამეფოში ხელოვნური ინტელექტის (AI) გამოყენების რეგულირებისთვის. „თეთრი წიგნი" არის ხელოვნური ინტელექტის რეგულირების პოლიტიკის დოკუმენტის გაგრძელება, რომელმაც წარმოადგინა გაერთიანებული სამეფოს მთავრობის ხედვა მომავალი „ინოვაციის მომხრე" და „კონტექსტური სპეციფიკური" ხელოვნური ინტელექტის მარეგულირებელი რეჟიმის შესახებ გაერთიანებულ სამეფოში.

[34] Government of Canada, The Artificial Intelligence and Data Act (AIDA)- Companion document, <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document?trk=article-ssr-frontend-pulse_little-text-block> [01.04.2024].

[35] *Kohn B., Pieper F.U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[36] *Prinsley M.A., Yaros O., Randall R., Hajda O., Hepworth E.,* UK's Approach to Regulating the Use of Artificial Intelligence, <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence> [10.04.2024].

„თეთრი წიგნი“ გვთავაზობს განსხვავებულ მიდგომას ხელოვნური ინტელექტის რეგულირების მიმართ ევროკავშირის AI აქტთან შედარებით. გაერთიანებულ სამეფოში ხელოვნური ინტელექტის რეგულირებისთვის, ახალი ფართომასშტაბიანი კანონმდებლობის დანერგვის ნაცვლად, გაერთიანებული სამეფოს მთავრობა ორიენტირებულია ხელოვნური ინტელექტის განვითარებისა და გამოყენების მოლოდინების ჩამოყალიბებაზე. ასევე მთავრობა ფოკუსირებულია არსებული მარეგულირებლების გაძლიერებაზე, როგორებიცაა ინფორმაციის კომისრის ოფისი (“ICO”), ფინანსური ქცევის ორგანო (“FCA”) და კონკურენციისა და ბაზრის ორგანო (“CMA”), რათა გასცენ სახელმძღვანელო მითითებები და დაარეგულირონ ხელოვნური ინტელექტის გამოყენება მათი უფლებამოსილების ფარგლებში.

დანიის[37] სტრატეგია - „დანიის ციფრული ზრდისთვის“ 2018 წელს გამოქვეყნდა და მიზნად ისახავს გახდეს ციფრული ინდუსტრიის რევოლუციის ლიდერი ქვეყანა და ამ მხრივ შეუწყოს ხელი დანიელ ხალხს სიმდიდრის ზრდასა და განვითარებაში.

გერმანიის[38] მთავრობამ 2018 წელს გამოაქვეყნა ხელოვნური ინტელექტის სტრატეგია. სტრატეგია ერთობლივად შემუშავდა ეკონომიკის სამინისტროს, კვლევის სამინისტროსა და შრომის სამინისტროს მიერ. ფედერალური მთავრობის მიზანია დაიცვას გერმანიის გამორჩეული პოზიცია, როგორც კვლევითი ცენტრი, გააძლიეროს გერმანული ინდუსტრიის კონკურენტუნარიანობა და ხელი შეუწყოს AI-ს გამოყენების მრავალ გზას საზოგადოების ყველა ნაწილში ხელოვნური ინტელექტის შესახებ. თავისი ამბიციური მიზნების მისაღწევად ფედერალურმა მთავრობამ გადაწყვიტა, დამატებით ნახევარი მილიარდი ევროს ინვესტიცია განახორციელოს 2019 წელს ხელოვნური ინტელექტის ხელშეწყობის პოლიტიკაში.

ინდოეთმა[39] 2018 წელს გამოაქვეყნა ხელოვნური ინტელექტის სტრატეგია, რომელიც მიზნად ისახავს, თუ როგორ შეუძლია ინდოეთს გამოიყენოს ხელოვნური ინტელექტი არა მხოლოდ ეკონომიკური ზრდისთვის, არამედ სოციალური ჩართულობისთვისაც. ინდოეთს, როგორც ერთ-ერთ ყველაზე სწრაფად მზარდი ეკონომიკის მქონე ქვეყანას, მნიშვნელოვანი წილი აქვს ხელოვნური ინტელექტის რევოლუციაში, რომელმაც მსოფლიო ქარიშხალი შექმნა. აღნიშნული სტრატეგიული დოკუმენტი გვიჩვენებს, რომ ინდოეთს აქვს ძალა და მახასიათებლები იმისთვის, რომ ადგილი დაიკავოს ლიდერებს შორის გლობალური AI რუკაზე. იგი ასევე ყურადღებას ამახვილებს იმაზე, თუ როგორ შეუძლია ინდოეთს გამოიყენოს ტრანსფორმაციული

[37] Agency for Digital Government, The Danish National Strategy for Artificial Intelligence, <https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/> [10.04.2024].

[38] German Federal Government’s AI Strategy, <https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html> [12.04.2024].

[39] India’s National Strategy for Artificial Intelligence, 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> [17.04.2024].

ტექნოლოგიები, რათა უზრუნველყოს სოციალური და ინკლუზიური ზრდა მთავრობის განვითარების ფილოსოფიის შესაბამისად.

იტალიამ[40] 2018 წელს გამოაქვეყნა ე. წ. „თეთრი ფურცელი“ ხელოვნური ინტელექტის შესახებ. სხვა სტრატეგიებისგან განსხვავებით, რომლებიც ფოკუსირებულია კვლევასა და განვითარებაზე ან კერძო სექტორის ათვისებაზე, „თეთრი ფურცელი“ ყურადღებას ამახვილებს იმაზე, თუ როგორ შეუძლია მთავრობას ხელი შეუწყოს საჯარო ადმინისტრაციებში ხელოვნური ინტელექტის ტექნოლოგიების დანერგვას.

მალაიზიამ[41] 2021 წელს მიიღო ხელოვნური ინტელექტის სტრატეგია 2021-2025. ეროვნული ხელოვნური ინტელექტის „საგზაო რუკა“ (შემდგომში AI-Rmap) აღწერს, თუ როგორ იქნება მალაიზიის AI შესაძლებლობების გამოყენება მომდევნო 5 წლის განმავლობაში, 2021 წლიდან 2025 წლამდე. COVID-19 პანდემიამ შექმნა კრიზისი ქვეყნებისთვის მთელს მსოფლიოში, მათ შორის, იგი იყო კატალიზატორი მალაიზიაში ციფრული ტრანსფორმაციისა და ტექნოლოგიების დანერგვის დაჩქარებისთვის. “AI-Rmap”-ს აქვს სამი განმასხვავებელი მახასიათებელი მის განვითარებაში: (1) სტრატეგიული თანხვედრა გლობალურ და ეროვნულ სტრატეგიულ დოკუმენტებთან, რომლებიც ეხება მეცნიერებას, ტექნოლოგიასა და ინოვაციას, (2) სტრატეგიული თანამშრომლობა მთავრობას, აკადემიას, ინდუსტრიასა და საზოგადოებას შორის (“GAIS”, ან “Quadruple Helix”) და (3) სრულად 100% ვირტუალური და ონლაინ შეხვედრები და პრეზენტაციები, პროექტის დაწყებიდან პროექტის დასრულებამდე. “AI-Rmap”-ის მთავარი მიზანია შექმნას აყვავებული და მდგრადი AI ინოვაციური ეკოსისტემა, რომელიც მალაიზიას აქცევს მაღალტექნოლოგიურ და მაღალშემოსავლიან ერად ხელოვნური ინტელექტის გამოყენებით.

პოლონეთის[42] მთავრობამ 2018 წლის მაისში გამართა პირველი მრგვალი მაგიდა პოლონეთის ხელოვნური ინტელექტის სტრატეგიის შემუშავების შესახებ. 2020 წლის დეკემბერში მინისტრთა საბჭომ მიიღო პოლონეთის ეროვნული ხელოვნური ინტელექტის სტრატეგია.

სტრატეგია ორიენტირებულია საზოგადოებაზე, განათლებაზე, მეცნიერებაზე, ბიზნესზე, საზოგადოებრივ საქმეებსა და საერთაშორისო ურთიერთობებზე, ადამიანის უფლებებისა და ღირსების დაცვაზე, სამართლიანი კონკურენციის პირობების ხელშეწყობაზე და ა. შ. პოლონეთი ახორციელებს სანდო ხელოვნური ინტელექტის ეთიკურ ჩარჩოს და ამოქმედებს ხელოვნური ინტელექტის პოლონური ეკოსისტემის აყვავების

[40] European Commission, National strategies on Artificial Intelligence A European perspective in 2019, Country report – Italy, <https://knowledge4policy.ec.europa.eu/sites/default/files/italy-ai-strategy-report.pdf> [17.04.2024].

[41] Navigating the Future Malaysia’s Ethical AI Vision, <https://thesun.my/business/navigating-the-future-malaysia-s-ethical-ai-vision-IP12485793> [29.05.2024].

[42] Poland AI Strategy Report, <https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en> [18.04.2024].

მექანიზმს ეთიკურ, იურიდიულ, ტექნიკურ-ოპერაციულ და საერთაშორისო განზომილებაში.

სინგაპურმა[43] 2017 წელს აამოქმედა ხუთწლიანი, 150 მილიონი აშშ დოლარის ღირებულების ეროვნული პროგრამა ხელოვნური ინტელექტის სფეროში სინგაპურის შესაძლებლობების გასაუმჯობესებლად. 2019 წელს სინგაპურმა გამოაქვეყნა პირველი ეროვნული AI სტრატეგია, რომელშიც ასახულია გეგმები ხელოვნური ინტელექტის გამოყენების გაღრმავებისთვის ეკონომიკის გარდასაქმნელად.

ხელოვნური ინტელექტის ამ ახალ ეპოქაში სინგაპურის მთავრობის განახლებული "NAIS 2.0" ასახავს ამბიციას და ვალდებულებას, აშენდეს სანდო და პასუხისმგებელი ხელოვნური ინტელექტის ეკოსისტემა, ხელი შეეწყოს ინოვაციებსა და გაიზარდოს ხალხის ჩართულობა ბიზნესის კეთებაში. AI წარმოადგენს შესაძლებლობებს და რისკებს სინგაპურისთვის, სადაც ხალხი ყოველდღიურად ურთიერთობს ციფრულ ტექნოლოგიებთან. ხელოვნური ინტელექტის დაუფლება საშუალებას მისცემს ბიზნესს და მოქალაქეებს, გამოიყენონ ახალი სამუშაო შესაძლებლობები და შექმნან ახალი ღირებულებები, რაც განბლოკავს მომავალ საზღვრებს ეკონომიკური ზრდისთვის. თუმცა ხელოვნური ინტელექტი უნდა იმართებოდეს პასუხისმგებლობით და მდგრადობით, რათა თავიდან იქნას აცილებული პოტენციური მავნე ეფექტები.

კორეის[44] მთავრობამ 2019 წლის 17 დეკემბერს დაადგინა ხელოვნური ინტელექტის ეროვნული სტრატეგია. სტრატეგიით, „AI მსოფლიო ლიდერისკენ IT მიღმა", კორეა მიზნად ისახავს მიაღწიოს ციფრულ კონკურენტუნარიანობას, შექმნას ხელოვნური ინტელექტის უზარმაზარი ეკონომიკური ეფექტი და გააუმჯობესოს ადამიანების ცხოვრების ხარისხი 2030 წლისთვის.

2018 წლის მაისში შვედეთის[45] მთავრობამ გამოაქვეყნა თავისი ეროვნული AI სტრატეგია – ხელოვნური ინტელექტის ეროვნული მიდგომა. ეს სტრატეგია მიუთითებს ხელოვნური ინტელექტის ზოგად მიმართულებაზე შვედეთში, რათა შეიქმნას საფუძველი მომავალი პოლიტიკის ქმედებებისა და პრიორიტეტებისთვის. ამ თვალსაზრისით, ეს სტრატეგია ემსახურება მომავალი პოლიტიკის ინიციატივების გამოკვეთას, რათა გააძლიეროს შვედეთის კეთილდღეობა და კონკურენტუნარიანობა ხელოვნური ინტელექტის საშუალებით. ამ მიზნით შვედეთის სტრატეგია ფოკუსირებულია

[43] National Artificial Intelligence Strategy 2.0 to Uplift Singapore's Social and Economic Potential, 2023, <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> [15.04.2024].

[44] National Strategy for Artificial Intelligence of Korea, <https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9> [15.04.2024].

[45] European Commission, National Strategies on Artificial Intelligence A European perspective in 2019, Country report Sweden, <https://knowledge4policy.ec.europa.eu/sites/default/files/sweden-ai-strategy-report.pdf> [15.04.2024].

შემდეგ პრიორიტეტულ სფეროებზე: განათლება, კვლევა, ინოვაცია და ინფრასტრუქტურა.

არაბეთის გაერთიანებული საემიროების[46] მთავრობამ 2017 წლიდან დაიწყო ხელოვნური ინტელექტის სტრატეგიის შემუშავება და ახლო აღმოსავლეთში ამ მიმართულებით ლიდერი ქვეყანა გახდა[47]. უფრო მეტიც, ის არის მსოფლიოში პირველი ქვეყანა, რომელმაც შექმნა ხელოვნური ინტელექტის სამინისტრო.[48] სტრატეგიის მთავარი მიზანია ხელოვნური ინტელექტის გამოყენება მთავრობის მუშაობის ეფექტიანობის გასაზრდელად.

არაბეთის გაერთიანებული საემიროები აყალიბებს მკაფიო ხედვას, თავისი ხელოვნური ინტელექტის სტრატეგიით 2031 წლისთვის გახდეს მსოფლიო ლიდერი ხელოვნური ინტელექტის სფეროში.

2018 წლის მაისში[49] დანიის, ესტონეთის, ფინეთის, ფარერის კუნძულების, ისლანდიის, ლატვიის, ლიეტუვის, ნორვეგიის, შვედეთისა და ალანდის კუნძულების ციფრულ განვითარებაზე პასუხისმგებელმა სამინისტროებმა გამოაქვეყნეს დეკლარაცია ხელოვნური ინტელექტის შესახებ სკანდინავიურ/ბალტიის რეგიონებში. ქვეყნები შეთანხმდნენ თანამშრომლობაზე, რათა „განავითარონ და ხელი შეუწყონ ხელოვნური ინტელექტის გამოყენებას ადამიანებისთვის“. მათ აღნიშნეს, რომ ისინი ითანამშრომლებენ შემდეგი მიზნებისთვის: 1. უნარების განვითარების შესაძლებლობების გაუმჯობესებაზე, 2. მონაცემებზე წვდომის გაზრდაზე, 3. ეთიკური და გამჭვირვალე სახელმძღვანელოების, სტანდარტების, პრინციპებისა და ღირებულებების შემუშავებაზე, 4. სტანდარტების შემუშავებაზე აპარატურისა და პროგრამული უზრუნველყოფისთვის, რაც შესაძლებელს გახდის კონფიდენციალობას, უსაფრთხოებასა და ნდობას, 5. იმის უზრუნველყოფა, რომ ხელოვნური ინტელექტი მნიშვნელოვან როლს შეასრულებს ერთიანი ციფრული ბაზრის შესახებ ევროპულ დისკუსიებში, 6. თავიდან აიცილებს არასაჭირო რეგულაციებს და 7. გამოიყენებს სკანდინავიურ/ბალტიკური რეგიონის მინისტრთა საბჭოს სკანდინავიურ პოლიტიკას თანამშრომლობის გასაადვილებლად.

