პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

თებერვალი / 2024

მთავარი სიახლეები

სააღსრულებო წარმოების პროცესში მონაცემთა ბაზების რეალიზაციის თაობაზე ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”) გენერალური ადვოკატის მოსაზრება გამოქვეყნდა

ევროპარლამენტმა „პოლიტიკური რეკლამის გამჭვირვალობისა და მიზნობრივი დანიშნულების შესახებ“ რეზოლუცია მიიღო

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) „საპოლიციო დირექტივის“ ფარგლებში პერსონალურ მონაცემთა შენახვის საკითხებზე იმსჯელა

ევროპარლამენტი შეშფოთებას გამოხატავს სათვალთვალო პროგრამების აღმოჩენის შესახებ

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) „საპოლიციო დირექტივის“[1] ფარგლებში პერსონალურ მონაცემთა შენახვის საკითხებზე იმსჯელა

30.01.2024

ფოტო: european-union.europa.eu

2024 წლის 30 იანვარს, ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) მიიღო გადაწყვეტილება საპოლიციო დირექტივის (“LED”) შესაბამისად[2] მსჯავრდებულთა პერსონალური მონაცემების შენახვის შესახებ.

ფაქტობრივი გარემოებების თანახმად, პირი სასჯელის მოხდის შემდეგ ითხოვდა პოლიციაში არსებული დოკუმენტაციიდან მისი მონაცემების წაშლას. კომპეტენტურმა უწყებამ წაშლაზე უარი განაცხადა იმ მოტივით, რომ ეროვნული კანონმდებლობით სასჯელის მოხდა არ წარმოადგენდა მონაცემთა წაშლის საფუძველს. აღსანიშნავია, რომ ეროვნულ დონეზე საქმეს განიხილავდა ბულგარეთის ადმინისტრაციული სასამართლო, რომელმაც “CJEU”-ს მიმართა შემდეგი კითხვით:

? საპოლიციო დირექტივის მე-5 („შენახვის ვადები და გადასინჯვა“) და მე-13 (2)(b)(3) („ინფორმაცია, რომელიც ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტისათვის ან უნდა გადაეცეს მონაცემთა სუბიექტს“) მუხლების გათვალისწინებით, რამდენად დასაშვებია, რომ ეროვნული კანონმდებლობით უზრუნველყოფილი იქნეს კომპეტენტური ორგანოების შეუზღუდავი უფლებამოსილება, დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნებისთვის, პერსონალური მონაცემების დამუშავებასთან მიმართებით.

[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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[2] Judgment of the Court (Grand Chamber), In Case C-118/22, 30 January 2024, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=282264&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1207402, [7.3.2024].

ზემოაღნიშნულ კითხვებზე დაყრდნობით, ევროკავშირის მართლმსაჯულების სასამართლომ იმსჯელა „სამართლებრივი რეაბილიტაციის“ (“Legal Rehabilitation”) პროცესში, განუსაზღვრელი ვადით პერსონალურ მონაცემთა დამუშავების მართლზომიერების შესახებ.

☑ სასამართლომ ხაზგასმით აღნიშნა მონაცემთა მინიმიზაციისა და პროპორციულობის პრინციპების დაცვის მნიშვნელობა. კერძოდ, მონაცემები უნდა ინახებოდეს განსაზღვრული ვადით, რაც აუცილებელია ლეგიტიმური მიზნის მისაღწევად. ამასთან, მნიშვნელოვანია, პერსონალურ მონაცემთა შენახვის საჭიროება გადაისინჯოს პერიოდულად. პერსონალურ მონაცემთა დამუშავების ფარგლებსა და გამოყენების შეზღუდვასთან დაკავშირებით აუცილებელია წევრი სახელმწიფოების მიერ შესაბამისი წესების შემუშავება, რათა დაცული იქნას ინდივიდთა ძირითადი უფლებები.

გარდა ზემოაღნიშნულისა, ევროკავშირის მართლმსაჯულების სასამართლომ განიხილა „საპოლიციო დირექტივის“ დებულებები, რომლებიც შეეხება განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებას, მაგალითად, როგორიცაა ბიომეტრიული და გენეტიკური მონაცემები. შესაბამისად, უნდა არსებობდეს მონაცემთა დამუშავების აუცილებლობა და მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების გაძლიერებული დაცვის საჭიროება. ამასთან, თუ პერსონალურ მონაცემთა დამუშავებით ირღვევა ევროკავშირის მონაცემთა დაცვის სტანდარტები, აუცილებელია მათი დაუყოვნებლივ წაშლა.

