



პერსონალური მონაცემების დამუშავების სტანდარტი დასაქმებულის სამუშაო სივრცის ვიდეომონიტორინგისას

სიმონი ტაკაშვილი

სულხან-საბა ორბელიანის უნივერსიტეტის
ასოცირებული პროფესორი, ადვოკატი

<https://orcid.org/0000-0001-8608-170X>

I. შესავალი

შრომითსამართლებრივ ურთიერთობებში დასაქმებულის პერსონალური მონაცემების დაცვა ძალიან მნიშვნელოვანი და ამავედროულად, პრობლემური საკითხია. საკითხის სირთულე გამომდინარეობს ამ სამართალურთიერთობის სპეციფიკიდან, რადგან დამსაქმებელს როგორც წინასახელშეკრულებო შრომითი ურთიერთობის დროს, ასევე შემდგომ პერიოდშიც დასაქმებულთან დაკავშირებით საკმაოდ მოცულობითი პერსონალური მონაცემების დამუშავება უწევს.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალმა კანონმა საკმაოდ დეტალურად მოაწესრიგა პერსონალურ მონაცემთა დამუშავების საფუძვლები და ზოგადი სტანდარტები, თუმცა კანონის არაერთი ნორმა ბუნდოვანი და პრაქტიკაში საკმაოდ რთულად განსახორციელებელია. ამდენად, კანონმა, მართალია, დეტალურად განსაზღვრა ვიდეო და აუდიომონიტორინგის განხორციელების წესი და საფუძვლები, თუმცა, რა თქმა უნდა, რჩება გაუგებრობები, რომლებიც კანონით დადგენილი წესის აღსრულებას თან ახლავს.

სტატიის მიზანია, გაანალიზოს ისეთი პერსონალური მონაცემების დამუშავების სპეციფიკა, რაც დასაქმებულის სამუშაო სივრცის ვიდეომონიტორინგს შეეხება. ამ მიზნით შედარებითსამართლებრივი მეთოდით გაანალიზებულია უახლესი საკანონდებლო მიდგომები, უცხოური ლიტერატურა და უცხოური სასამართლო პრაქტიკა. აღსანიშნავია, რომ ახალი კანონით დადგენილ მონესრიგებასა და მის პრობლემურ საკითხებზე ჯერჯერობით ქართული სასამართლო პრაქტიკა და პრინციპში, სამეცნიერო ნაშრომებიც არ არსებობს, თუმცა, ამ მხრივ, საორიენტაციოა ევროპული გამოცდილების გაცნობა და შემდეგ მისი ქართულ რეალობაში გადმოტანა.

ნაშრომში მოტანილია ადამიანის უფლებათა ევროპული სასამართლოს რამდენიმე გადაწყვეტილება, რომელიც დასაქმებულის ვიდეომონიტორინგის გზით პერსონალური მონაცემების დამუშავებას შეეხება. ეს გადაწყვეტილებები იმდენად მნიშვნელოვანია, რომ თითქმის ყველა თანამედროვე იურიდიულ ლიტერატურაშია მათზე საუბარი. შესაბამისად, ახალადამოქმედებული კანონის უკეთ გაგებასა და რაც მთავარია, პრაქტიკაში დანერგვის მიზნით, უცხოური პრაქტიკისა და გამოცდილების გაცნობას უდიდესი მნიშვნელობა და დატვირთვა აქვს. დასკვნაში შეჯამდება კვლევის შედეგები და დაისახება გარკვეული რეკომენდაციები, რომელთა პრაქტიკაში გათვალისწინებაც სასურველია შრომით ურთიერთობებში პერსონალურ მონაცემთა დაცვის უკეთესი სამართლებრივი რეჟიმისათვის.

II. ზოგადად შრომით ურთიერთობაში პერსონალური მონაცემების დამუშავების შესახებ

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მიღება განპირობებული იყო საქართველოსა და ევროკავშირის შორის დადებული ასოცირების შესახებ შეთანხმებით, რომლის მე-14 მუხლის თანახმადაც, მხარეები თანხმდებიან, რომ ითანამშრომლე-

ბენ, რათა უზრუნველყონ პერსონალურ მონაცემთა მაღალ დონეზე დაცვა შეთანხმების დანართში მითითებული ევროკავშირის, ევროპის საბჭოსა და საერთაშორისო სამართლებრივი დოკუმენტებისა და სტანდარტების შესაბამისად. შესაბამისად, საქართველომ პერსონალური მონაცემების დაცვის სფეროში საორიენტაციოდ აიღო ევროკავშირში დადგენილი სტანდარტები. რა თქმა უნდა ეს სტანდარტები შეეხო უშუალოდ შრომით ურთიერთობებში არსებულ პერსონალურ მონაცემებსა და მათ დაცვას.

ევროკავშირში დასაქმებულის პერსონალური მონაცემების დაცვა ერთ-ერთი მნიშვნელოვანი საკითხია. აღნიშნულს საფუძვლად უდევს რეგულაცია, რომელიც GDPR-ის სახელითაა ცნობილი და რომელიც ევროკავშირის მასშტაბით ძალაში შევიდა 2018 წლის 25 მაისს.¹ აღსანიშნავია, რომ ერთ-ერთი პირველი სახელმწიფო, რომელმაც შრომით ურთიერთობებში GDPR-ით დადგენილი სტანდარტები კანონმდებლობაში ასახა, იყო გერმანია,² მან პირველმა დაიწყო პერსონალური მონაცემების შესახებ თავისი კანონმდებლობის მორგება GDPR-ით დადგენილ სტანდარტებთან.³ ეს პროცესი, რა თქმა უნდა, შეეხო დასაქმებულის, როგორც მონაცემთა სუბიექტის, უფლებების დაცვას, რადგან პერსონალური მონაცემების დამუშავების ერთ-ერთი მნიშვნელოვანი სფერო შრომითი ურთიერთობებია, სადაც სოციალური ურთიერთობისა და ციფრული ტექნოლოგიების ბოლოდროინდელმა უპრეცედენტო განვითარებამ

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) [2016] OJ L 119.

² Eecke V. P., Šimkus A., Article 88. Processing in the Context of Employment, in: *The EU General Data Protection Regulation (GDPR), A Commentary*, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020, 1231.

³ Federal Data Protection Act (BDSG) of the Federal Republic of Germany, 2017, Section 26.

ვიდეომონიტორინგის ფართო გამოყენება გამოიწვია.⁴ ამ თვალსაზრისით, მნიშვნელოვანი საკითხია შრომით ურთიერთობაში დასაქმებულის სამუშაო სივრცის ვიდეომონიტორინგის გზით კონტროლი. ზოგადად, თანამედროვე ტექნოლოგიების განვითარების ფონზე, დასაქმებულის პერსონალური მონაცემების დაცვის უფლება შესაძლოა მრავალი საშუალებითა და ასპექტში დაირღვეს.⁵

სამუშაო ადგილისა და სამუშაო პროცესის მონიტორინგი დამსაქმებლის უფლებაა, რათა მან გააკონტროლოს განხორციელებული სამუშაოს ხარისხი, რაც, საბოლოო ჯამში, დამსაქმებელი კომპანიის წარმატებას განაპირობებს.⁶ დამსაქმებლის ეს უფლება შრომის სამართალში სუბორდინაციული დამოკიდებულებითაცაა განპირობებული.⁷ ამდენად, შრომით ურთიერთობებში პერსონალური მონაცემების, განსაკუთრებით კი, აუდიო და ვიდეომონიტორინგის საშუალებით დამუშავება, ერთ-ერთი საკვანძო და პრობლემური საკითხია.