რაც შეეხება საქართველოს, აღსანიშნავია, რომ 2024 წლიდან საქართველოს ხელი მოწერილი აქვს ევროპის საბჭოს ჩარჩო კონვენციისთვის. როგორც პოსტსაბჭოთა სივრცის ქვეყანა, ის ჯერ კიდევ განვითარების პროცესშია მაღალტექნოლოგიური მიმართულებით, რის გამოც ხელოვნური

[46] UAE National Strategy for Artificial Intelligence 2031, <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> [15.04.2024].

[47] UAE Strategy for Artificial Intelligence, <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence> [15.04.2024].

[48] არაბეთის გაერთიანებული საემიროების ხელოვნური ინტელექტის სამინისტრო, <https://ai.gov.ae/> [15.04.2024].

[49] Nordic Co-operation, AI in the Nordic-Baltic region, <https://www.norden.org/en/declaration/ai-nordic-baltic-region> [17.04.2024].

ინტელექტის პროგრამების შექმნა და განვითარება გარკვეულ გამოწვევებთან არის დაკავშირებული. 2024 წელს საქართველოს იუსტიციის მინისტრის განცხადებით[50], ტექნოლოგიურმა პროგრესმა წარმოქმნა იმგვარი სამართლებრივი რეგულაციების შემოღების საჭიროება, რომლებიც, ერთი მხრივ, ხელს შეუწყობს ინოვაციების განვითარებას, მეორე მხრივ კი, დაიცავს ადამიანის უფლებებს. შესაბამისად, იუსტიციის სამინისტროში ჩამოყალიბდება უწყებათაშორისი სამუშაო ჯგუფი, რომელიც იმუშავებს ევროკავშირის სამართალთან თავსებად ხელოვნური ინტელექტის სამართლებრივ რეგულირებაზე.

ამჟამად საქართველოში არ არსებობს სპეციალური საკანონმდებლო აქტი, რომელიც პირდაპირ არეგულირებს ხელოვნური ინტელექტის სამართლებრივ სტატუსს, ზღვარს ან ეთიკურ სტანდარტებს. მიუხედავად იმისა, რომ ტექნოლოგიის გამოყენება რეგულირდება ზოგადი ნორმებით (მაგალითად, კონსტიტუციით გარანტირებული პირადი ცხოვრების ხელშეუხებლობა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი და სხვა დარგობრივი აქტები), არ არსებობს სპეციალური დებულებები, რომლებიც განსაზღვრავენ:

- ალგორითმული გამჭვირვალობის კრიტერიუმებს;
- გადაწყვეტილების ავტომატურობის ხარისხის სამართლებრივ შეფასებას;
- ხელოვნური ინტელექტის ეთიკურ ჩარჩოს საჯარო ან კერძო სექტორში.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი პირდაპირ ხელოვნური ინტელექტის მომწესრიგებელ დებულებას არ ითვალისწინებს, თუმცა გარკვეული ნორმები შეეხება ავტომატიზებული მონაცემთა დამუშავების საკითხებს, რაც შეიძლება AI-ს გამოყენებასაც მოიცავდეს. კანონით დაშვებულია ავტომატიზებული გადაწყვეტილებების მიღება მხოლოდ იმ შემთხვევაში, თუ უზრუნველყოფილია მონაცემთა სიზუსტე, ინფორმირებულობა, უსაფრთხოება და სუბიექტის უფლებები. მიუხედავად ამისა, კანონი არ ითვალისწინებს AI-ს სპეციფიკურ რისკებს და რეგულირების თანამედროვე მოთხოვნებს, ამიტომ საჭიროა დამატებითი საკანონმდებლო ჩარჩოს შემუშავება.

აღსანიშნავია, რომ 2025 წელს საქართველოს მთავრობამ დაამტკიცა „საქართველოს ციფრული მმართველობის 2025-2030 წლების სტრატეგია“, რომლითაც პრევენციულად შემუშავდა ხელოვნური ინტელექტის რეგულირების ეთიკური და სამართლებრივი ჩარჩო.[51]

ზემოთ აღნიშნული ქვეყნები არ ასახავს სრულ სურათს, რადგან არსებობენ სხვა ქვეყნები, რომლებიც ცდილობენ, მოაწესრიგონ ხელოვნურ

[50] განცხადება ხელმისაწვდომია https://justice.gov.ge/?m=articles&id=OrginiwJBU

[51] საქართველოს მთავრობის 2025 წლის 3 აპრილის N100 დადგენილება „საქართველოს ციფრული მმართველობის 2025 – 2030 წლების სტრატეგიისა“ და „საქართველოს ციფრული მმართველობის 2025 – 2030 წლების სტრატეგიის 2025-2026 წლების სამოქმედო გეგმის“ დამტკიცების შესახებ.

ინტელექტთან დაკავშირებული საკითხები. მაგალითად, პოლიტიკის დოკუმენტები აღნიშნულ თემაზე აქვთ შემდეგ ქვეყნებს: არგენტინა, ჩილე, კოლუმბია და ისრაელი. სამოქმედო გეგმის სახით მიღებული აქვთ შემდეგ ქვეყნებს: ავსტრალია, ბანგლადეში, ეგვიპტე, ინდონეზია, მავრიკი, პერუ და საუდის არაბეთი. რაც შეეხება ტაივანს, მთავრობა აქტიურად მუშაობს ხელოვნური ინტელექტის მარეგულირებელი საკანონმდებლო აქტის, კანონის მიღებაზე, შემუშავებული არის კანონის პროექტი, თუმცა ჯერ-ჯერობით დამტკიცების მოლოდინშია.

4. საკანონმდებლო დონეზე ხელოვნური ინტელექტისა და პერსონალური მონაცემების ურთიერთმიმართების საკითხი

ხელოვნური ინტელექტი უკვე დიდი ხანია, აღარ წარმოადგენს მომავლის ტექნოლოგიას. მრავალი მიმართულებით იგი უკვე აწმყოს პროდუქტია, რომელიც ცხოვრების გამარტივებასთან ერთად მრავალი გამოწვევის წინაშე აყენებს როგორც მწარმოებლებს, ისე მომხმარებლებს. ერთ-ერთი მნიშვნელოვანი გამოწვევა უკავშირდება ზღვარს, რომელიც ხელოვნური ინტელექტის სიკეთეებსა და პერსონალურ მონაცემებს შორის გადის. პირად მონაცემებთან დაკავშირებული გამოწვევა ხელოვნური ინტელექტის არეალის გაფართოებასთან ერთად იზრდება. ამის ყველაზე კარგი მაგალითი სოციალური ქსელებია, რომლებიც წლიდან წლამდე მდიდრდება ავტომატიზებული, ჭკვიანი ალგორითმებით. ჯამურად, ეს ყველაფერი ხელოვნურ ინტელექტზე დაფუძნებულ სისტემებს აძლევს შესაძლებლობას, რომ მოახდინოს ჩვენი ონლაინ აქტივობების კონტროლი, რაც პირდაპირი მნიშვნელობით არის ჩვენს პირად ცხოვრებაში ჩარევა.[52]

ხელოვნური ინტელექტის მიერ მონაცემთა დამუშავების პროცესში ხშირად ირღვევა მონაცემთა დაცვის ძირითადი რეგულაციის (“GDPR”) ძირითადი პრინციპები, როგორებიცაა: ანგარიშვალდებულება, გამჭვირვალობა, კანონიერების საფუძველი და მინიმიზაცია. AI სისტემები ხშირად აგროვებენ მონაცემებს იმგვარად, რომ არ არის მკაფიოდ განსაზღვრული, რა მიზნებისთვის მოხდება მათი გამოყენება, რაც ეწინააღმდეგება მიზანმიმართულობის პრინციპს. გარდა ამისა, მონაცემთა დამუშავება ხშირად ხდება სამართლებრივი საფუძვლის გარეშე, ინახება გაურკვეველი დროით და შესაძლოა გამოყენებულ იქნას წინასწარ შეუთანხმებელი მიზნებისთვის, რაც არღვევს მონაცემთა რაოდენობრივ შეზღუდვასთან დაკავშირებულ (მინიმიზაციის) მოთხოვნებს. ტექნოლოგიის სირთულისა და სწრაფი განვითარებიდან გამომდინარე, რთულია ეფექტიანი

[52] ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2.

კონტროლისა და აუდიტის უზრუნველყოფა, რაც დამატებით გამოწვევას წარმოადგენს მონაცემთა დაცვის თვალსაზრისით.[53]

ხელოვნური ინტელექტს აქვს უნარი, ამოიცნოს ადამიანის თვალისთვის უხილავი ნიმუშები, ისწავლოს და გააკეთოს პროგნოზები ინდივიდებისა და ჯგუფების შესახებ. ამ თვალსაზრისით, AI-ს შეუძლია შექმნას ინფორმაცია, რომელიც რთულია შესაგროვებლად ან უკვე აღარ არსებობს. ეს ნიშნავს, რომ შეგროვებული და გამოყენებული ინფორმაცია შეიძლება გამოიყენებოდეს იმაზე მეტ ხანსა და ფართო მიზნით, რაც თავდაპირველად შეგნებულად გამჟღავნდა. ხელოვნური ინტელექტის გაზრდილი შესაძლებლობები, სავარაუდოდ, შექმნის ისეთ გარემოს, რომელშიც ინდივიდის მიერ გენერირებული ან მასთან დაკავშირებული ინფორმაციით იქნება იდენტიფიცირებადი.[54]

ხელოვნური ინტელექტის მეშვეობით ყველა კატეგორიის პერსონალური მონაცემი შეიძლება გამოყენებულ იქნას ადამიანის ქცევის გასაანალიზებლად, პროგნოზირებისთვის და ზემოქმედებისთვის, ხელოვნურ ინტელექტს აქვს შესაძლებლობა, რომელიც ამ მონაცემებს და მათი დამუშავების შედეგებს ძვირფას პროდუქტად გარდაქმნის. კერძოდ, ხელოვნური ინტელექტი იძლევა გადაწყვეტილების ავტომატიზებული მიღების შესაძლებლობას იმ დომეინებშიც კი, რომლებიც საჭიროებენ კომპლექსურ არჩევანს, მრავალ ფაქტორზე და არაგანსაზღვრულ კრიტერიუმებზე დაყრდნობით. ხშირ შემთხვევაში ავტომატური პროგნოზები და გადაწყვეტილებები არა მხოლოდ უფრო ხელმისაწვდომია, არამედ უფრო ზუსტი და მიუკერძოებელი, ვიდრე ადამიანური, რადგან AI სისტემებს შეუძლიათ აირიდონ ადამიანის ფსიქოლოგიის ტიპიური შეცდომა და შეიძლება დაექვემდებაროს მკაცრ კონტროლს. თუმცა ალგორითმული გადაწყვეტილებები ასევე შეიძლება იყოს მცდარი ან დისკრიმინაციული.[55] აღსანიშნავია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომლის მიხედვითაც მონაცემთა სუბიექტს უფლება აქვს, არ დაექვემდებაროს მხოლოდ ავტომატიზებულად, მათ შორის პროფაილინგის საფუძველზე, მიღებულ გადაწყვეტილებას, რომელიც მისთვის წარმოშობს სამართლებრივ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს,[56] როგორც უკვე აღინიშნა, ავტომატიზებულ საშუალებებში შესაძლებელია ვიგულისხმოთ ხელოვნური ინტელექტიც.

გამომდინარე იქიდან, რომ ხელოვნური ინტელექტის მარეგულირებელი სპეციალური საკანონმდებლო აქტები ჯერჯერობით არ არსებობს, საკანონმდებლო დონეზე მკაფიოდ არ არის განსაზღვრული ხელოვნური

[53] *Chalubinska-Jentiewicz K., Nowikowska M.,* Artificial Intelligence v. Personal Data, Polish Political Science Yearbook, vol 5., Poland 2022, 188-189.

[54] OVIC, Artificial Intelligence and Privacy – Issues and Challenges, <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/> [05.05.2024].

[55] European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020,
<https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [05.05.2024].

[56] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ მუხლი 19.

ინტელექტისა და პერსონალური მონაცემების ურთიერთმიმართების საკითხი. თუმცა შესაძლებელია მიჩნეულ იქნას, რომ თითქმის ყველა ქვეყნის პერსონალურ მონაცემთა დაცვის მარეგულირებელი აქტები შეიცავს დებულებას, რომ მონაცემთა დამუშავება ხორციელდება როგორც ავტომატური, ისე არაავტომატური საშუალებით, რაშიც ფართო გაგებით შეგვიძლია ვიგულისმოთ ხელოვნური ინტელექტიც.

საერთაშორისო დონეზე ძირითადი მარეგულირებელი აქტი, რომელიც ადგენს ხელოვნური ინტელექტისა და პერსონალური მონაცემების დაცულობის ვალდებულებასა და სტანდარტს საკანონმდებლო დონეზე, არის ევროპარლამენტის მიერ ახლად მიღებული აქტი ხელოვნური ინტელექტის შესახებ. კერძოდ, აღნიშნული აქტის მე-7 და მე-8 მუხლები ეხება კონკრეტულად პერსონალური მონაცემებისა და პირადი ცხოვრების ხელშეუხებლობისა და პატივისცემის უფლებას.[57] გასათვალისწინებელია, რომ ევროპის საბჭოს მიერ მიღებული ჩარჩო კონვენცია სამართლებრივად სავალდებულო (“first-ever legally binding international treaty”) საერთაშორისო აქტია, რომელიც ამ სფეროს არეგულირებს და რელევანტურია საქართველოსთვისაც.

ხელოვნური აქტის 28-ე მუხლის თანახმად, რომ, ხელოვნური ინტელექტის მიერ ჯანდაცვის სფეროში საქმიანობის განხორციელების დროს, დაცული უნდა იყოს ფუნდამენტურ უფლებათა ქარტიით დაცული უფლებები, მათ შორის პირის პირადი და ოჯახური ცხოვრების პატივისცემისა და პერსონალური მონაცემების დაცვის უფლება. ხელოვნური ინტელექტის სისტემები, რომლებიც გამოიყენება მიგრაციაში, თავშესაფარსა და საზღვრის კონტროლის მენეჯმენტში, გავლენას ახდენს ადამიანებზე, რომლებიც ხშირად არიან განსაკუთრებით დაუცველ მდგომარეობაში და დამოკიდებულნი არიან კომპეტენტური სახელმწიფო ორგანოების ქმედებების შედეგზე. ამრიგად, ამ კონტექსტში გამოყენებული ხელოვნური ინტელექტის სისტემების სიზუსტე, არადისკრიმინაციული ბუნება და გამჭვირვალობა განსაკუთრებით მნიშვნელოვანია დაზარალებული პირების ფუნდამენტური უფლებების პატივისცემის უზრუნველსაყოფად.[58]

პერუს აღმასრულებელმა ხელისუფლებამ გამოაქვეყნა კანონი, რომელიც ხელს უწყობს ხელოვნური ინტელექტის (AI) გამოყენებას ქვეყნის ეკონომიკური და სოციალური განვითარებისთვის, რაც მას, კანონმდებლობის თვალსაზრისით, ერთ-ერთ წამყვან ქვეყნად აქცევს ლათინურ ამერიკაში ამ ტექნოლოგიის სასარგებლოდ. პერუს ხელოვნური ინტელექტის კანონპროექტი დეტალურად აღწერს რისკზე დაფუძნებულ მიდგომას ხელოვნური ინტელექტის რეგულირებისადმი, ევროკავშირის AI აქტის მსგავსი, პოტენციური რისკების იმავე კატეგორიზაციისა და AI სისტემების გადაფარვის

[57] ევროკავშირის ხელოვნური ინტელექტის აქტი (EU AI Act), პარაგრაფი 2.
[58] იქვე, პარაგრაფი 39.