აღნიშნული გადაწყვეტილება ნათლად წარმოაჩენს პერსონალურ მონაცემთა დამუშავების პრინციპებისა და ინდივიდთა პირადი ცხოვრების ხელშეუხებლობის დაცვის მნიშვნელობას. იგი ქმნის ერთგვარ პრეცედენტს წევრი სახელმწიფოებისთვის, რათა მონაცემთა შენახვა განხორციელდეს ევროკავშირის კანონმდებლობით დადგენილი სტანდარტების შესაბამისად. ამასთან დაკავშირებით აღსანიშნავია პროპორციულობისა და მონაცემთა მინიმიზაციის პრინციპები და, ასევე, მონაცემთა წაშლის უფლება. აღნიშნული საქმე აძლიერებს ევროკავშირის ვალდებულებას, რომ სისხლისსამართლებრივ სფეროში პერსონალური მონაცემების დამუშავებისას დაცული იქნას

პერსონალური მონაცემები და ძირითადი უფლებები.[3]

სააღსრულებო წარმოების პროცესში მონაცემთა ბაზების რეალიზაციის თაობაზე ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”) გენერალური ადვოკატის მოსაზრება გამოქვეყნდა

22.02.2024

ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”) გენერალური ადვოკატის, პრიიტ პიკამაეს მოსაზრებით, სააღსრულებო წარმოების პროცესში შესაძლებელია, პერსონალური მონაცემების შემცველი ბაზა, გარკვეული ფაქტობრივი გარემოებების გათვალისწინებით, გასხვისდეს, იმ შემთხვევაშიც კი, თუ აღნიშნულზე მონაცემთა სუბიექტებს არ აქვთ გაცხადებული თანხმობა.[4]

საქმის ფაქტობრივი გარემოებების მიხედვით[5], პოლონეთის სასამართლო განიხილავდა კრედიტორ კომპანიასა და მოვალე კომპანიის დირექტორთა საბჭოს წევრს შორის დავას. აღსანიშნავია, რომ ორივე კომპანია ონლაინ გაყიდვების სფეროში საქმიანობდა და კრედიტორ კომპანიას წარმოეშვა დავალიანებასთან დაკავშირებული რიგი მოთხოვნები.

საგულისხმოა, რომ კრედიტორი კომპანიის მოთხოვნათა დაკმაყოფილების მიზნით, შესაძლებელია, მოვალე კომპანიის დირექტორთა საბჭოს წევრი გახდეს პირადად და უშუალოდ პასუხისმგებელი, თუკი არ იარსებებს კრედიტორული მოთხოვნის დაკმაყოფილებისთვის შესაბამისი აქტივი. დირექტორთა საბჭოს წევრის მოსაზრებით, მოვალე კომპანიას, სხვა ქონებასთან ერთად, გააჩნდა მის მიერ შექმნილი ონლაინ პლატფორმის მომხმარებლების ორი მონაცემთა ბაზა, რომელიც, მოცემულ შემთხვევაში, წარმოადგენდა კომპანიის აქტივს და შესაძლოა, დათმობოდა კრედიტორული მოთხოვნის დაკმაყოფილებას. საგულისხმოა, რომ მონაცემთა ბაზები შეიცავდა ასობით ათასი მომხმარებლის პერსონალურ მონაცემებს, რომელთა პლატფორმის მიღმა მესამე მხარისთვის გადაცემაზე თანხმობა მონაცემთა სუბიექტებს არ გაუციათ.

პოლონეთის სასამართლომ კითხვით მიმართა ევროკავშირის

[3] GDPRbuzz, CJEU rules on data storage under Law Enforcement Directive, <https://gdprbuzz.com/news/cjeu-rules-on-data-storage-under-law-enforcement-directive/>, [7.03.2024].

[4] იხ. ელექტრონული ბმული: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-02/cp240035en.pdf>.

[5] Case C-693/22: Request for a preliminary ruling from the Sąd Rejonowy dla m.st. Warszawy w Warszawie (Poland) lodged on 10 November 2022 — I. sp. z o.o. v M.W., OJ C 35, 30.1.2023, p. 36–36.