ქართულ რეალობაში პერსონალური მონაცემების დაცვა არა მხოლოდ ეროვნული საკანონმდებლო ნორმებით, არამედ არაერთი საერთაშორისო აქტით ხდება. ევროკონვენციის მე-8 მუხლი სწორედ პირადი ცხოვრების ხელშეუხებლობასა და დაცულობას განამტკიცებს, რაც, თავის მხრივ, პირის პერსონალური მონაცემების დაცვის ძირითადი და ზოგადი დაცვის საშუალებაა. როდესაც დასაქმებულის მონიტორინგი ხდება, ეს სწორედ პირად ცხოვრებაში ჩარევად და პერსონალური მონაცემების დამუშავებად მიიჩნევა⁸, რაც შესაძ-

⁴ Tiainen M.K., Solving the Surveillance Problem, Media Debates about Unwanted Surveillance in Finland, in: Privacy, Data Protection and Cybersecurity in Europe, Edited by W.J. Schunemann, M. Baumann, Springer, 2017, 61.

⁵ Rycak A., New Technologies and the Employee's Right to Privacy, in: Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 175.

⁶ იქვე, 176.

⁷ Lukacs A., Employees' Right to Privacy and Right to Data Protection on Social Network Sites, Szeged, 2021, 78.

⁸ Rycak A., New Technologies and the Employee's Right to Privacy, in: Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 176.

ლოა კანონიერი ან უკანონო იყოს. შესაბამისად, სამართლებრივი თვალსაზრისით, დასაქმებულის, მონაცემთა სუბიექტის პერსონალური მონაცემების, განსაკუთრებით ვიდეო და აუდიომონიტორინგის გზით, დამუშავება სპეციფიკური და ხშირ შემთხვევაში ცალკე საკანონმდებლო ნორმებით მონესრიგებული სფეროა.⁹ ამასთან, არის ქვეყნები, სადაც დასაქმებულის ვიდეომონიტორინგის შესახებ ცალკე დებულებები არაა და ის ზოგადი მონესრიგების ფარგლებში ექცევა (მაგალითად, გაერთიანებული სამეფო).¹⁰

III. ვიდეომონიტორინგის საშუალებით პერსონალური მონაცემების დამუშავება შრომით ურთიერთობაში

1. ვიდეომონიტორინგის ცნება და მიზანი

ვიდეომონიტორინგი დასაქმებულის პერსონალური ინფორმაციის დამუშავებისა და ზედამხედველობის განსაკუთრებული და უფლებაში უხეშად ჩარევის ერთ-ერთი ფორმაა.¹¹ ამავდროულად, ისიც უნდა აღინიშნოს, რომ შესასრულებელი სამუშაოს სპეციფიკის გათვალისწინებით, ზოგიერთ შემთხვევაში ვიდეომონიტორინგი დამსაქმებლის არათუ უფლება, არამედ ვალდებულებაცაა.¹² თანამედროვე ტექნოლოგიების გამოყენებით დამსაქმებლის მიერ დასაქმებული კონტროლი, შესაძლოა, გამართლდეს სხვადასხვა საფუძვლით, მაგალითად, დამსაქმებლის საკუთრების დაცვის, დამსაქმებელი კომპანიის კარგი რეპუტაციის შენარჩუნებით, კომპანიის კონფიდენციალური ინფორმაციის გამჟღავნების

⁹ შეად., Komukai T., *Data Protection in the Internet: Japanese National Report*, in: *Data Protection in the Internet*, Edited by D. M. Vicente, S. V. de Casimiro, Springer, 2020, 260.

¹⁰ Morris G., *Protection of Employees' Personal Information and Privacy in English Law*, in: *Protection of Employees' Personal Information and Privacy*, Edited by R. Blanpain, H. Nakakubo, T. Araki, Wolters Kluwer, 2014, 224.

¹¹ იქვე.

¹² Lukacs A., *Employees' Right to Privacy and Right to Data Protection on Social Network Sites*, Szeged, 2021, 79.

პრევენციით, დასაქმებულის უსაფრთხოების დაცვითა და სხვ.¹³ ამდენად, უნდა არსებობდეს ლეგიტიმური მიზანი, რაც ვიდეომონიტორინგს კანონიერად და გამართლებულად აქცევს, თუმცა ლეგიტიმური მიზანი და ინტერესი ხშირ შემთხვევაში ორაზროვანი და საკამათოა.¹⁴ ამასთან, დამსაქმებლის ლეგიტიმურმა ინტერესმა მხოლოდ მას შემდეგ შეიძლება გადანონოს სხვა ინტერესი, თუ იგი დასაქმებულის ანუ მონაცემთა სუბიექტის ფუნდამენტურ უფლებებსა და თავისუფლებებს არ არღვევს.¹⁵

ვიდეომონიტორინგის ცნება „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-3 მუხლის „დ“ ქვეპუნქტშია მოცემული, რომლის თანახმადაც, ვიდეომონიტორინგი არის საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ვიზუალური გამოსახულების მონაცემთა დამუშავება, კერძოდ, ვიდეოკონტროლი ან/და ვიდეოჩანერა (გარდა ფარული საგამოძიებო მოქმედებისა). ვიდეომონიტორინგი შესაძლოა რეალურ დროშიც მიმდინარეობდეს და ამ შემთხვევაში ის დასაქმებულის პერსონალურ უფლებებში უფრო მეტად უხეშ/მკაცრ ჩარევას ნიშნავს.¹⁶

„პერსონალური მონაცემების დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის პირველი პუნქტი ჩამოთვლის იმ შემთხვევებს, როდესაც შესაძლებელია ზოგადად ვიდეომონიტორინგი. მე-3 პუნქტის თანახმად კი, დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი დასაშვებია მხოლოდ გამონაკლის შემ-

¹³ Rycak A., *New Technologies and the Employee's Right to Privacy*, in: *Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes*, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 175.

¹⁴ Dehon E., Carey P., *Fair, Lawful and Transparent Processing*, in: *Data Protection, A Practical Guide to UK and EU Law*, 5th Ed., Edited by P. Carey, Oxford University Press, 2018, 57.

¹⁵ Krzysztofek M., *GDPR: General Data Protection in the European Union*, Wolters Kluwer, 2019, 108.

¹⁶ *Guidelines 3/2019 on Processing of Personal Data through Video Devices, Version for Public Consultation*, Adopted on 10 July 2019, 9.

თხვევაში, თუ ამ მუხლის პირველი პუნქტით განსაზღვრული მიზნების მიღწევა სხვა საშუალებით შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. ამდენად, კანონმდებლობა მხოლოდ გამონაკლის შემთხვევებში მიიჩნევს დასაშვებად ვიდეომონიტორინგს. მაგალითად, ერთ-ერთ საქმეში პერსონალური მონაცემთა დაცვის ინსპექტორმა ვიდეომონიტორინგის განხორციელება და შესაბამისად, პერსონალურ მონაცემთა დამუშავება უკანონოდ სცნო, რადგან როგორც დადგინდა, ვიდეომონიტორინგის თავდაპირველი მიზანი იყო კომპანიის მიერ განხორციელებული მომსახურების კონტროლი.¹⁷ ამდენად, ინსპექტორმა მიიჩნია, რომ მხოლოდ მომსახურების ხარისხის კონტროლი არ შეიძლებოდა ყოფილიყო ვიდეომონიტორინგის გზით დასაქმებულთა ქცევის განმკონტროლებელი. შესაბამისად, გასაზიარებელია იურიდიულ ლიტერატურაში გამოთქმული შეხედულება, რომ დასაქმებულის ვიდეომონიტორინგი დამსაქმებლის ლეგიტიმურ მიზანს უნდა ემსახურებოდეს და მისი საშუალებით პერსონალური მონაცემების დამუშავება სპეციფიკური მიზნის მიღწევის საშუალება უნდა იყოს.¹⁸ ამასთან, ვიდეომონიტორინგს შესაძლოა განგრძობითი ან ერთჯერადი სახე ჰქონდეს.¹⁹

გასაზიარებელია ლიტერატურაში გამოთქმული შეხედულება, რომლის თანახმადაც, ვიდეომონიტორინგის სისტემები, რომლებიც გამოიყენება შრომით ურთიერთობებში მონიტორინგისთვის, ისეთ ადგილებზე, როგორიცაა, შესასვლელი და გასასვლელი სანარმოს

¹⁷ პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის 12 იანვრის Nგ-1/007/2016 გადაწყვეტილება.