აკრძალვების ჩათვლით.[59] პერუს კანონმდებლობაში პირდაპირ ვხვდებით ჩანაწერს მონაცემთა დაცვასა და კონფიდენციალობასთან დაკავშირებით, კერძოდ, კანონის ერთ-ერთი პრინციპი არის „ხელოვნური ინტელექტის კონფიდენციალობა“, რაც გულისხმობს შემდეგს, რომ ხელოვნური ინტელექტი არ უნდა არღვევდეს ადამიანების კონფიდენციალობას.[60] კონფიდენციალურობის უფლება უფრო ფართო ცნებაა და გულისხმობს პირის პირადი ცხოვრების, კომუნიკაციისა და სივრცის დაცვას გარე ჩარევისგან, პერსონალურ მონაცემთა დაცვის უფლება კი ამ უფლების ნაწილია და ფოკუსირებულია მხოლოდ იმაზე, რომ პირადი მონაცემები შეგროვდეს, დამუშავდეს და შენახულ იქნას კანონიერად, სამართლიანად და გამჭვირვალედ.

საინტერესო ჩანაწერი გვხვდება საუდის არაბეთის სტრატეგიაში, კერძოდ, ინაუგურაციის დღიდან საუდის არაბეთის მონაცემთა და ხელოვნური ინტელექტის ორგანომ (“SDAIA”) ეროვნული მონაცემები და ხელოვნური ინტელექტის დღის წესრიგი სამეფოს ხედვის 2030-ის მიზნების წინსვლის მიზნით წარმართა. სულ ახლახან “SDAIA”, ტელეკომუნიკაციებისა და საინფორმაციო ტექნოლოგიების სამინისტროსთან (“MCIT”) პარტნიორობით, ხელმძღვანელობდა “G20”-ის ციფრულ ეკონომიკას. სამუშაო ჯგუფი ხელმძღვანელობდა სამეფოს პასუხს Covid-19-ზე ისეთი აპლიკაციების გაშვებით, როგორიცაა “Tawaklna” და “Tabaud”. გარდა ამისა, ხელისუფლებამ გამოაქვეყნა პოლიტიკის ნაკრები. მათ შორისაა: სამეფოს მონაცემთა კლასიფიკაციის პოლიტიკა, პერსონალური მონაცემთა დაცვის პოლიტიკა, მონაცემთა გაზიარების პოლიტიკა, ინფორმაციის თავისუფლების პოლიტიკა და ღია მონაცემთა პოლიტიკა — გზა გაეხსნა ძლიერი, ბიზნესისთვის მეგობრული მარეგულირებელი გარემო.

ქვემოთ განხილულია რამდენიმე სასამართლო გადაწყვეტილება ხელოვნური ინტელექტისა და პერსონალური მონაცემების ურთიერთმიმართებასთან დაკავშირებით.

2023 წლის 28 ივნისს აშშ ფედერალურმა სასამართლომ განიხილა საქმე “P.M. v. OpenAI LP”, მოსარჩელეთა ანონიმურმა ჯგუფმა შეიტანა სარჩელი “OpenAI LP-ის (OpenAI)” და “Microsoft, Inc.”-ის (“Microsoft”) წინააღმდეგ, რომლის თანახმად, “OpenAI”-მ მიითვისა მილიონობით ადამიანის კუთვნილი პირადი და პერსონალური ინფორმაცია ინტერნეტიდან და სოციალური მედიის პლატფორმებიდან საჯაროდ ხელმისაწვდომი მონაცემების შეგროვებით, მომხმარებლებისგან მათი ინფორმირებულობის ან თანხმობის გარეშე. მოსარჩელეები ამტკიცებდნენ, რომ “OpenAI”-ის პრაქტიკა გამოიყენოს ინტერნეტიდან შეგროვებული ინფორმაციის მონაცემთა ნაკრები მისი გენერაციული AI ინსტრუმენტების მოსამზადებლად წარმოადგენს ქურდობას,

[59] Access Alert: Peru’s congress introduces bill to regulate AI, 2024, <https://accesspartnership.com/access-alert-perus-congress-introduces-bill-to-regulate-ai/> [05.05.2024].

[60] Peru Law - LAW THAT PROMOTES THE USE OF ARTIFICIAL INTELLIGENCE IN FAVOR OF THE ECONOMIC AND SOCIAL DEVELOPMENT OF THE COUNTRY, Unique item, f, <https://busquedas.elperuano.pe/dispositivo/NL/2192926-1> [05.05.2024].

მითვისებას და მათი კონფიდენციალობისა და საკუთრების უფლებების დარღვევას. ინფორმაცია მოიცავდა სახელებს, მისამართებს, ტელეფონის ნომრებს, ელექტრონული ფოსტის მისამართებს და ფინანსურ მონაცემებს. “OpenAI”-მ და “Microsoft”-მა გამოიყენეს აღნიშნული პერსონალური ინფორმაცია “ChatGPT”-ის განსავითარებლად, რაც არღვევდა აშშ-ის ელექტრონული კონფიდენციალობის კომუნიკაციების აქტს, რომელიც სასამართლოს წინასწარი თანხმობის გარეშე კრძალავს ელექტრონული კომუნიკაციების ჩარევას.

განხილული საქმე მეტად აქტუალურია, რადგან აუცილებელია, რომ ხელოვნური ინტელექტის კომპანიებმა გამჭვირვალედ იმოქმედონ მონაცემთა შეგროვების პროცესში და დაეყრდნონ შესაბამის სამართლებრივ საფუძველს, როგორიცაა თანხმობა პერსონალური მონაცემების შეგროვებამდე. ეს ასევე ერთგვარი შეხსენებაა, რომ მომხმარებლებმა უნდა იცოდნენ ხელოვნური ინტელექტის მქონე პროდუქტებისა და სერვისების გამოყენების კონფიდენციალობის შესახებ საავტორო უფლებების დარღვევის თაობაზე მათი პრეტენზიების მიმართ, ისევე, როგორც მის თეორიებთან დაკავშირებული ზიანის მიყენების სხვადასხვა ფორმა.[61]

2023 წლის 11 ივლისს საქმეში “J.L. v. Alphabet Inc.”, ამერიკის ფედერალურ სასამართლოში Google-ის წინააღმდეგ წარდგენილ იქნა ჯგუფური სარჩელი. მოსარჩელეები ამტკიცებდნენ, რომ კომპანიამ დაარღვია კონფიდენციალობისა და საავტორო უფლებების კანონები. ასევე ამტკიცებდნენ იმას, რომ Google-ის გენერაციული AI პროდუქტები, მათ შორის, “Bard” (ტექსტის გენერატორი), “Imagen” და “Gemini” (ტექსტი-სურათის დიფუზიის ორი მოდელი), “MusicLM” (ტექსტი-მუსიკის ხელსაწყო) და “Duet AI” (მონაცემთა ვიზუალიზაციის ხელსაწყო), ეყრდნობოდა მონაცემებს, რომლებიც “Google”-მა შეაგროვა ინტერნეტიდან.[62]

სარჩელში აღნიშნულია, რომ Google ონლაინ ტრენინგებისთვის იყენებდა ინფორმაციას, რომელიც ინტერნეტში იყო განთავსებული და აღნიშნულისთვის არ ითხოვდა თავად ინფორმაციის მესაკუთრის თანხმობას, კერძოდ, Google-ის ხელოვნური ინტელექტის პროდუქტებში, სავარაუდოდ, გამოიყენებოდა საავტორო უფლებებით დაცული ტექსტი, მუსიკა, სურათები და მონაცემები სასწავლო მიზნებისთვის.[63]

ინტერნეტში საჯაროდ განთავსებული ინფორმაციის ხელოვნური ინტელექტის მიერ გამოყენებას ეხება ამერიკის შეერთებული შტატების სასამართლო საქმე: “HiQ Labs, Inc. v. LinkedIn Corp.”, კერძოდ, მოცემულ საქმეში hiQ Labs, Inc.-მა, ინფორმაციამ „ამოიღო“ ინფორმაცია ბიზნეს-ქსელების

[61] Conexus law, OpenAI, and Microsoft sued in the US for §3 billion over alleged ChatGPT privacy violations, <https://www.conexuslaw.com/insight/openai-and-microsoft-sued-in-us-for-3-billion-over-alleged-chatgpt-privacy-violations/> [25.04.2024].

[62] J.L. et al. v. Alphabet Inc. et al. - 3:23-cv-03440

[63] *Christopher J. Valente, Stortz M.J., Wong A., Soskin P.E., Meredith M.W.,* US Litigation and Dispute Resolution Alert, 2023, <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> [25.04.2024].

საიტის LinkedIn-ის ონლაინ მომხმარებელთა საჯაროდ ხელმისაწვდომი პროფილებიდან, რათა დამსაქმებლებისთვის მიეწოდებინა მონაცემები და ანალიზი სამუშაოს მაძიებლებისა და ხშირად მოძებნადი სამუშაოს ტიპის შესახებ. სასამართლომ აღნიშნა, რომ საჯაროდ ხელმისაწვდომი მონაცემების გამოყენება არ გულისხმობს კონფიდენციალობის უფლების ხელყოფას. აღნიშნული უფლება დაირღვევა იმ შემთხვევაში, თუ ხელოვნური ინტელექტის სისტემა გამოიყენებს იმ მონაცემს, რომელიც არ არის საჯაროდ განთავსებული და მინიჭებული აქვს სტატუსი „პირადი“.[64]

იტალია პირველი დასავლური ქვეყანაა, რომელმაც ჩატბოტი “ChatGPT” დაბლოკა. იტალიის მონაცემთა დაცვის ორგანომ “Microsoft”-ის მიერ მხარდაჭერილი, ამერიკული “OpenAI”-ს მიერ შექმნილი ჩატბოტის დაბლოკვის და გამოძიების დაწყების გადაწყვეტილება კონფიდენციალობასთან დაკავშირებული პრობლემებიდან გამომდინარე მიიღო. იტალიაში “ChatGPT”-ს აეკრძალა ფუნქციონირება მას შემდეგ, რაც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განაცხადა, რომ არ არსებობს სამართლებრივი საფუძველი პერსონალური მონაცემების შეგროვებისა და „მასიური შენახვის“ გასამართლებლად “GPT AI”-ის მომზადების მიზნით.[65] პროგრამული უზრუნველყოფის აკრძალვის გადაწყვეტილება მას შემდეგ მიიღეს, რაც “Garante”-მ (იტალიის პერსონალურ მონაცემთა დაცვის ზედამხედველი), მონაცემთა დაცვის იტალიურმა ორგანიზაციამ, “OpenAI” დაადანაშაულა იტალიელ მონაცემთა სუბიექტების მონაცემების არასწორად შეგროვებასა და შენახვაში და შესაბამისად, “GDPR”-ის დარღვევაში. შეშფოთების მიზეზი ისიც ხდება, რომ პროგრამულ უზრუნველყოფას შეუძლია არასრულწლოვანთათვის საზიანო შინაარსის მასალის მიწოდება ასაკის გადამოწმების პროცედურის არარსებობის გამო. ამასთან, გამოძიების ეტაპზე დადგინდა, რომ ხელოვნური ინტელექტი ამუშავებდა პირების საუბარს, ელ. ფოსტის მისამართებს და, მათ შორის, საბანკო ბარათის ბოლო ოთხ ციფრს. “BBC”-ის ცნობით, იტალიის ხელისუფლებამ “OpenAI”-ს 20 დღე მისცა პრობლემების გადასაჭრელად, ვითარების გამოუსწორებლობის შემთხვევაში კი ის დაჯარიმდება წლიური შემოსავლის 4%-ამდე. OpenAI-მ ბრალდებები უარყო.[66] თუმცა, საბოლოოდ, “ChatGPT”-ის დროებითი დაბლოკვა იტალიაში მოხდა 2023 წლის 31 მარტს და დასრულდა 2023 წლის 28 აპრილს, ანუ დაბლოკვა დაახლოებით 4 კვირა, 28 დღე, გაგრძელდა.

“ChatGPT” იტალიის გარდა ჩინეთი ქვეყნის უმსხვილეს ტექნოლოგიურ კომპანიებს მომხმარებლებისთვის “ChatGPT”-ის სერვისის შეთავაზებას უკრძალავს. “Nikkei Asia”-ს თანახმად, სხვა შემთხვევაში პასუხებს, რომელთაც Microsoft-ის მხარდაჭერით “OpenAI”-ის მიერ შექმნილი ხელოვნური

[64] იქვე.

[65] Dan Milmo and agencies, Italy’s privacy watchdog bans ChatGPT over data breach concerns, <https://www.theguardian.com/technology/2023/mar/31/italy-privacy-watchdog-bans-chatgpt-over-data-breach-concerns> [30.04.2024].

[66] იტალიაში ChatGPT დაიბლოკა, ბიზნეს ფორმულა, <https://businessformula.ge/News/13437> [30.04.2024].

ინტელექტის ჩატბოტი იძლევა, ჩინეთის კომუნისტური პარტიის ("CCP") ცენზურა შეეხებოდა. "ChatGPT"-ის სერვისი ოფიციალურად ჩინეთში ხელმისაწვდომი არაა. თუმცა ინტერნეტში მომხმარებელთა ნაწილმა ვირტუალური კერძო ქსელის ("VPN") გამოყენებით "AI chatbot"-ზე წვდომის დამყარება მაინც მოახერხა.[67]

საბერძნეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("Hellenic DPA") დააკისრა ჯარიმა ოცი მილიონი ევროს ოდენობით "Clearview AI Inc"-ს კანონიერებისა და გამჭვირვალობის პრინციპების დარღვევისთვის. გარდა აღნიშნულისა, ხელისუფლებამ კომპანიას აუკრძალა საბერძნეთის ტერიტორიაზე პერსონალური მონაცემების შეგროვება და შენახვა შესაბამისი საფუძვლის არსებობის გარეშე. "Clearview AI Inc" ფლობს სახის ამომცნობ ბაზას, რომელშიც პერსონალური მონაცემები, ამ შემთხვევაში ფოტოები, მოპოვებულია მონაცემთა სუბიექტის თანხმობის გარეშე.[68]

საბერძნეთის შემდეგ ავსტრიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მიიღო გადაწყვეტილება სახის ამომცნობი კომპანიის "Clearview AI"-ის წინააღმდეგ. გავრცელებული ინფორმაციით, კომპანია ფლობს მონაცემთა ბაზას, რომელიც მოიცავს 30 მილიარდზე მეტ სახის სურათს მთელი მსოფლიოდან. ისინი ამოღებულია საჯარო წყაროებიდან (მედია საშუალებები, სოციალური მედია, ონლაინ ვიდეოები). მომხმარებელს შესთავაზა დახვეწილი საძიებო სერვისი, რომელიც საშუალებას აძლევს ხელოვნური ინტელექტის სისტემების მეშვეობით შექმნას პროფილები სურათებიდან ამოღებული ბიომეტრიული მონაცემების საფუძველზე. პროფილები შეიძლება გამდიდრდეს იმ სურათებთან დაკავშირებული ინფორმაციებით, როგორებიცაა გამოსახულების ტეგები და გეოლოკაცია ან წყაროს ვებ გვერდები.[69]

[67] *პაპალაშვილი ს.,* Nikkei Asia: ჩინეთი კომპანიებს ChatGPT-ის სერვისის გამოყენებას უკრძალავს, <https://forbes.ge/nikkei-asia-chinethi-kompaniebs-chatgpt-is-servisis-gamoqhenebas-ukrdzalavs/> [25.04.2024].