მართლმსაჯულების სასამართლოს (“CJEU”) იმის დასადგენად, სამოქალაქოსამართლებრივი მოთხოვნების აღსრულების მიზნით, მონაცემთა სუბიექტების თანხმობის გარეშე მონაცემთა ბაზების რეალიზაცია შეესაბამებოდა თუ არა ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციას“ (“GDPR”)?

ფოტო: en.wikipedia.org

ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”) გენერალური ადვოკატის, პრიიტ პიკამაეს მოსაზრებით, აღმასრულებლის მიერ აღნიშნული მონაცემთა ბაზების ღირებულების შეფასება და მათი საჯარო აუქციონის წესით რეალიზაცია შეესაბამება “GDPR”-ის მოთხოვნებს. აღმასრულებლის მიერ განსახორციელებელი ოპერაციები გულისხმობს, სულ მცირე, პერსონალური მონაცემების მოძიებას, კონსულტაციის გაწევას, გამოყენებასა და მყიდველისთვის ხელმისაწვდომობას, ამდენად, “GDPR”-ის მნიშვნელობით წარმოადგენს მონაცემთა „დამუშავებას“. გარდა ამისა, გენერალურმა ადვოკატმა აღნიშნა, რომ აღმასრულებელი მონაცემთა დამუშავებისთვის პასუხისმგებელ პირად უნდა მიჩნეულიყო. ამასთანავე, მისი მოსაზრებით, ამგვარი დამუშავება იყო კანონიერი, ვინაიდან იგი წარმოადგენდა აუცილებლობას აღმასრულებელი ორგანოს მიერ სამსახურებრივი უფლებამოსილების ფარგლებში განსახორციელებელი დავალების შესასრულებლად.

ფოტო: freepik.com

გენერალურმა ადვოკატმა, ასევე, აღნიშნა, რომ აღმასრულებლის მიერ განხორციელებული დამუშავების მიზანი განსხვავდებოდა ონლაინ გაყიდვების პლატფორმის გამოყენების საწყისი მიზნისაგან. “GDPR”-თან თავსებადობის უზრუნველსაყოფად, ყოველი შემდგომი დამუშავება უნდა იყოს „აუცილებელი“ და „პროპორციული ღონისძიება“ დემოკრატიულ საზოგადოებაში, რადგან მიღწეულ იქნას ევროკავშირის რეგულაციით გათვალისწინებული ერთ-ერთი საჯარო ინტერესი. გენერალური ადვოკატის განმარტებით, სამოქალაქოსამართლებრივი მოთხოვნების აღსრულების მიზნით,

შესაძლებელია, გამართლებული ყოფილიყო მონაცემების ამგვარი დამუშავება. მან ასევე აღნიშნა, რომ სასამართლოს უნდა შეეფასებინა ღონისძიების „პროპორციულობა“, რაც გულისხმობს კრედიტორი კომპანიის საკუთრების უფლებასა და შესაბამისი ონლაინ პლატფორმის მომხმარებლების პერსონალური მონაცემების დაცვის უფლებას შორის ბალანსის მიღწევას.[6]

საგულისხმოა, რომ აღნიშნული საქმე განხილვის პროცესშია, ხოლო გენერალური ადვოკატის მოსაზრება ევროკავშირის მართლმსაჯულების სასამართლოს არ არის სავალდებულო ძალის მქონე.

[6] იხ. ელექტრონული ბმული: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-02/cp240035en.pdf>.

ევროპარლამენტმა „პოლიტიკური რეკლამის გამჭვირვალობისა და მიზნობრივი დანიშნულების შესახებ“ რეზოლუცია მიიღო

27.02.2024

ფოტო: euobserver.com

2024 წლის 27 თებერვალს ევროპარლამენტმა მიიღო რეზოლუცია[7] „პოლიტიკური რეკლამის გამჭვირვალობისა და მიზნობრივი დანიშნულების შესახებ“[8]. რეზოლუციის მიხედვით, პოლიტიკურ რეკლამას უნდა ჰქონდეს მკაფიო მითითება: შესაბამისი კატეგორიის, სამიზნე აუდიტორიის, დამფინანსებლების — პოლიტიკური ან სხვა სუბიექტების, დაფინანსების ოდენობის და არჩევნების თარიღის შესახებ.