¹⁸ Lee S.-W., Protection of Employees' Personal Information and Privacy at a Crossroads in Korea, in: Protection of Employees' Personal Information and Privacy, Edited by R. Blanpain, H. Nakakubo, T. Araki, Wolters Kluwer, 2014, 150.

¹⁹ Rycak A., New Technologies and the Employee's Right to Privacy, in: Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 176.

შენობაში ან ადგილები, სადაც განთავსებულია სეიფები ან ელექტრომექანიკური აღჭურვილობები, შეესაბამება და ამართლებს დამსაქმებლის მიზანს, თუ კამერები ფოკუსირებულია ქონებაზე ან საქონელზე.²⁰ ერთ-ერთ საქმეში, რომელიც კანადური სარკინიგზო კომპანიის მიერ ვიდეომონიტორინგს შეეხებოდა, სასამართლომ არ დაადგინა დასაქმებულის პერსონალური მონაცემების დარღვევის ფაქტი, რადგან ვიდეომონიტორინგის გარდა სხვა საშუალება ვანდალიზმის, ქურდობისა და მსგავსი დანაშაულებების აღსაკვეთად უშედეგო და ფინანსურად ძალიან ძვირი იყო.²¹ ამგვარად, მიზნისა და საშუალების შეფასებით სასამართლომ იმ დასაქმებულთა პერსონალური მონაცემების დარღვევა, რომლებიც კამერის ხედვის არეალში ხვდებოდნენ, არ დაადგინა. ამავდროულად, ვიდეომონიტორინგისას ყველა შემთხვევაში, დაცული უნდა იყოს პრინციპი, რომლის მიხედვითაც, ვიდეომონიტორინგი უნდა იყოს ყველაზე ბოლო/უკანასკნელი საშუალება იმ მიზნის მისაღწევად, რასაც დამსაქმებელი ისახავს. მაგალითად, პორტუგალიის შრომის კოდექსის მიხედვით, დამსაქმებელმა ვიდეომონიტორინგი არ უნდა გამოიყენოს დასაქმებულის პროფესიული მოქმედების/ქცევის გასაკონტროლებლად.²² ამავდროულად, ვიდეომონიტორინგი გამართლებულია, თუ ის მიზნად ისახავს ადამიანების, ან საქონლის/ნივთების დაცვას და უსაფრთხოებას ან როდესაც ვიდეომონიტორინგი გამართლებულია საქმიანობის შესრულების ხასიათიდან გამომდინარე.²³

²⁰ Kourtis V., *Data Protection in the Internet: Greece*, in: *Data Protection in the Internet*, Edited by D. M. Vicente, S. V. de Casimiro, Springer, 2020, 223.

²¹ Davidov G., *A Purposive Approach to Labour Law*, Oxford University Press, 2016, 184-185.

²² Civil Code of the Republic of Portugal, 2009, Art. 20(1).

²³ დამატებით იხ., Sousa Pinheiro A., *Data Protection in the Internet: The Portuguese Case*, in: *Data Protection in the Internet*, Edited by D. M. Vicente, S. V. de Casimiro, Springer, 2020, 275-ე და შემდეგი გვერდები.

2. ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული გადაწყვეტილებები

ვიდეომონიტორინგის განხორციელების წინაპირობებსა და მიზნებზე ადამიანის უფლებათა ევროპული სასამართლოს რამდენიმე მნიშვნელოვანი და იურიდიულ ლიტერატურაში ხშირად ციტირებადი გადაწყვეტილება არსებობს. საგულისხმოა, რომ თითოეული ეს გადაწყვეტილება ხაზს უსვამს შრომითი ურთიერთობის სპეციფიკასა და ამ ურთიერთობაში დასაქმებულის, როგორც მონაცემთა სუბიექტის, უფლებების დაცვის ხარისხს, რადგანაც მიჩნეულია, რომ ადამიანის პირადი სივრცე არ არსებობს მისი პროფესიული საქმიანობის გარეშე.²⁴

Köpke v. Germany

ერთ-ერთი ცნობილი საქმე, რომელიც ადამიანის უფლებათა ევროპულ სასამართლოს განუხილავს ვიდეომონიტორინგთან, როგორც დასაქმებულის პერსონალური მონაცემების დამუშავებასთან, დაკავშირებით, არის **Köpke v. Germany**.²⁵ სასამართლოს უნდა განეხილა, თუ რამდენად მიიჩნეოდა დასაქმებულის პერსონალური მონაცემების დარღვევად ფარული ვიდეომონიტორინგი, რომლის მიზანიც დამსაქმებლის კუთვნილ მაღაზიაში შესაძლოა ქურდობის ფაქტების გამოვლენა იყო. მომჩივანი აცხადებდა, რომ ფარული ვიდეომონიტორინგისას მისი, როგორც დასაქმებულის (მოლარის), პერსონალური მონაცემების დამუშავების წესი დაირღვა. გერმანულმა სასამართლოების შეფასებით, დამსაქმებლის მიზანი, გამოველინა ქურდობის ფაქტები, ამართლებდა და-

²⁴ Rycak A., *New Technologies and the Employee's Right to Privacy*, in: *Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes*, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 173.

²⁵ Köpke v. Germany [ECtHR], App. no. 420/07, 5 October 2010.

საქმებულის/მონაცემთა სუბიექტის (ამ შემთხვევაში მომჩივნის) პერსონალური მონაცემების დამუშავების ამგვარ მეთოდს. საგულისხმოა, რომ ვიდეომონიტორინგი მხოლოდ განსაზღვრულ დროს (2 კვირა) და მხოლოდ განსაზღვრულ პერიმეტრზე (მხედველობის არეზე) მიმდინარეობდა. სწორედ ამიტომ ევროსასამართლომ არ დაადგინა ადამიანის უფლებათა ევროპული კონვენციის ნორმების დარღვევა და მომჩივანს უარი უთხრა საჩივრის დაკმაყოფილებაზე. ამგვარად, ევროსასამართლომ პერსონალური მონაცემების დამუშავების საკითხი მონიტორინგის მიზნიდან გამომდინარე შეაფასა და პირადი ცხოვრების უფლების დარღვევა არ დაადგინა.²⁶

López Ribalda and Others v. Spain

კიდევ ერთი ცნობილი გადაწყვეტილება, სადაც სასამართლომ ასევე შეაფასა ვიდეომონიტორინგის განხორციელების მართლზომიერება იყო *López Ribalda and Others v. Spain*.²⁷ ამ გადაწყვეტილებაში სასამართლომ პირიქით განმარტა, – თუ სუპერმარკეტის ასისტენტმა/დასაქმებულმა არ იცის, რომ მისი ვიდეომონიტორინგი ხდება, აღნიშნული მონაცემთა სუბიექტის პერსონალური მონაცემების დამუშავების ნესსა და პირად ცხოვრებას არღვევს.²⁸ ამ საქმის ფაქტობრივი გარემოებების მიხედვით, დამსაქმებელმა, ქურდობის გამოვლენის მიზნით, მაღაზიაში დაამონტაჟა ხილული და ფარული კამერები, თუმცა დასაქმებულებს აცნობა, რომ

²⁶ Rycak A., *New Technologies and the Employee's Right to Privacy*, in: *Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes*, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 177.