[68] Hellenic DPA fines Clearview AI 20 million euros, <https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en> [25.04.2024].

[69] Decision by the Austrian SA against Clearview AI Infringements of Article 5,6,9,27 GDPR, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en> [25.04.2024].

5. დასკვნა

მიუხედავად იმისა, რომ მსოფლიოსთვის ჯერ კიდევ ახალ რეალობას წარმოადგენს ხელოვნური ინტელექტი და მისი რეგულირება, რთულია რაიმე გადაწყვეტილების მიღება ისეთ სისტემის მიმართ, რომელიც ყოველდღიურად იცვლება და ვითარდება.

ხელოვნური ინტელექტის მიერ მონაცემების დამუშავების პროცესში შესაძლოა დაირღვეს მონაცემთა დაცვის ძირითადი რეგულაციის აუცილებელი მოთხოვნები, კერძოდ, ისინი, რომლებიც ეწინააღმდეგება ანგარიშვალდებულების, გამჭვირვალობის, მონაცემთა დამუშავების კანონიერი საფუძვლის არსებობისა და მინიმიზაციის პრინციპს. ბევრი AI აპლიკაცია ამუშავებს პერსონალურ მონაცემებს. ერთი მხრივ, პერსონალურმა მონაცემებმა შეიძლება ხელი შეუწყოს მონაცემთა ნაკრებებს, რომლებიც გამოიყენება მანქანური სწავლების სისტემების მოსამზადებლად, კერძოდ, მათი ალგორითმული მოდელების შესაქმნელად. მეორე მხრივ, ასეთი მოდელები შეიძლება გამოყენებულ იქნას პერსონალურ მონაცემებზე კონკრეტული პირების შესახებ დასკვნების გასაკეთებლად.

როგორც წინამდებარე ნაშრომში გამოჩნდა, პერსონალური მონაცემების დაცვის მარეგულირებელი აქტები გვხვდება როგორც საერთაშორისო, ისე ადგილობრივ დონეზე, თუმცა მონაცემთა დაცვისა და დამუშავების ძირითად სტანდარტებსა და პრინციპებს ადგენს ევროპის საბჭოს მიერ მიღებული მონაცემთა დაცვის ძირითადი რეგულაცია. რაც იმას ნიშნავს, რომ პერსონალურ მონაცემთა დაცვის საკმაოდ მაღალი სტანდარტი არის დადგენილი. რაც შეეხება ხელოვნური ინტელექტის მარეგულირებელ საერთაშორისო აქტს, ეს უკანასკნელი ჯერ კიდევ ახალი და პრაქტიკაში „გამოუცდელია“. მოძიებული და დამუშავებული მასალიდან გამოჩნდა, რომ სხვადასხვა ქვეყანას ეროვნულ დონეზე მიღებული აქვს ხელოვნურ ინტელექტთან დაკავშირებული რეკომენდაციები, სტრატეგიები, სამოქმედო გეგმები თუ პოლიტიკის დოკუმენტები. თუმცა აღსანიშნავია, რომ ისინი მხოლოდ სარეკომენდაციო ხასიათისაა და არ აქვთ მბოჭავი ეფექტი.

ბიბლიოგრაფია:

1. ადამიანის უფლებათა ევროპული კონვენცია, 1950, მუხლი 8, 12.
2. ევროკავშირის ხელოვნური ინტელექტის აქტი (EU AI Act), პარაგრაფი 2.
3. ევროკავშირის ხელოვნური ინტელექტის აქტი (EU AI Act), პარაგრაფი 2.
4. ევროპის საბჭო, კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ CETS No. 108, 1981.
5. ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 1995 L 281.
6. მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 4 (1);
7. მონაცემთა დაცვის ძირითადი რეგულაცია, პრეამბულა, პუნქტი 26.
8. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 14/06/2023
9. საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ (ICCPR) 1976, მუხლი 17.
10. ყველა მიგრანტი მუშაკისა და მათი ოჯახის წევრების დაცვის შესახებ კონვენცია, მუხლი 14.
11. შეზღუდული შესაძლებლობების მქონე პირთა უფლებების კონვენცია, მუხლი 22.
12. *გაბისონია ზ.,* ინტერნეტ სამართალი და ხელოვნური ინტელექტი, „იურისტების სამყარო“, თბილისი 2022, 513, 526.
13. ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2.
14. *პაპალაშვილი ს.*, Nikkei Asia: ჩინეთი კომპანიებს ChatGPT-ის სერვისის გამოყენებას უკრძალავს, <https://forbes.ge/nikkei-asia-chinethi-kompaniebs-chatgpt-is-servisis-gamoqhenebas-ukrdzalavs/> [25.04.2024].
15. სამეცნიერო ჟურნალი “ახალგაზრდა ადვოკატები“ N5, „ახალგაზრდა ადვოკატებისა“ და „ადვოკატთა საგანმანათლებლო ცენტრის“ ერთობლივი გამოცემა, თბილისი 2016, 34.
16. საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 მარტის N1/4/757 გადაწყვეტილება საქმეზე „საქართველოს მოქალაქე გიორგი კრავეიშვილი საქართველოს მთავრობის წინააღმდეგ“, II-4.
17. Access Alert: Peru’s congress introduces bill to regulate AI, 2024, <https://accesspartnership.com/access-alert-perus-congress-introduces-bill-to-regulate-ai/> [05.05.2024].
18. Agency for Digital Government, The Danish National Strategy for Artificial Intelligence, <https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/> [10.04.2024].

19. European Commission, National strategies on Artificial Intelligence A European perspective in 2019, Country report – Italy, <https://knowledge4policy.ec.europa.eu/sites/default/files/italy-ai-strategy-report.pdf> [17.04.2024].
20. European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020, <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [05.05.2024].
21. German Federal Government's AI Strategy, <https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html> [12.04.2024].
22. Government of Canada, The Artificial Intelligence and Data Act (AIDA)- Companion document, <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document?trk=article-ssr-frontend-pulse_little-text-block> [01.04.2024].
23. India's National Strategy for Artificial Intelligence, 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> [17.04.2024].
24. National Artificial Intelligence Strategy 2.0 to Uplift Singapore's Social and Economic Potential, 2023, <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> [15.04.2024].
25. National Strategy for Artificial Intelligence of Korea, https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9 [15.04.2024].
26. Navigating the Future Malaysia's Ethical AI Vision, <https://thesun.my/business/navigating-the-future-malaysia-s-ethical-ai-vision-IP12485793> [29.05.2024].
27. Poland AI Strategy Report, <https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en> [18.04.2024].
28. UAE National Strategy for Artificial Intelligence 2031, <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> [15.04.2024].
29. Alfredsson G., Eide Asbjorn, The Universal Declaration of Human Rights A Common Standard of Achievement, Hague, Kluwer Law International, 1999, 257-258.
30. Chalubinska-Jentiewicz K., Nowikowska M., Artificial Intelligence v. Personal Data, Polish Political Science Yearbook, vol 5., Poland 2022, 188-189.
31. Christopher J. Valente, Stortz M.J., Wong A., Soskin P.E., Meredith M.W., US Litigation and Dispute Resolution Alert, 2023, <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> [25.04.2024].

32. Decision by the Austrian SA against Clearview AI Infringements of Article 5,6,9,27 GDPR, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en> [25.04.2024].
33. Dutton T., An Overview of National AI Strategies, Politics + AI 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> [10.03.2024].
34. EDPS, The History of the General Data Protection Regulation, ხელმისაწვდომია: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [15.01.2024].
35. European Commission, What is personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> [17.01.2024].
36. *Habuka Hiroki*, Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency, Report 2023, <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7 presidency#:~:text=As%20mentioned%20above%2C%20there%20are,occurs%20due%20to%20AI%20systems?trk=article-ssr-frontend-pulse_little-text-block> [30.03.2024].
37. *Klimentov M.,* From China to Brazil, here's how AI regulated around the world, September 2023, <https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/?trk=article-ssr-frontendpulse_little-text-block> [25.03.2024].
38. *Kohn B.,* Pieper F.U., AI Regulation Around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].
39. OECD Recommendation of the Council on Artificial Intelligence, 2024.
40. OVIC, Artificial Intelligence and Privacy – Issues and Challenges, <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/> [05.05.2024].
41. *Prinsley M.A., Yaros O., Randall R., Hajda O., Hepworth E.,* UK's Approach to Regulating the Use of Artificial Intelligence, <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence> [10.04.2024].
42. *Russel S., Norvig P.*, Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003, 27, 32–58, 968–972.
43. Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2009, 2.

გიორგი ხორბალაძე*

ფიზიკური პირის მიერ მონაცემთა სუბიექტის პერსონალური მონაცემების გამჟღავნების გზით დამუშავება სოციალურ ქსელებში

ინფორმაციული ტექნოლოგიების განვითარებამ უამრავ შესაძლებლობასთან ერთად წარმოშვა რისკები, რომლებიც ხშირად პირის პირადი ცხოვრების უფლების ეფექტიანად სარგებლობის ხელშეშლას უკავშირდება. ინტერნეტსივრცეში მონაცემთა დამუშავება სულ უფრო მეტად ფართო მასშტაბს იღებს. განსაკუთრებით აქტუალურია სხვადასხვა სოციალურ ქსელსა თუ პლატფორმაზე მონაცემების გამჟღავნების გზით დამუშავება, რაც აკრძალულ ქმედებად არ მიიჩნევა იმ შემთხვევაში, თუ დამუშავება პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოთხოვნებთან თავსებადია.

წინამდებარე ნაშრომის მიზანია, პრაქტიკული მაგალითების საფუძველზე წარმოაჩინოს სოციალურ ქსელებში მონაცემთა გამჟღავნებით დამუშავების თავისებურებები და განსაზღვროს გარემოებები და კრიტერიუმები, რომელთა არსებობის, დაკმაყოფილების შემთხვევაში მონაცემთა დამუშავება კანონიერად მიიჩნევა.

საკვანძო სიტყვები: *მონაცემთა სუბიექტი, დამუშავებისთვის პასუხისმგებელი პირი, მონაცემთა დამუშავება, სოციალური ქსელები.*

1. შესავალი

საინფორმაციო ტექნოლოგიების განვითარების კვალდაკვალ პერსონალურ მონაცემთა დამუშავების კანონშესაბამისობის საკითხი სულ უფრო მეტად აქტუალური ხდება. მონაცემთა ავტომატური საშუალებებით დამუშავების პროცესში არსებული გამოწვევების, რისკებისა და საფრთხეების მიუხედავად, ხშირად საკუთარ მონაცემებს ინტერნეტსივრცეში თავად მონაცემთა სუბიექტები ასაჯაროებენ ისე, რომ პერსონალური მონაცემების

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის აპარატის უფროსი იურისტი.

სხვათა მიერ შესაძლო, არასასურველ დამუშავებაზე არ ფიქრობენ და, შესაბამისად, დარღვეული უფლების აღდგენის მიზნით, მიმართავენ შესაბამის დაწესებულებას, უფლებამოსილ პირს ან სასამართლოს.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა დამუშავების ფორმებს ამომწურავად არ ჩამოთვლის. მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება თავისთავად მიიჩნევა მონაცემთა დამუშავებად. განსახილველ შემთხვევაში წინამდებარე კვლევის მიზანი არ არის სოციალურ ქსელებში მონაცემთა დამუშავების ყველა ფორმისა თუ პროცესის სრულყოფილი მიმოხილვა და ანალიზი. საგულისხმოა, რომ პერსონალურ მონაცემთა დამუშავების ყველაზე გავრცელებულ ფორმას ინტერნეტსივრცეში მათი გამჟღავნება, გასაჯაროება, გავრცელება ან სხვაგვარად ხელმისაწვდომად გახდომა წარმოადგენს. საკითხს კიდევ უფრო მეტად ავიწროებს დამუშავებისთვის პასუხისმგებელი პირის წინმსწრებად იდენტიფიცირება, კერძოდ, ნაშრომში განიხილება ფიზიკური პირების და არა საჯარო თუ კერძო დაწესებულებების მიერ მონაცემთა დამუშავების შემთხვევები. საკითხის ამგვარი დაკონკრეტება განპირობებულია იმით, რომ მონაცემთა დაცვის ეროვნული კანონმდებლობა მხოლოდ ფიზიკურ პირს ანიჭებს შესაძლებლობას, აშკარა პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებისას არ შეიზღუდოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი მოთხოვნებით. შესაბამისად, საკითხს უფრო მეტად აქტუალურს ხდის პირადი ცხოვრების, პერსონალურ მონაცემთა დაცვის უფლების სხვა უფლებათა მიმართ პრიმატის ცალკეული შემთხვევების იდენტიფიცირებისა და მონაცემთა დამუშავების კონკრეტულ ფაქტებზე „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოქმედების გავრცელების თემატიკის მიმოხილვა.

ნაშრომში განიხილება ფიზიკურ პირთა მიერ სოციალურ ქსელებში მონაცემთა სუბიექტების (ფიზიკური პირების) პერსონალურ მონაცემთა გამჟღავნების გზით დამუშავების სამართლებრივი ასპექტები, საკითხთან დაკავშირებული თეორიული მსჯელობა, პერსონალურ მონაცემთა დაცვის სამსახურის რელევანტური პრაქტიკა, მონაცემთა დაცვის საზედამხედველო ორგანოების, ადამიანის უფლებათა ევროპული სასამართლოს მნიშვნელოვანი მიდგომები. ასევე, წინამდებარე სტატიაში განხილულია: სოციალურ ქსელებში პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძვლები, სამეწარმეო და ეკონომიკური საქმიანობის ფარგლებში მონაცემთა დამუშავების შემთხვევები სოციალურ ქსელებში, პროფესიული საქმიანობისა და სამსახურებრივი მოვალეობის შესრულების დროს სოციალურ ქსელებში მონაცემთა დამუშავების თავისებურებები და აშკარა პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავება.