რეზოლუციის მიზანია განისაზღვროს მკაფიო და კონკრეტული წესები ევროკავშირის მასშტაბით პოლიტიკური რეკლამის

[7] <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0090_EN.pdf

[8] https://www.dataguidance.com/news/eu-european-parliament-adopts-resolution-transparency

გავრცელებისთვის, რათა ჩამოყალიბდეს ფორმალური და შინაარსობრივი მოთხოვნები ონლაინ სარეკლამო პროდუქტის შექმნისა და საჯარო გავრცელებისთვის. აღნიშნული მიზნის შესაბამისად, ევროკავშირის ფარგლებს მიღმა დაფინანსებული პოლიტიკური რეკლამების გავრცელება იკრძალება არჩევნების ჩატარებამდე ან რეფერენდუმამდე სამი თვით ადრე.

რეზოლუცია ითვალისწინებს პერსონალური მონაცემების დამუშავებაზე დაფუძნებული პოლიტიკური რეკლამის გამოყენებას, თუმცა მიუთითებს საფრთხეზე, რომელიც უკავშირდება გამოხატვის თავისუფლების, პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის საკითხებს. ამიტომ, ახალი წესები ორიენტირებულია მხოლოდ პოლიტიკური რეკლამის რეგულირების საკითხზე, რათა შესაბამისი რეკლამის განთავსებისას მინიმუმამდე იქნას დაყვანილი დისკრიმინაციის, გამოხატვის თავისუფლების შეზღუდვის, პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევისა და პერსონალური მონაცემების უკანონო დამუშავებასთან დაკავშირებული რისკები.

რეზოლუციაში ხაზგასმულია, რომ იკრძალება იმგვარი მიზნობრივი პოლიტიკური რეკლამის გამოყენება, რომელიც ითვალისწინებს განსაკუთრებული კატეგორიის პერსონალური მონაცემების პროფაილინგს. ასევე, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა არ უნდა გამოიყენონ მესამე მხარისგან მიღებული პერსონალური მონაცემები მიზანმიმართული პოლიტიკური რეკლამისთვის.

რეზოლუციასთან დაკავშირებით აღინიშნა, რომ დემოკრატიულ საზოგადოებაში არჩევნების მნიშვნელობისა და მასთან დაკავშირებული რისკების დაზღვევისთვის, განსაკუთრებული როლი ენიჭება ციფრული ტექნოლოგიების განვითარებას, უტყუარი და უსაფრთხო ინფორმაციის გავრცელებას საარჩევნო პერიოდში დეზინფორმაციისა და უცხოური ჩარევის წინააღმდეგ. მიღებული წესები მოქალაქეებს დაეხმარებათ ინფორმირებული გადაწყვეტილების მიღებაში. შესაბამისად, არჩევნების მოახლოებასთან ერთად, ყველა ძირითადი ონლაინ პლატფორმა მიზნად უნდა ისახავდეს, გამჭირვალე პოლიტიკური იდეებისა და აზრების გაცვლისთვის ციფრული სივცრის უსაფრთხოების უზრუნველყოფას.

ევროპარლამენტი შეშფოთებას გამოხატავს სათვალთვალო პროგრამების აღმოჩენის შესახებ

28.02.2024

ფოტო: euractiv.com

ევროპარლამენტმა განსაკუთრებული ყურადღება მიაქცია კიბერუსაფრთხოების ღონისძიებებს მას შემდეგ, რაც თავდაცვის ქვეკომიტეტის ორი წევრის მობილურ ტელეფონში სათვალთვალო პროგრამა იქნა აღმოჩენილი.[9] უსაფრთხოებისა და თავდაცვის ქვეკომიტეტის (“SEDE”) ყველა წევრს მოუწოდეს, საკუთარი მოწყობილობები შესამოწმებლად წარედგინათ პარლამენტის ინფორმაციული ტექნოლოგიების სამსახურისთვის. ქვეკომიტეტის წევრების მობილური ტელეფონების შემოწმებისას სათვალთვალო პროგრამები პარლამენტის პრესსპიკერის მოადგილის მობილურ მოწყობილობაზეც იქნა აღმოჩენილი.

აღნიშნულის საპასუხოდ, ევროპის პარლამენტმა 2022 წელს დააარსა სპეციალური საგამოძიებო კომიტეტი. ამავე მიზნით, პარლამენტის IT სამსახურმა პრევენციული მექანიზმების განხორციელება გასული წლის აპრილიდან დაიწყო. ინიციატივა მოიცავდა წევრების ტელეფონების შემოწმებას (სკანირებას) სათვალთვალო პროგრამების იდენტიფიცირების მიზნით. აღსანიშნავია, რომ დღეის მდგომარეობით უკვე ასობით ოპერაცია წარმატებით იქნა განხორციელებული.