²⁷ López Ribalda and Others v. Spain [ECtHR], App. nos. 1874/13 and 8567/13, 17 October 2019.

²⁸ Rycak A., *New Technologies and the Employee's Right to Privacy*, in: *Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes*, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 177.

მხოლოდ ხილული კამერებით ხდებოდა მათი პერსონალური მონაცემების დამუშავება. ვიდეომონიტორინგის შედეგად, გამოვლინდა ქურდობის ფაქტები, რის შედეგადაც დასაქმებულები სამსახურიდან გაათავისუფლეს. ამ დასაქმებულებიდან რამდენიმემ იჩივლა და ესპანურმა სასამართლოებმა არ დააკმაყოფილეს მათი სარჩელები, რადგან მიიჩნიეს, რომ მიზანი, რაც დამსაქმებელს ჰქონდა და ამ მიზნის მიღწევის საშუალება, გამართლებული იყო. მიუხედავად იმისა, რომ ცალსახა იყო დამსაქმებლის მიზანი – გამოვევლინა ქურდობის ფაქტები, ევროსასამართლოს დიდმა პალატამ მიიჩნია, რომ ამ შემთხვევაში დაირღვა დასაქმებულების პირადი ცხოვრების უფლება და მათი პერსონალური მონაცემების დამუშავების კანონიერება, რადგან ესპანური სამართლის მიხედვით, მონაცემთა სუბიექტი გაფრთხილებული უნდა ყოფილიყო მისი პერსონალური მონაცემების იმგვარ დამუშავებაზე, როგორც ეს განსახილველ შემთხვევაში იყო. სასამართლომ დაადგინა, რომ დამსაქმებელს სხვა საშუალებითაც შეეძლო იმავე მიზნის მიღწევა და შესაბამისად, არ გაიზიარა ესპანური სასამართლოების მიდგომა პერსონალური მონაცემების დამუშავების პროპორციულობასა და კანონიერებაზე. ამგვარად, ფარული კამერებით პერსონალური მონაცემების დამუშავება უკანონოდ იქნა მიჩნეული.²⁹

ზემოთ მოტანილი სასამართლო გადაწყვეტილებების ანალიზზე, ცალსახად მხოლოდ ერთი რამ შეიძლება ითქვას, რომ თუ არსებობს სხვა საშუალება, რომელიც თუნდაც მაღალიაში, სუპერმარკეტში, თუ ნებისმიერ სხვა დანესებულებაში ქურდობის ან/და სხვა სახის კანონდარღვევას გამოავლენს, უმჯობესი იქნება, დამსაქმებელმა სწორედ ეს სხვა საშუალება აირჩიოს. რა თქმა უნდა, ურთულესია

²⁹ დამატებით იხ., Krzysztofek M., GDPR: General Data Protection in the European Union, Wolters Kluwer, 2019, 106.

პრაქტიკაში ამ ყველაფრის გათვალისწინება, თუმცა ცალსახაა, რომ სასამართლოების მიდგომა საკმაოდ მკაცრია და პერსონალური მონაცემების დამუშავების უკანონოდ ცნობის ალბათობა მაღალია. მაგალითად, თუ მარაგის გაკონტროლება სხვა სამუშაოებით შეიძლება, ვიდეომონიტორინგი არ უნდა იქნეს გამოყენებული.

Antović and Mirković v Montenegro³⁰

კიდევ ერთი პრეცედენტული და იურიდიულ ლიტერატურაში ძალიან ხშირად განხილული საქმე არის *Antović and Mirković v Montenegro*³¹. ფაქტობრივი გარემოებების მიხედვით, მომჩივანი იყო ლექტორი, რომელიც პრეტენზიას აცხადებდა აუდიტორიაში დამონტაჟებული ვიდეოკამერების გამო. კერძოდ, როგორც ირკვეოდა, აუდიტორიებში კამერები განათავსეს საკუთრების უფლების დაცვის მიზნით, თუმცა პროფესორის განცხადებით, აუდიტორიები დაკეტილი იყო ლექციების დაწყებამდე და ლექციების დასრულების შემდეგ კვლავ იკეტებოდა. შესაბამისად, არ არსებობდა საკუთრების უფლების ხელყოფის საფრთხე.

ევროსასამართლომ განმარტა, რომ აუდიტორიები არის სივრცე, სადაც პროფესორები არა მხოლოდ ასწავლიან სტუდენტებს, არამედ ურთიერთობენ მათთან, რითაც ავითარებენ ურთიერთკავშირს და აყალიბებენ მათ სოციალურ იდენტობას. სასამართლოს შეფასებით, მიუხედავად უნივერსიტეტის პოზიციისა, რომ კამერები საჭირო იყო უსაფრთხოების, უცხო პირების შემოსვლის აღკვეთისა და საკუთრების უფლების დასაცავად, ეს მაინც ვერ ქმნიდა იმ ლეგიტიმურ მიზანს, რომ ლექტორის/პროფესორის სამუშაო პროცესი, როგორც პირადი ცხოვრებით დაცული სფერო პერსონალური მონაცემე-

³⁰ Antović and Mirković v. Montenegro [ECtHR], App. no. 70838/13, 28 November 2017.

³¹ იქვე.

ბის დაცვის შესახებ კანონმდებლობის შესაბამისად დამუშავებულიყო.

ზემოაღნიშნულიდან გამომდინარე, ევროსასამართლომ კონვენციის მე-8 მუხლთან სანინალმდეგოდ მიიჩნია პროფესორის/ლექტორის ვიდეომონიტორინგი აუდიტორიაში, რადგან არ არსებობდა პერსონალური მონაცემების დამუშავების ასეთი ფორმის მიზანშეწონილობა საკუთრების უფლებების ან სხვა რაიმე მნიშვნელოვანი სიკეთის დაცვისათვის. ამავდროულად, სასამართლომ მიიჩნია, რომ კონვენციის მე-8 მუხლი ფართოდ უნდა განმარტებულიყო და პირადი ცხოვრების დაცვაში მოაზრებულიყო ასევე პირის (დასაქმებულის) კომუნიკაცია და ინტერაქცია სხვა პირებთან, განსახილველ შემთხვევაში სტუდენტებთან.³²

ვიდეომონიტორინგთან დაკავშირებით ზემოთ მოცემული გადანყვეტილებები საორიენტაციო და პრაქტიკაში ყველაზე მეტად გასათვალისწინებელია.³³ ამასთან, კიდევ ერთხელ უნდა აღინიშნოს, რომ ამ გადანყვეტილებებში ან თუნდაც კანონში მოცემული მონესრიგების პრაქტიკაში ზედმიწევნით სრულყოფილად გატა-

³² Sychenko E., Perulli A., *Employment Law and the European Convention on Human Rights, The Research of the Recent Jurisprudence of the ECtHR Related to Employment Law (2017-2021)*, Wolters Kluwer, 2023, 49.

³³ დასაქმებულის აუდიო და ვიდეომონიტორინგს არ შეეხება, თუმცა ერთ-ერთი პრეცედენტული და თანამედროვე იურიდიულ ლიტერატურაში ძალიან ხშირად ციტირებული საქმეა *Bărbulescu v. Romania*. ამ საქმეში სასამართლომ შეაფასა, დაირღვა თუ არა პერსონალური მონაცემების დამუშავების წესი დამსაქმებლის მიერ დასაქმებულის პერსონალური მოკლეთექსტური შეტყობინებების წაკითხვით, იმ პირობებში, როდესაც, დასაქმებულმა ისარგებლა სამსახურებრივი ინტერნეტით და ამით დაარღვია შრომითი ურთიერთობის მომწესრიგებელი წესები. ამდენად, სასამართლომ შეაფასა, რამდენად ჰქონდა სხვა ალტერნატიული საშუალება დამსაქმებელს, გამოევიდინა შრომითი ურთიერთობის მომწესრიგებელი წესების დარღვევა სხვა საშუალებით და არა დასაქმებულის მოკლეთექსტური შეტყობინების აღმოჩენითა და წაკითხვით. იხ., *Bărbulescu v. Romania* [ECtHR], App. no. 61496/08, 5 September 2017.