2. სოციალური ქსელის მეშვეობით პერსონალურ მონაცემთა დამუშავების სამართლებრივი საფუძვლები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი მოთხოვნები არ ვრცელდება ფიზიკურ პირზე, რომელიც აშკარად პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში დაამუშავებს პერსონალურ მონაცემებს. მოქმედი კანონმდებლობის თანახმად, ზემოაღნიშნული მიზნისა თუ საქმიანობის ფარგლებში მონაცემთა დამუშავება შესაძლოა სოციალურ ქსელში ფიზიკური პირის ინტერნეტაქტივობას მოიცავდეს, რასაც ბუნებრივია, რომ აქვს გარკვეული ფარგლები და ცალკეულ შემთხვევებში ფიზიკური პირი სოციალურ ქსელებში განხორციელებული მოქმედებებით პერსონალურ მონაცემთა დამუშავებისას შეზღუდულია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით დადგენილი მოთხოვნებით. მაგალითად, თუკი ფიზიკური პირი სოციალურ ქსელში გაამჟღავნებს სხვა პირის პერსონალურ მონაცემს და დადგინდება, რომ იგი იმავდროულად მოქმედებდა სამეწარმეო, ეკონომიკური, პროფესიული ან სამსახურებრივი მოვალეობის შესრულების ფარგლებში, მასზე, როგორც დამუშავებისთვის პასუხისმგებელ ან დამუშავებაზე უფლებამოსილ პირზე, კანონის მოქმედება გავრცელდება.

ამდენად, იმ შემთხვევაში, როცა ფიზიკური პირის მიერ მონაცემთა დამუშავება კანონით დადგენილ საგამონაკლისო შემთხვევებს არ მიესადაგება, დამუშავებისთვის პასუხისმგებელ პირს ექნება ვალდებულება, პერსონალურ მონაცემთა დაცვის სამსახურის მიერ განხორციელებულ მონაცემთა დამუშავების კანონიერების შესწავლის პროცესში თავად დაასაბუთოს მონაცემთა დამუშავების სამართლებრივი საფუძველი „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-5 ან მე-6 (განსაკუთრებული კატეგორიის მონაცემის დამუშავების შემთხვევაში) მუხლის შესაბამისად.

მონაცემთა დამუშავების ერთ-ერთი უნივერსალური სამართლებრივი საფუძველი თავად მონაცემთა სუბიექტის ზეპირი ან წერილობითი (მათ შორის, ელექტრონული) თანხმობაა (როდესაც პერსონალური მონაცემების მოპოვება თავად მონაცემთა სუბიექტისგან ხდება). იმ შემთხვევაში, თუ მონაცემთა სუბიექტის მიერ გაცხადებული თანხმობა მისი მონაცემების დამუშავების თაობაზე არ მოიცავს დამუშავებისთვის პასუხისმგებელი პირისათვის უფლებამოსილების მინიჭებას — მონაცემთა სუბიექტის მონაცემები დაამუშაოს სოციალურ ქსელში გამჟღავნების გზით, მონაცემთა დამუშავების შემთხვევაში იგი თავდაპირველ მიზანთან შეუთავსებელი იქნება და დამუშავებისთვის პასუხისმგებელ პირს ექნება ვალდებულება, მონაცემთა დამუშავების აღნიშნული პროცესი კანონით გათვალისწინებული სხვა რელევანტური სამართლებრივი საფუძვლით დაასაბუთოს. რთულად

წარმოსადგენია შემთხვევა, რომ ფიზიკური პირის მიერ სოციალურ ქსელში მონაცემთა გამჟღავნებას სამართლებრივ საფუძვლად მონაცემთა სუბიექტის თანხმობა დაედოს, როდესაც მონაცემთა დამუშავებას სადავოდ ხდის თავად მონაცემთა სუბიექტი.

განსაკუთრებით საინტერესოა შემთხვევა, როდესაც პერსონალური მონაცემების დამუშავება ეფუძნება გარემოებას, რომლის თანახმად, მონაცემთა სუბიექტმა მისივე მონაცემები მანამდე თავად გაასაჯაროვა, ხოლო განსაკუთრებული კატეგორიის მონაცემთა შემთხვევაში — გამოყენების აშკარა აკრძალვის დათქმის გარეშე საჯარო გახადა ისინი. ამ თვალსაზრისით რელევანტურია პერსონალურ მონაცემთა დაცვის სამსახურის მიერ არაგეგმური შემოწმების ფარგლებში შესწავლილი ერთ-ერთი შემთხვევა, რომელიც ზემოაღნიშნული საფუძვლით მონაცემთა დამუშავებას შეეხებოდა. საქმის გარემოებების თანახმად, მონაცემთა სუბიექტმა სოციალურ ქსელ “Tiktok”-ზე ვიდეოჩანაწერი განათავსა, რომელშიც იგი გარკვეული პროდუქტის სარგებლიანობის შესახებ საუბრობდა. გავრცელებული ვიდეოჩანაწერის ნაწილი, რომელიც განმცხადებლის პერსონალურ მონაცემებს (ვიზუალურ გამოსახულებასა და ხმას) შეიცავდა, სოციალურ ქსელ “Facebook”-ის, “Instagram”-ის და “Tiktok”-ის გვერდებზე ერთ-ერთი ანგარიშის მფლობელი ფიზიკური პირის მიერ განთავსდა. განმცხადებელი განმარტავდა, რომ, ანგარიშის მფლობელმა მისი ნებართვის გარეშე, კომერციული მიზნებისთვის (პროდუქტის რეკლამირებისთვის) გამოიყენა მისი პერსონალური მონაცემების შემცველი ვიდეორგოლი, რომელიც თავად სოციალურ ქსელ “Tiktok”-ის საკუთარ ანგარიშზე განათავსა, რომელზეც 500 000-ზე (ხუთასი ათასზე) მეტი მიმდევარი ჰყავდა. დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, იგი მონაცემთა სუბიექტის მიერ რეკლამირებული პროდუქტის ონლაინ გაყიდვას ახორციელებდა და სხვადასხვა სოციალურ ქსელში საკუთარ ანგარიშებზე განმცხადებლის პერსონალური მონაცემების შემცველი ვიდეოჩანაწერი პროდუქტის საქართველოში ხელმისაწვდომობის შესახებ საზოგადოების ინფორმირების მიზნით განათავსა. პერსონალურ მონაცემთა დაცვის სამსახურმა საქმის შესწავლის შედეგად დაადგინა, რომ განმცხადებელს მის მიერ განთავსებულ ვიდეოჩანაწერზე გააქტიურებული ჰქონდა გაზიარების, ასევე, “Duet” და “Stich” ფუნქციონალი, რაც სხვა ანგარიშის მფლობელის მიერ აღნიშნული ვიდეორგოლის, მისი ფრაგმენტის გამოყენების გზით, ახალი ვიდეოს შექმნის შესაძლებლობას იძლეოდა. სამსახურმა განმარტა, რომ ვიდეორგოლის განთავსებისას განმცხადებელს გააზრებული უნდა ჰქონოდა ვიდეორგოლის საჯაროდ ხელმისაწვდომობისა და მისი შემდგომი შესაძლო დამუშავების რისკი. დადგინდა, რომ მონაცემთა დამუშავება კანონის მე-5 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტით გათვალისწინებულ მონაცემთა დამუშავების საფუძვლიდან გამომდინარეობდა, ვინაიდან მონაცემთა სუბიექტმა თავისი პერსონალური მონაცემები საჯაროდ ხელმისაწვდომი გახადა. ამდენად, ფიზიკური პირის მიერ განმცხადებლის მონაცემთა სხვადასხვა სოციალურ ქსელში დამუშავების

პროცესში „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოთხოვნების დარღვევა არ გამოვლინდა.[1]

ასევე, მონაცემების საჯაროობა შესაძლოა გამომდინარეობდეს კანონმდებლობიდან. მაგალითად, „საჯარო რეესტრის შესახებ“ საქართველოს კანონის[2] მე-6 მუხლის პირველი პუნქტის თანახმად, საჯარო რეესტრში რეგისტრირებული მონაცემები და მარეგისტრირებელ ორგანოში დაცული დოკუმენტაცია არის საჯარო. რეესტრის საჯაროობასა და ინფორმაციის გამოქვეყნებას ვალდებულებას ასევე ითვალისწინებს „მეწარმეთა შესახებ“ საქართველოს კანონი.[3] აღნიშნულ მონაცემთა საჯაროობა შესაძლოა განპირობებული იყოს, მაგალითად, სამოქალაქო ბრუნვის სტაბილურობის მიზნის მიღწევით, თუმცა, რა მიზანსაც არ უნდა ისახავდეს კანონმდებელი მონაცემთა საჯაროობის დადგენისას, ასეთის არსებობის შემთხვევაში მონაცემთა სუბიექტისათვის მოულოდნელი არ უნდა იყოს მისი მონაცემთა დამუშავების თაობაზე ინფორმაცია.

პერსონალურ მონაცემთა დამუშავება ცალკეულ შემთხვევებში შესაძლოა დამუშავებისთვის პასუხისმგებელი ან მესამე პირის ლეგიტიმური ინტერესის დაცვის მიზანს ემსახურებოდეს, გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესზე პრევალირებს მონაცემთა სუბიექტის (მათ შორის, არასრულწლოვნის) უფლებების დაცვის აღმატებული ინტერესი.[4] დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური მიზანი და მონაცემთა დამუშავების აუცილებლობა თითოეულ ინდივიდუალურ შემთხვევაში დამოუკიდებლად უნდა შეფასდეს და მოხდეს მხარეთა ინტერესების შეპირისპირება კანონიერი და სამართლიანი გადაწყვეტილების მისაღებად. აღნიშნულ საკითხთან მიმართებით პერსონალურ მონაცემთა დაცვის სამსახურმა განიხილა საქმე, რომელიც ფიზიკური პირის მიერ მონაცემთა სუბიექტის მონაცემების სოციალურ ქსელ “Facebook”-ში გასაჯაროებას ეხებოდა. საქმის გარემოებების თანახმად, მხარეთა შორის ზეპირი შეთანხმება დაიდო. მონაცემთა სუბიექტმა თავისი სამეწარმეო საქმიანობიდან გამომდინარე, იკისრა ვალდებულება, დამუშავებისთვის პასუხისმგებელი ფიზიკური პირისთვის ჩინეთის სახალხო რესპუბლიკიდან საქართველოში სატრანსპორტო საშუალებები გარკვეული ანაზღაურების სანაცვლოდ გამოეგზავნა. დამუშავებისთვის პასუხისმგებელი პირი განმარტავდა, რომ მონაცემთა სუბიექტმა მასთან დადებული შეთანხმების პირობები დაარღვია, ვინაიდან სატრანსპორტო საშუალებები მეორადი მასალით/ნაწილებით იყო დამზადებული, რის გამოც მათ ექსპლუატაციას ვერ ახერხებდა, ხოლო განმცხადებელთან აღნიშნული პრობლემის აღმოფხვრის თაობაზე კომუნიკაცია უშედეგოდ მთავრდებოდა. საქმის შესწავლის ფარგლებში

[1] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 3 აპრილის №გ-1/107/2025 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით)*.

[2] „საჯარო რეესტრის შესახებ“ საქართველოს კანონი, 820, 19/12/2008, მუხლი 6, პუნქტი 1.

[3] „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-Xმპ, 02/08/2021, მუხლი 13, პუნქტი 1.

[4] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 5, პუნქტი 1, ქვეპუნქტი „ი“.

გამოიკვეთა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა სოციალურ ქსელ "Facebook"-ის პირად ანგარიშზე და ერთ-ერთ საჯარო ჯგუფში განმცხადებლის პერსონალური მონაცემები „პოსტისა" და „სქრინშოთის" სახით გამოაქვეყნა, რომლებიც განმცხადებლის ფეისბუქგვერდის პროფილის „სქრინშოთებს" (რომლებზეც ასახული იყო მისი სახელი, გვარი, ორი ფოტოსურათი („პროფილის" და "Cover" ფოტოსურათები) და პასპორტის ფოტოსურათის ნაწილს (ასევე, პასპორტის ფოტოს)) შეიცავდა. დამუშავებისთვის პასუხისმგებელი პირი განმარტავდა, რომ მონაცემთა გამჟღავნების მიზანს არა განმცხადებლის დისკრედიტაცია, შანტაჟი, არამედ საკუთარი ინტერესების დაცვა წარმოადგენდა, ხოლო ვინაიდან განმცხადებელმა არაერთ პირს მიაყენა ქონებრივი ზიანი, დაზარალებულთა წრე შესაძლოა კიდევ უფრო გაზრდილიყო. ამდენად, მისი ქმედება ემსახურებოდა ლეგიტიმურ მიზანს, დაეცვა თავისი და მესამე პირების ქონებრივი ინტერესები და მოეხდინა საზოგადოების ინფორმირება. აქედან გამომდინარე, იგი მიიჩნევდა, რომ სოციალურ ქსელ "Facebook"-ში გავრცელებული ინფორმაცია იყო პროპორციული და მინიმალური მოცულობისა. დამუშავებისთვის პასუხისმგებელი პირი დამატებით მისი გამოხატვის თავისუფლების უფლებით სარგებლობაზე მიუთითებდა. პერსონალურ მონაცემთა დაცვის სამსახურმა ლეგიტიმურად მიიჩნია დამუშავებისთვის პასუხისმგებელი პირის ზემოაღნიშნული ინტერესი, თუმცა განმარტა, რომ განმცხადებლის მონაცემთა დამუშავება არ აკმაყოფილებდა „აუცილებლობის" კრიტერიუმს. დადგინდა, რომ განმცხადებლის ფეისბუქგვერდის პროფილის „სქრინშოთებზე" ასახული ინფორმაცია თავად განმცხადებელს ჰქონდა გასაჯაროებული, რაც მათი დამუშავების სამართლებრივ საფუძველს ქმნიდა, თუმცა დამუშავებისთვის პასუხისმგებელ პირს მისი ლეგიტიმური ინტერესის დაცვა შეეძლო მონაცემთა სუბიექტის პირადი ცხოვრების უფლების სხვა უფრო ნაკლებად მზღუდავი საშუალებით - სოციალურ ქსელში განმცხადებლის პასპორტის „სქრინშოთის" გავრცელების გარეშე. ამდენად, მიუხედავად იმისა, რომ დამუშავებისთვის პასუხისმგებელი პირი სარგებლობდა გამოხატვის თავისუფლების უფლებით, იგი ვალდებული იყო, თავისი მიზანი — საკუთარი ქონებრივი ინტერესების დაცვა და მესამე პირებისთვის ინფორმაციის მიწოდება — მონაცემთა პროპორციული დამუშავებით მიეღწია. ზემოაღნიშნულიდან გამომდინარე, სამსახურმა დაადგინა კანონის მე-5 მუხლის დარღვევა და, შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს კანონის 67-ე მუხლით გათვალისწინებული ადმინისტრაციული სახდელი დააკისრა.[5]

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი დამუშავებისთვის პასუხისმგებელ პირს ავალდებულებს, პერსონალური მონაცემები დაამუშაოს სულ მცირე ერთ-ერთი სამართლებრივი საფუძვლიდან გამომდინარე, რომელთა ამომწურავი ჩამონათვალი განსაზღვრულია კანონის

[5] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 23 ივლისის №გ-1/259/2025 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).*

მე-5 და მე-6 მუხლებით. მონაცემთა დამუშავების ნებისმიერ პროცესში გამოყენებული სამართლებრივი საფუძვლის მტკიცების ტვირთი დამუშავებისთვის პასუხისმგებელ პირს აკისრია, რომლის რელევანტურობას მონაცემთა დამუშავების კანონიერების შესწავლის განმავლობაში პერსონალურ მონაცემთა დაცვის სამსახური აფასებს.