[9] https://gdprbuzz.com/news/eu-parliament-cybersecurity-concerns-amid-spyware-discovery/

„მონაცემთა დაცვის ევროპულმა საბჭომ“ (“EDPB”) მონაცემთა დამუშავების უსაფრთხოებისა და ინციდენტის შეტყობინების ვალდებულების შესახებ სახელმძღვანელო დოკუმენტი გამოსცა

6.02.2024

ფოტო: edpb.europa.eu

„მონაცემთა დაცვის ევროპულმა საბჭომ“ (“EDPB”) სახელმძღვანელო დოკუმენტი გამოაქვეყნა[10], რომელიც შეეხება მონაცემთა დამუშავების

[10] <https://gdprbuzz.com/news/edpb-releases-new-gdpr-security-and-breach-notification-guide>

უსაფრთხოებასა (GDPR-ის 32-ე მუხლი) და მონაცემთა უსაფრთხოების დარღვევის შეტყობინების ვალდებულებას (GDPR-ის 33-ე და 34-ე მუხლები). ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ ამოქმედების შემდეგ, მონაცემთა დაცვის საზედამხედველო ორგანოები ევროპის მასშტაბით თანამშრომლობენ მონაცემთა უსაფრთხოებისა და დარღვევების შესახებ გადაწყვეტილებების მიღების მიზნით.

სახელმძღვანელოში განხილულია GDPR-ის დებულებები, ასევე, სახელმწიფო ორგანოების განმარტებები ისეთ საკითხებზე, როგორიცაა: კიბერთავდასხმა, იმგვარი საზიანო პროგრამული უზრუნველყოფის გამოყენებით, რომელიც შექმნილია კომპიუტერულ სისტემაზე წვდომის დაბლოკვის მიზნით, ვიდრე გამოსასყიდის გადახდა არ განხორციელდება (“Ransomware Attack”); აგრეთვე, მონაცემთა გაუთვალისწინებელი გამჟღავნება და ა. შ.

სახელმძღვანელო დოკუმენტი უსაფრთხოების ინციდენტების სიღრმისეული შესწავლის შედეგია. მისი მიზანია, დაეხმაროს მონაცემთა დაცვის საზედამხედველო ორგანოებს სხვადასხვა სიტუაციებთან გამკლავებაში. ინფორმაცია, ასევე, სასარგებლოა ორგანიზაციებისთვის, მათ შორის, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის, დამუშავებაზე უფლებამოსილი პირებისთვის, რათა შეაფასონ უსაფრთხოების ზომების ეფექტიანობა.

GDPR-ის 33-ე და 34-ე მუხლებთან დაკავშირებით, გადაწყვეტილებები, უპირველეს ყოვლისა, ორიენტირებულია წამყვანი საზედამხედველო ორგანოების მიერ ჩატარებულ შეფასებაზე - შეესაბამება თუ არა საზედამხედველო ორგანოს პერსონალური მონაცემების დარღვევის შესახებ შეტყობინება და მონაცემთა სუბიექტების უფლებების დარღვევის შესახებ შეტყობინება GDPR-ის 33-ე და 34-ე მუხლებით განსაზღვრულ ვალდებულებას. აღსანიშნავია, რომ საზედამხედველო ორგანოსთვის შეტყობინების ვალდებულება არ წარმოიშობა, როდესაც პერსონალური მონაცემების დარღვევა ნაკლებად სავარაუდოა, რომ გამოიწვევს ფიზიკური პირების უფლებებისა და თავისუფლებების შელახვის საფრთხეს. სახელმძღვანელოში განხილული საქმეების ანალიზის საფუძველზე დგინდება, რომ პრაქტიკაში მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები, უმეტეს შემთხვევაში, აფრთხილებენ მონაცემთა დარღვევის შესახებ მონაცემთა დაცვის ორგანოებს.

ფოტო: edpb.europa.eu

ასევე, აღსანიშნავია, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ დამოუკიდებლად უზრუნველყონ ინციდენტის შეტყობინება, მაშინაც კი, თუ მათ მიაჩნიათ, რომ აღნიშნული შეიძლება, მონაცემთა უსაფრთხოების სხვა დარღვევას უკავშირდებოდეს.