რება ხშირად შეუძლებელია. შესაბამისად, ყოველ კონკრეტულ შემთხვევაში, ბიზნესის სპეციფიკის, ფინანსური დანახარჯებისა და ადამიანური რესურსის გათვალისწინებით უნდა შეირჩეს ვიდეომონიტორინგის, როგორც დასაქმებულის პერსონალური მონაცემების დამუშავების, მეთოდი.

3. თანხმობა ვიდეომონიტორინგზე

მონაცემთა სუბიექტის პერსონალური მონაცემების დამუშავებისთვის ყველაზე მნიშვნელოვანი იურიდიული აქტი არის თავად მონაცემთა სუბიექტის თანხმობა, როგორც საფუძველი, დამუშავდეს სუბიექტის პერსონალური მონაცემები. ამასთან, თანხმობა მხოლოდ მაშინაა კანონიერი, თუ ის ნების თავისუფლად გამოვლენის შედეგადაა მიღებული.³⁴ „პერსონალური მონაცემების დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „მ“ და „ნ“ ქვეპუნქტები თანხმობის სახეებს ჩამოთვლის და ადგენს, რომ მონაცემთა სუბიექტის თანხმობა არის მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ, მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით (მათ შორის, ელექტრონულად) ან ზეპირად, თავისუფლად და მკაფიოდ გამობატული ნება, ხოლო მონაცემთა სუბიექტის წერილობითი თანხმობა კი ნიშნავს თანხმობას, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან რომელიც მან სხვაგვარად გამობატა წერილობით (მათ შორის, ელექტრონულად) მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე შესაბამისი ინფორმაციის მიღების შემდეგ. პერსონალური მონაცემების დამუშავების მიზანი თავიდანვე უნდა განისაზღვროს და თუ აღნიშნული თავიდანვე

³⁴ Hendrickx F., Article 8 – Protection of Personal Data, The Charter of Fundamental Rights of the European Union and the Employment Relation, Edited by F. Dorssemont, K. Lorcher, S. Clauwaert and M. Schmitt, Hart Publishing, 2019, 265.

ნათლად და ერთმნიშვნელოვნად არ მოხდა, პერსონალური მონაცემების დამუშავება უკანონოა.³⁵

შრომით ურთიერთობებში დასაქმებულის, როგორც მონაცემთა სუბიექტის, წერილობითი თანხმობა როგორც წესი, შრომის ხელშეკრულებით ან/და ცალკე განცხადება/შეთანხმებითაა გამოხატული. შესაბამისად, შრომის ხელშეკრულების დადების შემდეგ დამსაქმებელს უკვე თავისუფლად შეუძლია შეაგროვოს და დაამუშაოს დასაქმებულის პერსონალური ინფორმაცია.³⁶ მონაცემთა დამუშავებაზე პასუხისმგებელი სუბიექტი ვალდებულია წარმოადგინოს მონაცემთა სუბიექტის თანხმობა პერსონალური მონაცემების დამუშავების შესახებ. შესაბამისად, მტკიცების ტვირთი იმისა, რომ პერსონალური მონაცემების მონაცემთა სუბიექტის თანხმობით მუშავდება, პერსონალური მონაცემების დამუშავებაზე პასუხისმგებელ პირს ეკისრება.³⁷

ხშირ შემთხვევაში, როდესაც დამსაქმებელი დასაქმებულს სთხოვს თანხმობას მისი პერსონალური მონაცემების დამუშავებაზე, დასაქმებულის, როგორც მონაცემთა სუბიექტის, თანხმობა სამომავლო გართულებებისგან, მათ შორის, სამსახურიდან გათავისუფლებისგან თავის არიდებითაა განპირობებული.³⁸ ამდენად,

³⁵ Terwangne D. E., Article 5. Principles Relating to Processing of Personal Data, in: The EU General Data Protection Regulation (GDPR), A Commentary, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020, 315.

³⁶ Lee S.-W., Protection of Employees' Personal Information and Privacy at a Crossroads in Korea, in: Protection of Employees' Personal Information and Privacy, Edited by R. Blanpain, H. Nakakubo, T. Araki, Wolters Kluwer, 2014, 151.

³⁷ Kosta E., Article 7. Conditions for Consent, in: The EU General Data Protection Regulation (GDPR), A Commentary, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020, 349.

³⁸ Eecke V. P., Šimkus A., Article 88. Processing in the Context of Employment, in: The EU General Data Protection Regulation (GDPR), A Commentary, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020, 1236.

შესაძლოა იყოს შემთხვევები, როდესაც კითხვის ნიშნის ქვეშ დადგეს დასაქმებულის ნებაყოფლობითი თანხმობა მისი პერსონალური მონაცემების დამუშავების შესახებ,³⁹ რადგან შრომითი ურთიერთობის სუბორდინაციულმა ხასიათმა შეიძლება დასაქმებულის ნების ფორმირება ისე მოახდინოს, რომ ამით მონაცემთა სუბიექტის უფლებები შეილახოს.⁴⁰ ამ საკითხზე საინტერესოა გერმანიის მონაცემთა დაცვის ფედერალური აქტი (BDSG), რომელიც სპეციალურ მუხლს ითვალისწინებს შრომით ურთიერთობებში დასაქმებულის, როგორც მონაცემთა სუბიექტის, პერსონალური მონაცემების დამუშავებაზე თანხმობისთვის.⁴¹ გერმანული კანონი ადგენს, რომ დასაქმებულის მიერ თანხმობის გამოხატვის დროს ყურადღება უნდა მიექცეს დასაქმებულის დამოუკიდებლობის ხარისხს (დონეს) რამდენად თავისუფლად გამოხატა მან თანხმობა/ნება თავისი პერსონალური მონაცემების დამსაქმებლის მხრიდან დამუშავებაზე. ამასთან, თანხმობა თავისუფლად გაცემულად მიიჩნევა, თუ ამას ეკონომიკური სარგებელი მოაქვს დასაქმებულისთვის ან თუ დამსაქმებელი და დასაქმებული ერთი ინტერესისთვის მოქმედებენ. ამგვარად, გერმანული კანონმდებლობა კონკრეტულ წინაპირობებსაც კი აწესებს, რაც შესაძლოა, საფუძვლად დაედოს დასაქმებულის, როგორც მონაცემთა სუბიექტის, თანხმობის გაცემას. შესაბამისად, ამ მოწესრიგებით, გერ-

³⁹ Krzysztofek M., GDPR: General Data Protection in the European Union, Wolters Kluwer, 2019, 104; Lee S.-W., Protection of Employees' Personal Information and Privacy at a Crossroads in Korea, in: Protection of Employees' Personal Information and Privacy, Edited by R. Blanpain, H. Nakakubo, T. Araki, Wolters Kluwer, 2014, 158.

⁴⁰ Vicente D. M., Casimiro S. V., Data Protection in the Internet: General Report, in: Data Protection in the Internet, Edited by D.M. Vicente, S.V. de Casimiro, Springer, 2020, 22; Bussche A. F., Voigt P., Data Protection in Germany, Including EU General Data Protection Regulation 2018, 2nd Ed., München, 2017, 52.

⁴¹ Federal Data Protection Act (BDSG) of the Federal Republic of Germany, 2017, Section 26.