3. სამეწარმეო და ეკონომიკური საქმიანობის ფარგლებში მონაცემთა დამუშავება

სამეწარმეო საქმიანობა არის მოგების მიღების მიზნით განხორციელებული მართლზომიერი, არაერთჯერადი, დამოუკიდებელი და ორგანიზებული საქმიანობა. სამეწარმეო საქმიანობა შეიძლება განხორციელდეს ინდივიდუალური მეწარმის ან სამეწარმეო საზოგადოების ფორმით.[6] ეკონომიკურ საქმიანობად კი განიხილება ნებისმიერი საქმიანობა, რომელიც ხორციელდება შემოსავლის ან კომპენსაციის მისაღებად, მიუხედავად ამ საქმიანობის შედეგისა.[7] ზემოაღნიშნულ საქმიანობათა ფარგლებში ფიზიკური პირის მიერ მონაცემთა დამუშავება არ მიიჩნევა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოქმედების სფეროდან გამონაკლისად და მსგავს შემთხვევებში ფიზიკური პირის მიერ მონაცემთა დამუშავება კანონით დადგენილ მოთხოვნებს უნდა შეესაბამებოდეს.

პერსონალურ მონაცემთა დაცვის სამსახურმა საქართველოს სახალხო დამცველის აპარატის შეტყობინების საფუძველზე განიხილა საქმე, რომელიც არასრულწლოვანთა მონაცემების სოციალურ ქსელ “Facebook“-ის ერთ-ერთი გვერდის მეშვეობით დამუშავებას ეხებოდა. საქმის გარემოებების თანახმად, ინდივიდუალური მეწარმის ფორმით მეწარმეთა და არასამეწარმეო იურიდიულ პირთა რეესტრში რეგისტრირებულმა დამუშავებისთვის პასუხისმგებელმა პირმა, რომელიც ზემოაღნიშნული სოციალური ქსელის გვერდს მართავდა, ამავე გვერდზე განათავსა პოსტი, რომლითაც გაავრცელა მოწოდება — არასრულწლოვნების მშობლებს/კანონიერ წარმომადგენლებს, როგორც ფეისბუქმომხმარებლებს, მცირეწლოვანთა ფოტოსურათები პოსტის კომენტარების ველში ფოტოგადაღების კონკურსში მონაწილეობის მიზნით აეტვირთათ. დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, კონკურსის გამარჯვებული პოსტის კომენტარების ველში განთავსებული ფოტოსურათის „მოწონების“ რაოდენობითა და კონკრეტული ელექტრონული პროგრამით შემთხვევითობის პრინციპით გამოვლინდებოდა. დადგინდა, რომ მცირეწლოვანთა ფოტოსურათები, რომელთა ნაწილი შიშველი ბავშვების ვიზუალურ გამოსახულებას შეიცავდა, პოსტის მეშვეობით საჯაროდ იყო

[6] „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-Xმპ, 02/08/2021, მუხლი 2, პუნქტი 2 და 3.
[7] საქართველოს კანონი „საქართველოს საგადასახადო კოდექსი“, 3591, 17/19/2010, მუხლი 9, პუნქტი 1. სსიპ საქართველოს სტატისტიკის ეროვნული სამსახურის მიერ დამტკიცებულია საქართველოს ეროვნული კლასიფიკატორით გათვალისწინებული ეკონომიკური საქმიანობის სახეები, იხ. <https://www.geostat.ge/media/70150/NACE-Rev_2_GE_2023.pdf> [30.8.2025].

განთავსებული კონკურსის დასრულების შემდეგაც. პერსონალურ მონაცემთა დაცვის სამსახურმა მიიჩნია, რომ ვინაიდან ფიზიკური პირი ზემოაღნიშნულ საქმიანობას ინდივიდუალური მეწარმის ფორმით ახორციელებდა, მონაცემთა დამუშავების პროცესზე „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი გავრცელდებოდა, ხოლო, მიუხედავად იმისა, რომ ამავე ფიზიკური პირის მიერ გამოქვეყნებულ პოსტზე მცირეწლოვანთა ფოტოსურათებს მათი მშობლები/კანონიერი წარმომადგენლები ათავსებდნენ, აღნიშნული ფიზიკური პირი მიჩნეულ იქნა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირად, ვინაიდან იგი ავტომატურად, ზემოთ დასახელებული გზით, კონკურსში მონაწილეთა ფოტოსურათებს თავისი სამეწარმეო საქმიანობის ფარგლებში აგროვებდა. მიუხედავად იმისა, რომ არასრულწლოვანთა ფოტოსურათები ინტერნეტსივრცეში მათი მშობლების/კანონიერი წარმომადგენლების ნება-სურვილით გავრცელდა, პერსონალურ მონაცემთა დაცვის სამსახურმა დამუშავებისთვის პასუხისმგებელ პირს მისცა შესასრულებლად სავალდებულო დავალება, არასრულწლოვანთა საუკეთესო ინტერესებიდან გამომდინარე, წაეშალა პოსტის კომენტარების ველში განთავსებული ფოტოსურათები კომენტარებთან ერთად, ხოლო იმავე ფორმატის კონკურსის ჩატარების შემთხვევაშიც, შესაბამისი მიზნის მიღწევის შემდეგ, შეესრულებინა ზემოაღნიშნული დავალება.[8]

საინტერესოა შემთხვევა, როდესაც პროფესიული საქმიანობის ფარგლებში მოქმედებს არა დამუშავებისთვის პასუხისმგებელი პირი, არამედ თავად მონაცემთა სუბიექტი და მონაცემების დამუშავება მის მიერ სამსახურებრივი საქმიანობის განხორციელებას უკავშირდება. ადამიანის უფლებათა ევროპულმა სასამართლომ განიხილა საქმე *“Toth and Crișan v. Romania”,*[9] რომლის ფაქტობრივი გარემოებების თანახმად, 2016 წლის 8 აპრილს პოლიციის ოფიცრებმა (მომჩივნებმა) ს.ტ.-ს და მის დედას საყოფაცხოვრებო ნარჩენის გადაყრის წესების დარღვევის გამო ჯარიმა დააკისრეს. იმავე დღეს ს.ტ.-მ სოციალურ ქსელ “Facebook”-ის პირადი ანგარიშის გამოყენებით საჯარო ჯგუფში გამოაქვეყნა პოსტი, რომელსაც თან ახლდა მომჩივნების ფოტოსურათი, რომელიც შემთხვევის ადგილზე იყო გადაღებული. პოსტი აღწერდა მომხდარ შემთხვევას და მასში მითითებული იყო, რომ პოლიციელებმა დედა-შვილზე ბავშვის თანდასწრებით ფიზიკურად იძალადეს და მათ სიტყვიერი შეურაცხყოფა მიაყენეს. საჯარო ჯგუფში განთავსებულ პოსტს მოჰყვა ჯგუფის წევრების გამოხმაურება. პოსტზე განთავსებული კომენტარებით ფეისბუქმომხმარებლები მომჩივნებს შეურაცხმყოფელი სიტყვებით (მაგ., „ნაძირლები“, „იდიოტები“, „გიჟები“, „გაუნათლებლები“) მოიხსენიებდნენ. ზოგიერთმა მომხმარებელმა ამოიცნო პოლიციის ოფიცრების ვინაობა, ისინი მიუთითებდნენ მათ მიერ ადრე ჩადენილ მსგავს შემთხვევებზე. პოსტის კომენტარებში ს.ტ.-მ გაამჟღავნა ერთ-

[8] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 1 აგვისტოს №გ-1/269/2025 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).*
[9] Case of Toth and Crișan v. Romania, [2025] ECHR, App. No. 45430/19.

ერთი მომჩივნის სახელი და გვარი და აღნიშნა, რომ იგი მიზნად არ ისახავდა მათ ცილისწამებას.

მომჩივნებმა ადგილობრივ სასამართლოს არამატერიალური ზიანის ანაზღაურების და ს.ტ.-ს მიერ ადგილობრივ გაზეთებსა და საჯარო ჯგუფში ბოდიშის მოხდის დავალდებულების მოთხოვნით მიმართეს, ვინაიდან მომჩივნების ფოტოსურათი და ერთ-ერთი მათგანის სახელი და გვარი მათი თანხმობის გარეშე ს.ტ.-მ გაასაჯაროვა, რამაც სხვათა მიერ შეურაცხმყოფელი კომენტარების განთავსება და დამსაქმებლის მიერ მათდამი დისციპლინური წარმოების აღძვრა გამოიწვია. ეროვნულმა სასამართლოებმა მომჩივნების მოთხოვნა არ დააკმაყოფილეს და მიიჩნიეს, რომ პოსტი არ იყო ცილისმწამებლური. იგი ს.ტ.-ს მიერ მოვლენის თავისებურ აღქმას გადმოსცემდა და წარმოადგენდა მისი გამოხატვის თავისუფლების უფლების რეალიზების საშუალებას — სოციალურ ქსელში საჯაროდ გაევრცელებინა ინფორმაცია მომხდარის თაობაზე მისი უკმაყოფილების შესახებ. ასევე, იგი ვერ იქნებოდა პასუხისმგებელი სხვათა მიერ განთავსებულ კომენტარებზე, რადგან მათი წაშლა ან განთავსების აკრძალვა არ შეეძლო. სასამართლოებმა ასევე განმარტეს, რომ მომჩივნების ფოტოსურათი და ერთ-ერთი მათგანის სახელი და გვარი საჯაროდ გავრცელა, თუმცა ისინი საჯარო პირები იყვნენ და ფოტოსურათში უხამსი ფორმით არ იყვნენ ასახული.

მომჩივნებმა ადამიანის უფლებათა ევროპულ სასამართლოს ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის სავარაუდო დარღვევის თაობაზე მიმართეს. სასამართლომ განმარტა, რომ ფოტოსურათის გამოქვეყნება პირადი ცხოვრების პატივისცემის უფლებაში უფრო არსებით ჩარევად მიიჩნევა, ვიდრე პირის სახელისა და გვარის გამჟღავნება. ამასთან, იმ შემთხვევაში, თუ ქმედება არ შედის პოლიტიკური ან საზოგადოებრივი დებატების სფეროში და გამოქვეყნებული ფოტოსურათი და პოსტის თანმხლები კომენტარები მხოლოდ პირის პირადი ცხოვრების დეტალებს ეხება, რომლის ერთადერთი მიზანია კონკრეტული მკითხველის ცნობისმოყვარეობის დაკმაყოფილება, გამოხატვის თავისუფლების უფლება ამ დროს უფრო ვიწრო ინტერპრეტაციას მოითხოვს. სასამართლოს განმარტებით, პირადი ცხოვრების პატივისცემის უფლებისა და გამოხატვის თავისუფლების უფლების დაბალანსების შესაბამისი კრიტერიუმებია: საზოგადოებრივი ინტერესის საკითხებში წვლილის შეტანა; „დაზარალებული“ პირის ცნობადობის ხარისხი; პირის წინარე ქცევა; ფოტოს გადაღების გარემოებები და გამოქვეყნებული ინფორმაციის შინაარსი, ფორმა და შედეგები. პოსტთან ერთად ფოტოსურათის განთავსება სასამართლომ გამართლებულად მიიჩნია, ვინაიდან აღნიშნული გზით ხდებოდა პოსტში მითითებული ინფორმაციის დადასტურება. სასამართლოს შეფასებით, საზოგადოებრივი ინტერესის საკითხზე დებატების შეზღუდვის შესაძლებლობა მცირეა. ეროვნული სასამართლოებისგან განსხვავებით, ევროსასამართლომ საჯარო პირებად არ მიიჩნია განმცხადებლები, თუმცა აღნიშნა, რომ მათი სტატუსისა და საქმიანობიდან გამომდინარე, მათდამი

დასაშვები კრიტიკის ფარგლები უფრო ფართო იყო. შესაბამისად, საზოგადოებას ჰქონდა უფლება, მიეღო ინფორმაცია იმ პროფესიის ადამიანების შესახებ, რომლებიც ხალხს ემსახურებოდნენ, ხოლო მომჩივნებს უნდა ჰქონოდათ მოლოდინი, რომ, მათი სტატუსისა და საჯარო ქცევის გათვალისწინებით, მათთვის ფოტოსურათის გადაღებისა და შემდგომი დამუშავების შესაძლებლობა არსებობდა. შესაბამისად, სასამართლომ ადამიანის უფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლის დარღვევა არ დაადგინა.

4. პროფესიული და სამსახურებრივი მოვალეობის შესრულებასთან დაკავშირებული საქმიანობისას სოციალურ ქსელებში მონაცემთა დამუშავება

პირის პროფესიული ან სამსახურებრივი მოვალეობის შესრულებასთან დაკავშირებული მონაცემთა დამუშავება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედების სფეროში ექცევა.

პერსონალურ მონაცემთა დაცვის სამსახურმა განიხილა საქმე, რომელიც სოციალურ ქსელ “Facebook”-ზე ფიზიკურ პირთა მიმოწერის ამსახველი ვიდეოჩანაწერის გასაჯაროებას ეხებოდა. საქმის გარემოებების თანახმად, მონაცემთა სუბიექტმა ერთ-ერთ კომპოზიტორთან დადო შეთანხმება, რომლის მიხედვით, გარკვეული ანაზღაურების სანაცვლოდ, აღნიშნულ პირს მისთვის სიმღერა უნდა დაეწერა. მხარეთა შორის არსებული შეთანხმების პირობების დარღვევის გამო კომპოზიტორმა, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, სოციალურ ქსელ “Facebook”-ის პირად გვერდზე მასსა და განმცხადებელს შორის შემდგარი კომუნიკაციის ამსახველი ვიდეოჩანაწერი გამოაქვეყნა. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი განმარტავდა, რომ ვიდეოჩანაწერის გასაჯაროებით მიზნად ისახავდა განმცხადებლის თაღლითური საქმიანობის შესახებ საზოგადოების ინფორმირებას და კუთვნილი ჰონორარის მიღებას. პერსონალურ მონაცემთა დაცვის სამსახურმა მიიჩნია, რომ ზემოაღნიშნულ სოციალურ ქსელში მონაცემთა გასაჯაროება დამუშავებისთვის პასუხისმგებელი პირის პროფესიულ საქმიანობას უკავშირდებოდა. სამსახურმა დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირის მიერ განხორციელებული ქმედება „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-5 მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით განსაზღვრულ „აუცილებლობის“ კრიტერიუმს არ აკმაყოფილებდა, ვინაიდან მას საკუთარი უფლების დაცვა მონაცემთა სუბიექტის უფლებაში ჩარევის გარეშე, მაგალითად, სასამართლოსთვის მიმართვის გზით შეეძლო, ხოლო მესამე პირთა კანონიერი ინტერესის დაცვა და დამკვეთის მხრიდან ვალდებულების შეუსრულებლობის პრევენცია ხელშეკრულების დადებითა და მასში შესაბამისი პირობების ასახვით შეიძლებოდა. კანონის 67-ე მუხლის საფუძველზე სამსახურმა

დამუშავებისთვის პასუხისმგებელ პირს ადმინისტრაციული პასუხისმგებლობა დააკისრა და განმცხადებლის პერსონალური მონაცემების შემცველი ვიდეოჩანაწერის ფეისბუქგვერდიდან წაშლა დაავალა.[10]