GDPR-ის 34-ე მუხლის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ვალდებულნი არიან, გაუმართლებელი შეფერხების გარეშე შეატყობინონ მონაცემთა სუბიექტს მონაცემთა უსაფრთხოების დარღვევის შესახებ, თუმცა მხოლოდ მაშინ, როდესაც დარღვევამ შესაძლოა, გამოიწვიოს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების მაღალი რისკი. ხაზგასასმელია, რომ მხოლოდ ერთ შემთხვევაში, ჩაატარა საზედამხედველო ორგანომ პერსონალური მონაცემების დარღვევით გამოწვეული კონკრეტული რისკის შეფასება მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების მიმართ.

სახელმძღვანელო დოკუმენტის სრულად გაცნობა შესაძლებელი „მონაცემთა დაცვის ევროპული საბჭოს“ ვებგვერდზე[11].

სახის ამომცნობი კამერების საფუძველზე ფიზიკურ პირთა შესაძლო დისკრიმინაციის საფრთხე გაერთიანებულ სამეფოში

7.02.2024

ფოტო: gdprbuzz.com

ციფრულ ეპოქაში სახის ამოცნობის ტექნოლოგია მნიშვნელოვანი და აქტუალურია. „სამხრეთ კოოპერატივი“ გაერთიანებულ სამეფოში დაფუძნებული სუპერმარკეტების ქსელია, რომელმაც “Facewatch”-ის ფირმის სახის ამომცნობი კამერები უსაფრთხოების (შესაძლო ქურდობებისგან თავდაცვის მიზნით) 34 მაღაზიაში განათავსა.[12] მართალია, სუპერმარკეტების ფილიალები ქალაქის მდიდარ უბნებშიც მდებარეობს, თუმცა სახის ამოცნობის ტექნოლოგია, ძირითადად, ეკონომიკურად ღარიბი უბნების მიმდებარედ გამოიყენებოდა.

ფიზიკური პირის პირადი ცხოვრების ხელშეუხებლობის თემატიკაზე მომუშავე ექსპერტები გამოთქვამენ

[11] https://www.edpb.europa.eu/our-work-tools/our-documents/other/one-stop-shop-case-digest-security-processing-and-data-breach_en

[12] https://gdprbuzz.com/news/facial-recognition-cameras-in-uk-supermarkets-rise-concerns-of-discrimination/

შეშფოთებას და მიიჩნევენ, რომ ამ ტიპის მეთვალყურეობა მიემართება საზოგადოების მოწყვლად ჯგუფებს და ისეთ პირებს, ვინც სოციალურ-ეკონომიკური გამოწვევების წინაშე დგანან. აღნიშნული კი ზრდის დისკრიმინაციის საფრთხეს და იწვევს მათი პირადი ცხოვრების ხელშეუხებლობის უფლების ხელყოფას.

აღსანიშნავია, რომ სახის ამომცნობი ტექნოლოგიის გამოყენება სულ უფრო მზარდია კერძო სექტორშიც. ტექნოლოგიის დანერგვის მომხრენი მიიჩნევენ, რომ აღნიშნული ხელს უწყობს დანაშაულის აღკვეთას და დამნაშავეების იდენტიფიცირებას, თუმცა რეგულირებისა და გამჭვირვალობის სიმწირის გამო, ბევრი მოწინააღმდეგეც გამოჩნდა.

ფოტო: flaticon.com

მიუხედავად იმისა, რომ მნიშვნელოვნად შემცირდება დანაშაულის მაჩვენებელი იმ ადგილებში, სადაც განლაგებულია სახის ამომცნობი კამერები, ადამიანის უფლებათა დამცველი ჯგუფები საცალო მოვაჭრეებს მოუწოდებენ, ხელახლა განიხილონ ამგვარი ინვაზიური თვალთვალის მეთოდის გამოყენების აუცილებლობა.

გაერთიანებული სამეფოს მთავრობის პოზიციით, სახის ამომცნობ ტექნოლოგიას აქვს მყარი საკანონმდებლო საფუძველი და მნიშნელოვან როლს ასრულებს დანაშაულის გამოძიებასა და პრევენციაში, თუმცა კვლავ აქტიურად განიხილება, თუ რამდენად შესაბამისობაშია ტექნოლოგია პერსონალურ მონაცემთა დაცვასა და ადამიანის უფლებათა შესახებ საკანონმდებლო რეგულაციებთან.

(+ 995 32) 242 1000
office@pdps.ge
www.pdps.ge