მანული სამართალი, ფაქტობრივად, საცილოდ მიიჩნევს ყველა გამოვლენილ ნებას, თუ ეს ნება ფორმირებული და გამოვლენილი არ არის იმ სტანდარტის დაცვით, რაც შესაბამის მუხლშია მოცემული. ასეთი ჩანაწერი არ ტოვებს ინტერპრეტაციის ფართო საშუალებას და კონკრეტული წინაპირობებით შემოსაზღვრავს დასაქმებულის მიერ თანხმობის გაცემას ისეთი სპეციფიკურ ურთიერთობაში, როგორც შრომითსამართლებრივი ურთიერთობაა.

ამდენად, დასაქმებულის, როგორც მონაცემთა სუბიექტის თანხმობა შრომით ურთიერთობაში პრობლემური საკითხია,⁴² რაც პრაქტიკაში შესაძლოა ერთ-ერთ მწვავე საკითხად დადგეს. საკითხს ართულებს ის, რომ ქართული კანონმდებლობა, გერმანული სამართლისგან განსხვავებით, არ იცნობს დასაქმებულის ნების გამოხატვის წინაპირობებს, რაც თანხმობას ნამდვილს ან პირიქით, არანამდვილს ხდის. შესაბამისად, საბოლოო ჯამში, ნების ნამდვილად გამოხატვის საკითხი, საქართველოს სამოქალაქო კოდექსის შესაბამისი მუხლებით დადგენილი წესის მიხედვით, სასამართლოს შესაფასებელი იქნება, თუ, რა თქმა უნდა, დასაქმებული ამას სადავოდ გახდის.

4. აუდიომონიტორინგის მიმართება აუდიომონიტორინგთან

ცალკე უნდა გამოიყოს აუდიომონიტორინგიც. ზოგადი მიდგომა, რომლის თანახმადაც, ნებისმიერი მონიტორინგი უნდა იყოს მისი მიზნის შესაბამისი და უფლებაში უხეშად არ უნდა ჩაერიონ,⁴³ აუდიომონიტორინგის შემთხვევაში ალბათ, ერთ-ერთი ძირითადი პრინციპია. „პერსონალური მონაცემების დაცვის შესახებ“ საქართველოს

⁴² Hendrickx F., Article 8 – Protection of Personal Data, The Charter of Fundamental Rights of the European Union and the Employment Relation, Edited by F. Dorssemont, K. Lorcher, S. Clauwaert and M. Schmitt, Hart Publishing, 2019, 265.

⁴³ Lukacs A., Employees' Right to Privacy and Right to Data Protection on Social Network Sites, Szeged, 2021, 171.

კანონის მე-3 მუხლის „ყ“ ქვეპუნქტის თანახმად, აუდიომონიტორინგი არის საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ხმოვანი სიგნალის მონაცემთა დამუშავება, კერძოდ, აუდიოკონტროლი ან/და აუდიოჩანერა (გარდა ფარული საგამოძიებო მოქმედებისა). ამავე კანონის მე-11 მუხლი აწესრიგებს აუდიომონიტორინგის განხორციელების წინაპირობებსა და წესს. აუდიომონიტორინგის მომწესრიგებელი ნორმა, ვიდეომონიტორინგის განსხვავებით, არ შეიცავს ცალკე მოწესრიგებას შრომით ურთიერთობებში დასაქმებულის პერსონალური მონაცემების აუდიოჩანერის გზით დამუშავებასთან დაკავშირებით. ამავდროულად, კანონი ჩამოთვლის სულ 4 შემთხვევას/საფუძველს, რა დროსაც შესაძლებელია აუდიომონიტორინგის განხორციელება.⁴⁴

იურიდიულ ლიტერატურაში გამოთქმულია შეხედულება, რომ დასაქმებულის მონიტორინგს შესაძლოა პრევენციული, ღია ან ფარული ხასიათი ჰქონდეს და დამსაქმებელმა დასაქმებულის კონტროლი უშუალოდ სხვა დასაქმებულთა დახმარებით ან/და სხვა, გარე ხელშემკვრელი კომპანიის მეშვეობით განახორციელოს.⁴⁵ ყველა შემთხვევაში, დაცული უნდა იყოს მნიშვნელოვანი პრინციპი, რომლის თანახმადაც, აუდიომონიტორინგი დასაქმებულის პერსონალური მონაცემების დამუშავების ყველაზე მეტად შესაფერისი და შეიძლება ითქვას, უკანასკნელი საშუალება უნდა იყოს. ამასთან, ცხადია, აუდიომონიტორინგის შემთხვევაშიც, დიდი მნიშვნელობა ენიჭება მონაცემთა სუბიექტის თანხმობას.

თანხმობასთან დაკავშირებით, მნიშვნელოვანია აღინიშნოს, რომ იგი უნდა გამოიხატოს კონკრეტულად ვიდეომონიტორინგზე,

⁴⁴ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-11 მუხლის პირველი პუნქტი.

⁴⁵ Rycak A., *New Technologies and the Employee's Right to Privacy*, in: *Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes*, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020, 176.

რადგან ხშირია შემთხვევა, როდესაც თანხმობის 1 მუხლში თავმოყრილია სხვადასხვა, ერთმანეთთან არდაკავშირებული მონიტორინგის საფუძვლები, მიზნები და საშუალებები, რაც მონაცემთა სუბიექტს არ აძლევს საშუალებას, გაარკვიოს და ზუსტად გაიაზროს, რაზე აცხადებს თანხმობას.⁴⁶ ეს განსაკუთრებით აქტუალურია აუდიომონიტორინგთან მიმართებით, რადგან პერსონალური მონაცემების ამ გზით დამუშავება მნიშვნელოვანი ჩარევაა მონაცემთა სუბიექტის უფლებებში. რეალურად, ინფორმირებული თანხმობა, რასაც გამოხატავს დასაქმებული, ნიშნავს იმას, რომ იქამდე, ვიდრე მონაცემთა სუბიექტი გასცემს თანხმობას, მას უნდა მიენდოს ინფორმაცია, თუ რა მიზნით და რისთვის ხდება მისი ინფორმაციის დამუშავება და ასევე, მან უნდა იცოდეს, რომ ნებისმიერ დროს შეუძლია თავისი თანხმობა უკან გამოითხოვოს.⁴⁷ აქვე უნდა აღინიშნოს ისიც, რომ დასაქმებულის პერსონალური მონაცემების დამუშავება აუდიომონიტორინგის გზით იმდენად გამონაკლისი შემთხვევაა, რომ იურიდიულ ლიტერატურაში მასზე დანვრილებით მსჯელობები უიშვიათესია.

5. ვიდეომონიტორინგის მასალების შენახვის ვადა

„პერსონალური მონაცემების დაცვის შესახებ“ კანონი ადგენს ზოგად წესს მოპოვებული პერსონალური მონაცემების შენახვისთვის. ცალკე ნორმა ან შენახვის ვადა შრომით ურთიერთობაში ვიდეომონიტორინგის შედეგად მოპოვებული პერსონალური მონაცემების შესახებ, არ არსებობს. კანონის მე-4 მუხლის „ე“ ქვეპუნქტის თანახმად, მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რო-

⁴⁶ Krzysztofek M., GDPR: General Data Protection in the European Union, Wolters Kluwer, 2019, 73.

⁴⁷ Dehon E., Carey P., Fair, Lawful and Transparent Processing, in: Data Protection, A Practical Guide to UK and EU Law, 5th Ed., Edited by P. Carey, Oxford University Press, 2018, 53.

მელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად.

იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით. ზოგადად, პერსონალური მონაცემების შენახვის პრინციპია, რომ მოპოვებული პერსონალური მონაცემები იმაზე მეტი ხნის განმავლობაში არ უნდა იქნეს შენახული, რა მიზნისთვისაცაა ისინი მოპოვებული.⁴⁸ ამდენად, არ არსებობს რაიმე ერთიანი ვადა, რომელიც ამა თუ იმ, მათ შორის, განსაკუთრებული კატეგორიის პერსონალური მონაცემების შენახვის ვადას განსაზღვრავს.

ტექნოლოგიური განვითარების ფონზე, ვიდეომონიტორინგის სხვადასხვა სისტემა მონაცემების შეგროვების/გადაღების სხვადასხვა პერიოდს ითვალისწინებს. მაგალითად, შესაძლოა ვიდეო კამერების ერთმა სისტემამ მოპოვებული ინფორმაცია 1 თვიდან 6 თვემდე ვადით ავტომატურად შეინახოს და 6 თვის შემდეგ, ასევე ავტომატურად ახალი ინფორმაცია ძველ მონაცემებზე გადაწეროს. შესაძლოა უფრო ნაკლები ან მეტი ვადით ავტომატურად ჩაინეროს და ახალი მონაცემების გადაწეროს ძველ მონაცემებს. ეს ყველაფერი ვიდეოსისტემების ხარისხსა და ტექნიკურ მახასიათებლებზეა დამოკიდებული. ამ თვალსაზრისით, საინტერესოა ქართულ რეალობაში, რამდენი ხნით უნდა შეინახონ შრომით ურთიერთობებში ვიდეომონიტორინგით მოპოვებული მონაცემები. როგორც ზემოთ აღინიშნა, ამაზე რაიმე საკანონმდებლო ჩანაწერი არ არის და ვერც იქნება, რადგან ყოველ კონკრეტულ შემთხვევაში დამსაქმებლის მხრიდანაა დასადგენი.

გასაზიარებელია იურიდიულ ლიტერატურაში გამოთქმული შეხედულება, რომ პერსონალური მონაცემები შესაძლოა შეინახონ

⁴⁸ Carey P., *Data Protection Principles*, in: *Data Protection, A Practical Guide to UK and EU Law*, 5th Ed., Edited by P. Carey, Oxford University Press, 2018, 38.

იქამდე, ვიდრე სავარაუდოა, რომ ამ მონაცემებიდან გამომდინარე შესაძლოა რაიმე სამართლებრივი პროცედურები, მაგალითად, სასარჩელო წარმოება დაიწყო.⁴⁹ ამდენად, შესაძლოა ვიდეომონიტორინგით მოპოვებული პერსონალური მონაცემების შენახვა სასარჩელო წარმოების ხანდაზმულობის ვადასაც კი დაუკავშირდეს. შესაძლებელია, ამ მოსაზრების სანინააღმდეგო მიდგომებიც არსებობდეს, რადგან საქართველოს შრომის კოდექსი შრომითსამართლებრივი ურთიერთობიდან გამომდინარე ხანდაზმულობის 1 წლიან ვადას⁵⁰, ხოლო სამოქალაქო კოდექსი კი სახელშეკრულებო, თუ დელიქტური ვალდებულებების მიმართ სამწლიან⁵¹ ხანდაზმულობას ადგენს და ცხადია, ორივე ვადა საკმაოდ დიდი პერიოდია იმისთვის, რომ ვიდეომონიტორინგის მასალები შეინახონ. მეტიც, მართალია, ძალიან დიდი და ალბათ, არაგონივრული იქნება, თუმცა ქართული სასამართლო პრაქტიკა უსაფუძვლო გამდიდრების მიმართ 10 წლიან ხანდაზმულობის ვადას ადგენს.⁵² შესაბამისად, შესაძლოა დამსაქმებელმა ამ ვადაზეც კი მიუთითოს ვიდეომონიტორინგის რაღაც ნაწილის შენახვისას.

სავარაუდოდ, უფრო მეტად ლოგიკური, სამართლებრივად სწორი და დასაბუთებული იქნება, თუ შრომითი ურთიერთობის დროს განხორციელებული ვიდეომონიტორინგის მასალები შეინახება 1 წლის განმავლობაში. აქვე, ისიც უნდა აღინიშნოს, რომ თუ არსებობს ეჭვი ან/და დასაბუთებული ვარაუდი, რომ რაღაც გადაცდომა, დანაშაული ან/და ზიანის მიყენება მოხდა, შესაძლოა დაარქივებული ვიდეომონიტორინგის მასალები კიდევ უფრო მეტ ხანსაც იქნეს შენახული. შესაბამისად, როდესაც არის ვარაუდი, რომ რაღაც

⁴⁹ იქვე.

⁵⁰ საქართველოს შრომის კოდექსის 74-ე მუხლი.

⁵¹ საქართველოს სამოქალაქო კოდექსის 129-ე და 1008-ე მუხლები.

⁵² საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2024 წლის 29 თებერვლის ას-565-2022 გადაწყვეტილება; საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2022 წლის 5 ოქტომბრის ას-646-2023 განჩინება.

მიზნებიდან გამომდინარე, დამსაქმებელს ვიდეომონიტორინგის მასალები სჭირდება, სანამ ყველა ეს მიზანი არ მიიღწევა, მონაცემთა დამუშავებაზე პასუხისმგებელ პირს შეუძლია, რომ შეინახოს ეს მონაცემი.⁵³ ყველა შემთხვევაში, დამსაქმებელს დასჭირდება იმის მტკიცება და დასაბუთება, თუ რატომ და რა მიზნით ინახავს კონკრეტულ მონაცემს.

IV. დასკვნა

წარმოდგენილი მსჯელობიდან გამომდინარე, რამდენიმე მნიშვნელოვანი საკითხის გამოყოფაა შესაძლებელი. უპირველეს ყოვლისა, უნდა აღინიშნოს, რომ შრომით ურთიერთობებში ვიდეომონიტორინგის გზით პერსონალური მონაცემების დამუშავება განსაკუთრებული სპეციფიკურობით ხასიათდება. ეს სპეციფიკურობა გამომდინარეობს, ერთი მხრივ, დამსაქმებელი ორგანიზაციის კუთვნილი ზოგადად სამუშაო სივრცის და მეორე მხრივ, დასაქმებულის სამუშაო ადგილის კონტროლიდან. აღნიშნულის გათვალისწინებით, განვითარებული ქვეყნების მიდგომაა, არ უნდა მოხდეს დასაქმებულის სამუშაო სივრცის იმგვარი მონიტორინგი, რომ ამით დაირღვეს დასაქმებულის, როგორც მონაცემთა სუბიექტის, პირადი ცხოვრების უფლება, რომელიც პირის ღირსებასა და პირადი ცხოვრების ხელშეუხებლობაზე გადის.

ახლადამოქმედებული ქართული კანონი საკმაოდ მკაცრ ტესტს ადგენს დამსაქმებლებისთვის, როგორც მონაცემებზე პასუხისმგებელ პირებზე, რომ მათ მონაცემთა სუბიექტების პერსონალური მონაცემები ვიდეომონიტორინგის საშუალებით დაამუშაონ. ამასთან, ქართული და შესაძლებელია ითქვას, ევროპული ქვეყნების საკანონმდებლო ნორმები, პრაქტიკაში საკმაოდ რთული განსახორციელებელია. საკითხს ართულებს ევროსასამართლოს პრეცედენტული

⁵³ Carey P., *Data Protection Principles*, in: *Data Protection, A Practical Guide to UK and EU Law*, 5th Ed., Edited by P. Carey, Oxford University Press, 2018, 39.