პერსონალურ მონაცემთა დაცვის სამსახურმა პროფესიული საქმიანობის ფარგლებში მონაცემთა დამუშავებად შეაფასა უძრავი ქონების აგენტის მიერ კლიენტის მონაცემების სოციალურ ქსელ "Facebook"-ის ერთ-ერთ დახურულ ჯგუფში (რომელიც 128 000-ამდე წევრისგან შედგებოდა) გამოქვეყნება. უძრავი ქონების აგენტი, როგორც დამუშავებისთვის პასუხისმგებელი პირი, განმარტავდა, რომ განმცხადებელთან საქმიანი ურთიერთობის შესახებ ინფორმაცია და საკომუნიკაციო პლატფორმა "WhatsApp"-იდან მოპოვებული მონაცემთა სუბიექტის სახელი, გვარი, სატელეფონო ნომერი და ფოტოსურათი არაკეთილსინდისიერი კლიენტის შესახებ მისი კოლეგების ინფორმირების მიზნით გაასაჯაროვა. სამსახურმა დაადგინა, რომ გამჟღავნებული მონაცემები მოპოვებულ იქნა კლიენტთან პროფესიული ურთიერთობის ფარგლებში, თუმცა აღნიშნული არ მიიჩნია პროფესიულ საიდუმლოებად, ვინაიდან მხარეთა შორის არ არსებობდა შეთანხმება კონფიდენციალობის თაობაზე. ამასთან, ვინაიდან მონაცემთა დამუშავების სამართლებრივ საფუძველს დამუშავებისთვის პასუხისმგებელი პირი ვერ ასაბუთებდა და აღნიშნული არც საქმის შესწავლის ფარგლებში გამოიკვეთა, უძრავი ქონების აგენტი სამსახურმა კანონის მე-5 მუხლის მოთხოვნათა დარღვევის გამო სამართალდარღვევად ცნო.[11]

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი ერთ-ერთი საქმის გარემოებების თანახმად, სოციალურ ქსელ "Facebook"-ის დახურულ ჯგუფში განმცხადებლის სახელისა და გვარის შემცველი ანონიმური პოსტი განთავსდა, რომლის კომენტარების ველში ერთ-ერთი კომპანიის თანამშრომელმა პოსტში მითითებული ფაქტის დამაზუსტებელი ინფორმაცია გაავრცელა. პოსტისა და კომენტარის მიხედვით, განმცხადებელი კომპანიაში მომხდარი ფაქტის მთავარ ფიგურანტად სახელდებოდა. სამსახურმა ანონიმური პოსტისგან დამოუკიდებლად შეაფასა დამუშავებისთვის პასუხისმგებელი პირის მიერ განთავსებული კომენტარით განმცხადებლის მონაცემების დამუშავება, რითაც პოსტში მითითებული ინფორმაციის დადასტურება/დაზუსტება ხდებოდა. საქმის შესწავლის შედეგად დადგინდა, რომ დამუშავებისთვის პასუხისმგებელი პირი კომპანიის უსაფრთხოების სამსახურის უფროსის პოზიციაზე იყო დასაქმებული და მასთან დადებული შრომითი ხელშეკრულება კონფიდენციალობის დაცვის ვალდებულების შესახებ რეგულაციას მოიცავდა. კომპანია და დამუშავებისთვის პასუხისმგებელი პირი განმარტავდნენ, რომ კომენტარის დაფიქსირებისას თანამშრომელი კომპანიის დავალებით არ მოქმედებდა და საქმის

[10] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 3 ივნისის №გ-1/183/2025 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).*

[11] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მოვალეობის შემსრულებლის, სამსახურის უფროსის პირველი მოადგილის 2024 წლის 19 დეკემბრის №გ-1/374/2024 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).*

გარემოებები მის მიერ სამსახურებრივი უფლებამოსილების დროს მიღებული ინფორმაციის გამჟღავნებას არ მიუთითებდა. ამასთან, დამუშავებისთვის პასუხისმგებელი პირი მის მიერ მონაცემთა დამუშავების საფუძველს არ ასახელებდა. მიუხედავად ამისა, სამსახურმა დაადგინა, რომ განმცხადებლის მონაცემთა გასაჯაროების გზით დამუშავებისას არ არსებობდა შესაბამისი სამართლებრივი საფუძველი და კომპანიის თანამშრომელს კანონის 67-ე მუხლით გათვალისწინებული ადმინისტრაციული სახდელი დააკისრა.[12]

5. მონაცემთა დამუშავება აშკარა პირადი მიზნით და ოჯახური საქმიანობის ფარგლებში

ფიზიკური პირის მიერ აშკარა პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავება, როგორც პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოქმედების სფეროდან გამონაკლისი, ჯერ კიდევ ევროკავშირის 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივით იყო გათვალისწინებული.[13] აღნიშნული დირექტივის გაუქმების შემდეგ გამონაკლისი აისახა ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციაში“ (“GDPR”).[14] ევროპული კანონმდებლობის მსგავს ჩანაწერს შეიცავს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი და ადგენს, რომ კანონის მოქმედება არ ვრცელდება ფიზიკური პირის მიერ აშკარად პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებაზე, რომელიც დაკავშირებული არ არის მის სამეწარმეო ან/და ეკონომიკურ, პროფესიულ საქმიანობასთან ან სამსახურებრივი მოვალეობის შესრულებასთან. პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავება შეიძლება მოიცავდეს, მათ შორის, მიმოწერას, მისამართების დამუშავებას, ინტერნეტაქტივობას (მათ შორის, სოციალურ ქსელში), რომელიც ამ საქმიანობის ფარგლებში ხორციელდება.[15]

„ინტერნეტსივრცეში პოსტის განთავსებისას პირმა უნდა გაიაზროს, რომ იგი კარგავს კონტროლს საკუთარ ფოტოსურათზე, ჩანაწერებსა ან/და სხვა პერსონალურ მონაცემებზე“.[16] დღესდღეობით სოციალური ქსელების მეშვეობით პერსონალურ მონაცემთა დამუშავება საინფორმაციო ტექნოლოგიების განვითარების კვალდაკვალ სულ უფრო მეტად ფართო მასშტაბს იღებს. ფიზიკური პირები მონაცემთა დამუშავების არაერთი

[12] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 24 ოქტომბრის №გ-1/307/2024 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).*

[13] ევროკავშირის 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივა, OJ L 281, 23/11/1995, მუხლი 3. იხ.: <https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng> [18.9.2025].

[14] ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“, OJ L 119, 4/5/2016, პრეამბულა, პუნქტი 18, იხ.: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [18.9.2025].

[15] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 2, პუნქტი 2, ქვეპუნქტი „ა“.

[16] Yekaterina Macuka, Director of DVI, interview with “LSM”, <https://shorturl.at/pKZlH> [14.9.2025].

პროცესის ინიციატორები არიან. შეუძლებელია, რომ ონლაინ სივრცეში მონაცემთა გამოქვეყნების ყველა შემთხვევა უპირობოდ შეიზღუდოს და მიჩნეულ იქნას პერსონალურ მონაცემთა დაცვის კანონმდებლობის დარღვევად. იმ შემთხვევაში, თუ ფიზიკური პირის მიერ სოციალურ ქსელებში მონაცემთა გამჟღავნება მისი სამეწარმეო/კომერციული ან პროფესიული/სამსახურებრივი საქმიანობიდან გამომდინარეობს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად, საზედამხედველო ორგანო შეაფასებს მონაცემთა დამუშავების კანონიერებას. სხვა შემთხვევაში, რამდენად „აუცილებელია“ დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური მიზნის განხორციელება, უნდა შეფასდეს ინდივიდუალურად, სხვადასხვა კრიტერიუმზე დაყრდნობით.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ განხილული ერთ-ერთი საქმის გარემოებების თანახმად, პაციენტი კლინიკაში სამედიცინო მომსახურების მიღების მიზნით იმყოფებოდა. კლინიკის მიერ გაწეული მომსახურებით უკმაყოფილომ სამედიცინო პერსონალს ფოტოსურათები გადაუღო და “Google Reviews”-ს გვერდზე საჯაროდ განათავსა ნეგატიური შინაარსის კომენტართან ერთად. სამსახურმა დაადგინა, რომ პირმა ინტერნეტსივრცეში პერსონალური მონაცემები კლინიკის მიერ გაწეული მომსახურების მიმართ საკუთარი აზრის, დამოკიდებულებისა და შეფასების საჯაროდ გამოხატვის მიზნით გაავრცელა, ხოლო მონაცემები არ დამუშავებულა სამეწარმეო/ეკონომიკური ან/და პროფესიული/სამსახურებრივი საქმიანობის ფარგლებში. სამსახურმა ასევე განმარტა, რომ, სავარაუდოდ, წინამდებარე შემთხვევაზე ვრცელდებოდა ცილისწამებისა და ღირსების შელახვის მარეგულირებელი ნორმები.[17] საქართველოს სამოქალაქო კოდექსი იცავს პირად არაქონებრივ უფლებებს, რაც მოიცავს ასევე სოციალური ქსელის მეშვეობით გავრცელებულ ინფორმაციას.[18] „სოციალური ქსელის მეშვეობით პირის მიერ გავრცელებული ინფორმაცია, გამოთქმული აზრი, დაფიქსირებული მონაცემები შესაძლოა სხვათა უფლებებს არღვევდეს“.[19]

სხვისი პერსონალური მონაცემების სოციალურ ქსელებში გასაჯაროება, ყველა მომხმარებლისთვის ხელმისაწვდომობის უზრუნველყოფა არ წარმოადგენს პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებას. მაგალითად, ზემოთ აღნიშნული გამონაკლისი მიემართება სოციალური ქსელების მეშვეობით მიმოწერას ახლო მეგობრებისთვის, ოჯახის წევრებისთვის მონაცემთა გაზიარებას, რის შედეგად სხვა პირთა მონაცემები არ ხდება ხელმისაწვდომი სოციალური ქსელის ყველა

[17] პერსონალურ მონაცემთა დაცვის სამსახურის საჯარო ინფორმაციის ხელმისაწვდომობის უზრუნველყოფაზე პასუხისმგებელი პირის 2025 წლის 17 სექტემბრის №PDPS 3 25 00015900 კორესპონდენცია *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით)*.

[18] „საქართველოს სამოქალაქო კოდექსი“, 786, 26/06/1997, მუხლი 18.

[19] სამოქალაქო კოდექსის კომენტარი, წიგნი I, სამოქალაქო კოდექსის ზოგადი დებულებები, თბილისი, 2017, გვ. 112, იხ.: <https://lawlibrary.info/ge/books/giz2017-ge-civil_code_comm_I_Book.pdf> [20.9.2025].

მომხმარებლისთვის. გამონაკლისის მოქმედების მიზნებისათვის აუცილებელია მონაცემთა მიმღებთა რაოდენობის დადგენა. შესაბამისად, ფიზიკური პირის მიერ მონაცემთა გასაჯაროება, მიუხედავად იმისა მოქმედებდა თუ არა იგი კომერციული ან პროფესიული საქმიანობის ფარგლებში, იმთავითვე გამორიცხავს მისი მხრიდან პირადი მიზნით ან/და ოჯახური საქმიანობისას მონაცემთა დამუშავებას და საზედამხედველო ორგანოს აქვს შესაძლებლობა, შეისწავლოს მონაცემთა დამუშავების კანონიერება. თუმცა, ამავე ორგანოს მანდატიდან გამომდინარე, იმ შემთხვევაში, თუ გამოიკვეთება დამუშავებისთვის პასუხისმგებელი ფიზიკური პირის მიერ, მაგალითად, მისი გამოხატვის თავისუფლების უფლებით აშკარა სარგებლობის შემთხვევა, საზედამხედველო ორგანოს უნდა ჰქონდეს შესაძლებლობა, უარი თქვას განცხადების/საჩივრის განხილვაზე. ზემოაღნიშნულ შემთხვევაში მხარემ უფლების დაცვის მიზნით უნდა მიმართოს სასამართლოს და მოითხოვოს საკუთარი პატივის, ღირსების, პირადი ცხოვრების საიდუმლოების, პირადი ხელშეუხებლობის ან საქმიანი რეპუტაციის დაცვა შელახვისაგან, რასაც უმეტეს შემთხვევაში დაუპირისპირდება მეორე მხარის სიტყვისა და გამოხატვის თავისუფლების უფლება.

შეფასება იმისა, გასცდა თუ არა პირი მისი გამოხატვის თავისუფლების უფლების ფარგლებს, არ წარმოადგენს საზედამხედველო ორგანოს კომპეტენციას. აღნიშნული საკითხი განიხილა ისლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ, რომელმაც უარი თქვა, შეესწავლა არასრულწლოვნის ფოტოსურათების სოციალურ ქსელ “Facebook”-ზე გამოქვეყნების კანონიერება. საქმის გარემოებების თანახმად, ბავშვის მშობლებს შორის არსებობდა დავა მეურვეობის საკითხებთან დაკავშირებით. ერთ-ერთმა მშობელმა და მესამე პირმა (სოციალური ქსელის მომხმარებელმა) ამავე პლატფორმაზე მოზარდის ფოტოსურათები მეორე მშობლის მიმართ ცილისმწამებლურ კომენტარებთან ერთად განათავსეს. საზედამხედველო ორგანომ მიიჩნია, რომ ბავშვი იდენტიფიცირებადი იყო ფოტოსურათების მეშვეობით და “GDPR”-ის მიხედვით, სახეზე იყო მონაცემთა დამუშავება ფოტოსურათისა და თანმხლები კომენტარის გამოქვეყნების გზით. საზედამხედველო ორგანომ დაადგინა, რომ აღნიშნული შემთხვევა არ ექცეოდა პირადი მიზნით ან ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავების ჭრილში. ამ მხრივ განიმარტა, რომ გამონაკლისი ვრცელდებოდა მხოლოდ სოციალური ქსელის დახურულ ანგარიშებზე, რომელთა მეშვეობით გავრცელებული პოსტი ხელმისაწვდომი იქნებოდა პირთა შეზღუდული წრისთვის და არა ფართო საზოგადოებისთვის. დადგინდა, რომ ბავშვის მონაცემები ხელმისაწვდომი იყო სოციალურ ქსელ “Facebook”-ის ყველა მომხმარებლისთვის, რაიმე კონკრეტული შეზღუდვის გარეშე. ამდენად, სახეზე არ იყო პირადი მიზნით/ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავება და “GDPR”-ის მოქმედება ამ შემთხვევაზე გავრცელდა. საზედამხედველო ორგანომ მიიჩნია, რომ მშობელმა, რომელმაც გამოაქვეყნა

ბავშვის მონაცემები, ისარგებლა გამოხატვის თავისუფლების უფლებით, კერძოდ, საზოგადოებას აცნობა თავისი რთული მდგომარეობის შესახებ, რაც დაკავშირებული იყო ბავშვის მეურვეობის საკითხთან. საზედამხედველო ორგანომ იმ მოტივით, რომ მას არ ჰქონდა უფლება გამოეტანა გადაწყვეტილება სხვა პირთა კონსტიტუციით გარანტირებული გამოხატვის თავისუფლების უფლების შეზღუდვის საკითხზე, მიიჩნია, რომ ზემოაღნიშნული შემთხვევა სასამართლოს განსახილველი იყო. შესაბამისად, უარყო საჩივარი ერთ-ერთი მშობლისა და მესამე პირის მიერ სოციალურ ქსელში ბავშვის მონაცემის დამუშავების თაობაზე.[20]

