

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 ანალიზებს 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 ასრულებს: აღმოჩენის, დადასტურების, იდენტიფიკაციის და ანალიზის.² აღმოჩენის ფუნქციის მიზანია დაადგინოს, რომ გამოსახულებაში

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

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

² იქვე, 4-5.

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 საზედამნებლო 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 გამოყენება განსაკუთრებულად საყურადღებოა, რადგან საპოლიციო დაწესებულებები სახის ამომცნობ ტექნოლოგიებს იყენებენ ეჭვმიტანილების იდენტიფიცირებისთვის, რომლებიც უარს აცხადებენ მათთან თანამშრომლობაზე, აგრეთვე, დამნაშავეთა ფოტოსურათების მონაცემთა

³ იქვე, 5-6.

⁴ იქვე, 7-10.

⁵ იქვე, 8.

⁶ იქვე, 11-12.

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 ამომცნობის 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 არა დადასტურებული ფაქტები.¹² ტრენინგის მონაცემების ხარისხი ფუნდამენტურად განსაზღვრავს ალგორითმის მუშაობას; არაწარმომადგენლობით მონაცემთა ბაზებზე დაყრდნობით გაწვრთნილი

⁷ იქვე, 13-14.

⁸ იქვე, 12.

⁹ იქვე, 14-15.

¹⁰ იქვე, 15.

¹¹ იქვე, 16.

¹² იქვე, 18-19.

სახის ამომცნობი სისტემები სხვადასხვა დემოგრაფიულ ჯგუფთან მიმართებით ამომცნობის 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. მოგვიანებით აღნიშნული სისტემა არასანდოდ იქნა მიჩნეული.¹⁸

¹³ იქვე, 16-17.

¹⁴ იქვე, 17-18.

¹⁵ იქვე, 21.

¹⁶ იქვე, 22.

¹⁷ იქვე, 23.

¹⁸ იქვე, 24.

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 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

¹⁹ იქვე, 25-27.

²⁰ იქვე, 28.

²¹ იქვე, 28-29.

²² იქვე, 30.

²³ იქვე, 30.

²⁴ იქვე, 30-31.

დაცვის საზედამხებდველო ორგანოებთან. სახის ამომცნობა საზოგადოებრივ ადგილებში უნდა ემსახუროდეს 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 ამომცნობის 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 გამოყენებულ იქნეს მონაცემთა მინიმუზაციის 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

²⁵ იქვე, 32.

²⁶ იქვე, 32.

²⁷ იქვე, 32-33.

²⁸ იქვე, 33.

²⁹ იქვე, 34.

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 ჯგუფის 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 მიაჩნია, 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.

³⁰ იქვე, 35.