პერსონალურ მონაცემთა დაცვის სამსახურმა აშკარა პირადი მიზნით მონაცემთა დამუშავებად არ მიიჩნია ფიზიკური პირის მიერ სოციალურ ქსელ "Facebook"-ზე ვიდეოჩანაწერის გამოქვეყნების გზით სხვა პირის პერსონალურ მონაცემთა დამუშავება. საქმის გარემოებების თანახმად, ფიზიკურმა პირმა ერთ-ერთი კომპანიის საკურიერო მომსახურებით ისარგებლა და საკვები პროდუქტი ადგილზე მიტანის სერვისით შეუკვეთა. შეკვეთის დაგვიანებით მიტანის გამო კომპანიის მომსახურებით უკმაყოფილო მომხმარებელმა მის მიღებაზე უარი განაცხადა და პრეტენზიის დაფიქსირების მიზნით ვიდეორგოლი ჩაწერა, რომელიც კურიერის ვიზუალურ გამოსახულებას შეიცავდა. დამუშავებისთვის პასუხისმგებელმა პირმა ვიდეორგოლი საკუთარ ფეისბუქგვერდზე საჯაროდ ხელმისაწვდომი ფორმით განათავსა. იგი განმარტავდა, რომ ვიდეოჩანაწერის შექმნისა და საჯაროდ ხელმისაწვდომი ფორმით განთავსების მიზანს წარმოადგენდა კომპანიის მიმართ პრეტენზიის დაფიქსირება და არა უშუალოდ კურიერისთვის შეურაცხყოფის მიყენება. სამსახურმა განმარტა, რომ ქმედება აშკარად პირადი ან ოჯახური საქმიანობის ფარგლებში განხორციელებულად ვერ მიიჩნევა, როდესაც მისი მიზანი შეგროვებული მონაცემების პირთა შეუზღუდავი რაოდენობისთვის ხელმისაწვდომობაა. ამასთან, გამონაკლისი ვერ გავრცელდება იმ შემთხვევაში, როცა კონკრეტული ქმედება/საქმიანობა, თუნდაც ნაწილობრივ, საჯარო სივრცეს მიემართება და პასუხისმგებელი პირის პირადი და ოჯახური საქმიანობის ფარგლებს სცდება. გადაწყვეტილებით დადგინდა, რომ სოციალური ქსელის გამოყენება და ონლაინ აქტივობები პირადი ან ოჯახური საქმიანობის კონტექსტში ექცევა, თუმცა აღნიშნული რელევანტურია მხოლოდ იმ შემთხვევაში, როდესაც მონაცემთა გაცვლა ხდება დახურულ ჯგუფებში, მომხმარებელთა პროფესიულ ან ეკონომიკურ საქმიანობასთან ყოველგვარი კავშირის გარეშე, ხოლო ასეთი სერვისების ექსკლუზიურად პირადი გამოყენება გამონაკლისის ფარგლებში ექცევა იმ პირობით, რომ მას თან არ უნდა ახლდეს პერსონალური მონაცემების ინტერნეტში შეუზღუდავად გამოქვეყნება. სამსახურმა შეაფასა დამუშავებისთვის პასუხისმგებელი პირის მნიშვნელოვანი ლეგიტიმური ინტერესის არსებობა და მის დასაცავად

[20] ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს 2021 წლის 17 ნოემბრის №2020010552 გადაწვეტილება, <https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_no._2020010552> [30.8.2025].

მონაცემთა დამუშავების აუცილებლობა (მონაცემთა დამუშავება აუცილებელია, როდესაც არ არსებობს მნიშვნელოვანი ლეგიტიმური ინტერესის დაცვის სხვა, უფრო მსუბუქი საშუალება). დამუშავებისთვის პასუხისმგებელმა პირმა საკუთარ პირად ფეისბუქგვერდზე განთავსებულ ვიდეოჩანაწერში ასახული პირის პერსონალური მონაცემების საჯაროდ ხელმისაწვდომი ფორმით განთავსების სამართლებრივი საფუძველი ვერ დაასაბუთა. სამსახურმა განმარტა, რომ მას შესაძლებლობა ჰქონდა, კომპანიის მიმართ უკმაყოფილების გამოხატვის ისეთი ალტერნატიული საშუალება გამოეყენებინა, რომელიც ვიდეოჩანაწერზე ასახული პირის პერსონალური მონაცემების დაცვის უფლებაში ნაკლებ ჩარევას გამოიწვევდა. მაგალითად, ზემოაღნიშნული ვიდეოჩანაწერი პირად ფეისბუქგვერდზე, თუმცა პირთა შეზღუდული წრისთვის ხელმისაწვდომი ფორმით ან დახურულ ჯგუფში განეთავსებინა ან/და კომპანიისთვის პრეტენზიის დაფიქსირების მიზნით წერილობითი კორესპონდენციით მიემართა. აღნიშნულ შემთხვევაზე სამსახურმა კანონის მე-5 მუხლის (დამუშავების სამართლებრივი საფუძველი) დარღვევა დაადგინა.[21]

ზემოთ მოხმობილი განმარტებებიდან გამომდინარე, ცხადია, რომ აშკარა პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავება არ არის სახეზე, როდესაც პერსონალური მონაცემები ხელმისაწვდომი ხდება პირთა განუსაზღვრელი წრისთვის.[22] მაგალითად, სოციალურ ქსელში ფიზიკური პირის მიერ მონაცემთა სუბიექტის ჯანმრთელობის შესახებ მონაცემის გამოქვეყნება, მიუხედავად მისი საქმიანობის ფარგლებისა, მოექცევა კანონის მოქმედების ქვეშ და საზედამხედველო ორგანო შეაფასებს, არსებობდა თუ არა ზემოაღნიშნული გზით მონაცემთა დამუშავების სამართლებრივი საფუძველი. საზედამხედველო ორგანოს ცალკეულ შემთხვევაში ასევე მართებს იმის შეფასება, საკითხი სრულად ხომ არ უკავშირდება დამუშავებისთვის პასუხისმგებელი პირის მიერ გამოხატვის თავისუფლების უფლებით სარგებლობას. მაგალითად, ამ შემთხვევაში გასათვალისწინებელია დამუშავების სოციალური ასპექტი, მხარეთა შორისი წინარე ურთიერთობა, პერსონალურ მონაცემთა დამუშავების ფაქტისა და მხარეთა შორის არსებული სასამართლო დავის ურთიერთკავშირი და ა.შ.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, პერსონალურ მონაცემთა დაცვის სამართალში ჩამოყალიბებული მიდგომების გათვალისწინებით, შესაძლებელია რამდენიმე კრიტერიუმის გამოყოფა, რომლებიც

[21] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 23 სექტემბრის №გ-1/355/2025 გადაწყვეტილება *(სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).*

[22] ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებით, თუ ფიზიკური პირის მიზანია შეგროვებული მონაცემების პირთა შეუზღუდავი წრისთვის ხელმისაწვდომობის უზრუნველყოფა, მაშინ სახეზე არ არის აშკარა პირადი მიზნით მონაცემთა დამუშავების შემთხვევა, იხ.: <https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].

საზედამხედველო ორგანოებს საკითხის სწორად შეფასებაში დაეხმარებათ.[23] საზედამხედველო ორგანოებმა ფიზიკური პირის მიერ პირადი ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავების შემთხვევის არსებობა უნდა დაადგინონ შემდეგი კრიტერიუმების გამოყენებით:

- **მონაცემთა დამუშავების სივრცე** - სოციალურ ქსელებში პირთა განუსაზღვრელი წრისთვის მონაცემთა გაზიარება არ არის პირადი მიზნით მონაცემთა დამუშავება;
- **დამუშავების სოციალური ასპექტი** - გასათვალისწინებელია გარემო, რომელშიც ფიზიკური პირი პერსონალურ მონაცემებს ამუშავებს, ასევე - მონაცემთა სუბიექტები და პირთა წრე, რომელთათვისაც ხელმისაწვდომია გავრცელებული მონაცემები;
- **მონაცემთა დამუშავების აუცილებლობა** - დამუშავება უნდა იყოს აუცილებელი ფიზიკური პირის ლეგიტიმური მიზნის მისაღწევად (მაგ., გამოხატვის თავისუფლების უფლებით სარგებლობის შემთხვევაში);
- **ფიზიკური პირის საქმიანობის სფერო** - ეკონომიკური/სამეწარმეო ან პროფესიული/სამსახურებრივი საქმიანობის ფარგლებში მონაცემთა დამუშავება არ მიიჩნევა პირადი მიზნით დეტერმინირებულ მონაცემთა დამუშავების შემთხვევად.

6. დასკვნა

ინფორმაციული ტექნოლოგიების განვითარებამ უამრავ შესაძლებლობასთან ერთად წარმოშვა რისკები, რომლებიც განსაკუთრებით პირადი ავტონომიის, პირადი ცხოვრების უფლების ეფექტიანად სარგებლობის რეალიზების ხელშეშლას მიემართება. ინტერნეტსივრცეში მონაცემთა დამუშავება სულ უფრო მეტად ფართო მასშტაბს იღებს. სოციალური ქსელის მომხმარებლები ხშირად აზიარებენ საკუთარ პერსონალურ მონაცემებს ფართო აუდიტორიის წინაშე და არ ფიქრობენ საფრთხეებზე, რომლებიც აღნიშნულ მონაცემთა სხვა პირების მიერ დამუშავებას შეიძლება მოჰყვეს. სოციალურ ქსელებში საკუთარი მონაცემების გაზიარება დღეს აქტუალურად ითვლება, თუმცა მომავლის პერსპექტივიდან შესაძლოა აღნიშნული უხერხულადაც კი მიიჩნეოდეს. „ინტერნეტსივრცეში რთული, მტკივნეული და ზოგჯერ შეუძლებელიც კია წაშალო საკუთარი პერსონალური მონაცემი“.[24]

პერსონალური მონაცემების გასაჯაროებისას მონაცემთა სუბიექტებს მართებთ მაქსიმალური სიფრთხილე, ვინაიდან მათი შემდგომი უნებართვო და არასასურველი დამუშავება, შესაძლოა იყოს „პერსონალურ მონაცემთა

[23]იხ.:<https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].

[24] იხ.: <https://www.facebook.com/photo/?fbid=1094114552832861&set=a.181886710722321> [14.9.2025].

დაცვის შესახებ“ კანონთან თავსებადი, ვინაიდან მონაცემთა დაცვის კანონმდებლობა დამუშავებისთვის პასუხისმგებელ პირს ანიჭებს უფლებას, დაამუშაოს პერსონალური მონაცემები, მაგალითად, იმ შემთხვევაში თუ მონაცემთა სუბიექტმა ისინი თავად გახადა საზოგადოებისთვის ხელმისაწვდომი.

პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები არ არის აბსოლუტური ხასიათის და ამ უფლებათა შეზღუდვა შესაძლებელია, მაგალითად, კანონის საფუძველზე ან სხვათა უფლებების დასაცავად. დემოკრატიული საზოგადოების არსებობის პირობებში ადამიანის უფლებათა კონკურენტულიხასიათიდან გამომდინარე, აუცილებელია სამართლიანი ბალანსის დაცვა უფლებათა შორის და ერთი სუბიექტის ინტერესის დაცვა მეორე პირის ინტერესის ხელყოფის ხარჯზე გაუმართლებელია. შეიძლება ითქვას, რომ პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოქმედების ფარგლების შეზღუდვა ფიზიკური პირის მიერ აშკარად პირადი ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავების შემთხვევებზე გამომდინარეობს სწორედ სხვა უფლებათა მიმართ სამართლიანი ბალანსის დაცვის უზრუნველყოფის მიზნიდან. კანონმდებელმა პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებად არ მიიჩნია სამეწარმეო ან/და ეკონომიკური, პროფესიული საქმიანობიდან ან სამსახურებრივი მოვალეობის შესრულებიდან გამომდინარე მონაცემთა დამუშავება. ასევე, ფიზიკური პირის საქმიანობის სფეროს მიუხედავად, მონაცემთა დაცვის ეროვნული თუ საერთაშორისო პრაქტიკა ადასტურებს, რომ სოციალურ ქსელებში დამუშავებისთვის პასუხისმგებელი ფიზიკური პირის მიერ სხვა პირთა პერსონალური მონაცემების გასაჯაროება არ მიიჩნევა აშკარა პირადი მიზნით მონაცემთა დამუშავებად და მისი კანონიერება პერსონალურ მონაცემთა დაცვის კანონმდებლობის შესაბამისად უნდა შეფასდეს. მნიშვნელოვანია აღინიშნოს, რომ ფიზიკური პირის მიერ სოციალურ ქსელებში მონაცემთა სუბიექტის პერსონალური მონაცემების გამჟღავნების გზით დამუშავება, მიუხედავად იმისა, რომ ხშირ შემთხვევაში ექცევა პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოქმედების სფეროში, იმთავითვე არ გულისხმობს ქმედების უკანონობას, ვინაიდან შესაძლოა სახეზე იყოს მონაცემთა დამუშავების „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული სამართლებრივი საფუძვლები.

ბიბლიოგრაფია:

1. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023.
2. „საქართველოს სამოქალაქო კოდექსი“, 786, 26/06/1997.
3. „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-Xმპ, 02/08/2021.
4. საქართველოს კანონი „საქართველოს საგადასახადო კოდექსი“, 3591, 17/19/2010.
5. „საჯარო რეესტრის შესახებ“ საქართველოს კანონი, 820, 19/12/2008.
6. სამოქალაქო კოდექსის კომენტარი, წიგნი I, სამოქალაქო კოდექსის ზოგადი დებულებები, თბილისი, 2017, 112.
7. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 23 სექტემბრის №გ-1/355/2025 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
8. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 1 აგვისტოს №გ-1/269/2025 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
9. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 23 ივლისის №გ-1/259/2025 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
10. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 3 ივნისის №გ-1/183/2025 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
11. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2025 წლის 3 აპრილის №გ-1/107/2025 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
12. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მოვალეობის შემსრულებლის, სამსახურის უფროსის პირველი მოადგილის 2024 წლის 19 დეკემბრის №გ-1/374/2024 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
13. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 24 ოქტომბრის №გ-1/307/2024 გადაწყვეტილება (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
14. პერსონალურ მონაცემთა დაცვის სამსახურის საჯარო ინფორმაციის ხელმისაწვდომობის უზრუნველყოფაზე პასუხისმგებელი პირის 2025 წლის 17 სექტემბრის №PDPS 3 25 00015900 კორესპონდენცია (სამსახურიდან გამოთხოვილია საჯარო ინფორმაციის სახით).
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.

16. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995.
17. *Case of Toth and Crișan v. Romania*, [2025] ECHR, App. No. 45430/19.
18. Persónuvernd (Iceland) - no. 2020010552 [17.11.2021] (<https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_no._2020010552> [30.8.2025]).
19. <https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].
20. <https://www.facebook.com/photo/?fbid=1094114552832861&set=a.181886710722321> [14.9.2025].
21. <https://shorturl.at/pKZlH> [14.9.2025].

© პერსონალურ მონაცემთა დაცვის სამსახური, 2025

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის №7, 0105
ბათუმი, ბაქოს ქუჩა, №48, 6010
www.pdps.ge
ტელ.: (+995 32) 242 1000
E-mail: office@pdps.ge