გადანყვეტილებები, რომლებიც ადგენენ ძირითად, საორიენტაციო პრინციპებს ვიდეომონიტორინგის განხორციელებისთვის. ვიდეომონიტორინგისას დაცული უნდა იყოს პრინციპი, რომლის მიხედვითაც, ვიდეომონიტორინგი უნდა იყოს ყველაზე ბოლო/უკანასკნელი საშუალება იმ მიზნის მისაღწევად, რასაც დამსაქმებელი ისახავს და შესაბამისად, დამსაქმებელმა ვიდეომონიტორინგი არ უნდა გამოიყენოს დასაქმებულის პროფესიული მოქმედების/ქცევის გასაკონტროლებლად.

საკითხის გაანალიზების შედეგად დადგინდა, რომ დასაქმებულის, როგორც მონაცემთა სუბიექტის, თანხმობა შრომით ურთიერთობაში ერთ-ერთი პრობლემური და საკვანძო საკითხია. საკითხს ართულებს ის, რომ ქართული კანონმდებლობა, გერმანული სამართლისგან განსხვავებით, არ იცნობს დასაქმებულის ნების გამოხატვის წინაპირობებს, რაც თანხმობას ნამდვილს ან პირიქით, არანამდვილს ხდის შრომით ურთიერთობებში. შესაბამისად, საბოლოო ჯამში, ნების ნამდვილად გამოხატვის საკითხი, საქართველოს სამოქალაქო კოდექსის შესაბამისი მუხლებით დადგენილი წესის მიხედვით, სასამართლოს შესაფასებელი იქნება. ეს რამდენად კარგია ან ცუდი, ამას მომავალში სასამართლო პრაქტიკა აჩვენებს.

ნაშრომში მოკლედ გაანალიზდა აუდიომონიტორინგის წესი და პირობები, რის შემდეგაც შეიძლება ითქვას, რომ დასაქმებულის პერსონალური მონაცემების დამუშავება აუდიომონიტორინგის გზით საკმაოდ იშვიათი მოვლენაა, იგი, როგორც წესი, პერსონალური მონაცემების დამუშავების თვალსაზრისით, ვიდეომონიტორინგზე მეტად უხემ ფორმად მიიჩნევა. ამდენად, უცხოური დამსაქმებელიც და პრინციპში, საქართველოს დამსაქმებელი ორგანიზაციებიც ერიდებიან აუდიომონიტორინგის გზით დასაქმებულთა პერსონალური ინფორმაციის დამუშავებას.

რაც შეეხება ვიდეომონიტორინგის გზით მოპოვებული მასალების შენახვის ვადებს, კვლევის შედეგად გამოიკვეთა, რომ არც ქარ-

თული კანონმდებლობა და არც უცხოური, მათ შორის არც **GDPR** რაიმე სახის სპეციფიკურ ვადას პირდაპირ არ ითვალისწინებს. შესაბამისად, სავარაუდოა, რომ შრომით ურთიერთობაში ვიდეომონიტორინგის შედეგად, თუ დადგინდება დასაქმებულის ან თუნდაც დამსაქმებლის გადაცდომა, ზიანის მიყენება ან რაიმე სამართალდარღვევა, შრომის კოდექსით დადგენილი ხანდაზმულობის ვადა გამოიყენება და ვიდეომონიტორინგის მასალები დაარქივებული სახით 1 წლის განმავლობაში შეინახება. ამასთან, ეს ვადა საორიენტაციოა და შესაძლოა სხვადასხვა დამსაქმებელმა თავისუფლად დაასაბუთოს 3 წლიანი ხანდაზმულობის ვადის გამოყენების მიზანშეწონილობაც. ამგვარად, ვიდეომონიტორინგის შედეგად მოპოვებული პერსონალური მონაცემები როგორც დამუშავების, ისე შენახვის თვალსაზრისით, სპეციფიკურობით ხასიათდება და შრომით ურთიერთობაში არსებული მხარეებისგან შესაბამის კანონიერ და რაციონალურ მოქმედებებს მოითხოვს.

გამოყენებული სამეცნიერო ლიტერატურა

- Bussche A. F., Voigt P., Data Protection in Germany, Including EU General Data Protection Regulation 2018, 2nd Ed., München, 2017
- Carey P., Data Protection Principles, in: Data Protection, A Practical Guide to UK and EU Law, 5th Ed., Edited by P. Carey, Oxford University Press, 2018
- Davidov G., A Purposive Approach to Labour Law, Oxford University Press, 2016
- Dehon E., Carey P., Fair, Lawful and Transparent Processing, in: Data Protection, A Practical Guide to UK and EU Law, 5th Ed., Edited by P. Carey, Oxford University Press, 2018
- Eecke V. P., Šimkus A., Article 88. Processing in the Context of Employment, in: The EU General Data Protection Regulation (GDPR), A Commentary, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020

- Hendrickx F., Article 8 – Protection of Personal Data, The Charter of Fundamental Rights of the European Union and the Employment Relation, Edited by F. Dorssemont, K. Lorcher, S. Clauwaert and M. Schmitt, Hart Publishing, 2019
- Komukai T., Data Protection in the Internet: Japanese National Report, in: Data Protection in the Internet, Edited by D. M. Vicente, S. V. de Casimiro, Springer, 2020
- Kosta E., Article 7. Conditions for Consent, in: The EU General Data Protection Regulation (GDPR), A Commentary, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020
- Kourtis V., Data Protection in the Internet: Greece, in: Data Protection in the Internet, Edited by D. M. Vicente, S. V. de Casimiro, Springer, 2020
- Krzysztofek M., GDPR: General Data Protection in the European Union, Wolters Kluwer, 2019
- Lee S.-W., Protection of Employees' Personal Information and Privacy at a Crossroads in Korea, in: Protection of Employees' Personal Information and Privacy, Edited by R. Blanpain, H. Nakakubo, T. Araki, Wolters Kluwer, 2014
- Lukacs A., Employees' Right to Privacy and Right to Data Protection on Social Network Sites, Szeged, 2021
- Morris G., Protection of Employees' Personal Information and Privacy in English Law, in: Protection of Employees' Personal Information and Privacy, Edited by R. Blanpain, H. Nakakubo, T. Araki, Wolters Kluwer, 2014
- Rycak A., New Technologies and the Employee's Right to Privacy, in: Labor Law and GIG Economy, Challenges Posed by the Digitalization of Labor Processes, Edited by J. Carby-Hall, L. M. Mendez, Routledge, 2020
- Sousa Pinheiro A., Data Protection in the Internet: The Portuguese Case, in: Data Protection in the Internet, Edited by D. M. Vicente, S. V. de Casimiro, Springer, 2020
- Sychenko E., Perulli A., Employment Law and the European Convention on Human Rights, The Research of the Recent Jurisprudence of the ECtHR Related to Employment Law (2017-2021), Wolters Kluwer, 2023
- Terwangne D. E., Article 5. Principles Relating to Processing of Personal Data, in: The EU General Data Protection Regulation (GDPR),

A Commentary, Edited by Chr. Kuner, L.A. Bygrave, Chr. Docksey, L. Drechsler, Oxford University Press, 2020

- Tiainen M.K., Solving the Surveillance Problem, Media Debates about Unwanted Surveillance in Finland, in: Privacy, Data Protection and Cybersecurity in Europe, Edited by W.J. Schunemann, M. Baumann, Springer, 2017
- Vicente D. M., Casimiro S. V., Data Protection in the Internet: General Report, in: Data Protection in the Internet, Edited by D.M. Vicente, S.V. de Casimiro, Springer, 2020

STANDARD OF THE PROCESSING OF THE PERSONAL DATA DURING A VIDEOMONITORING OF EMPLOYEES' WORKSPACE

SIMONI TAKASHVILI

Associate Professor at Sulkhani-Saba Orbeliani University,
Attorney at Law

<https://orcid.org/0000-0001-8608-170X>

Abstract

Protection of personal data is a challenge for Georgian and not only Georgian law and practice. The article analyzes the latest legal approaches, foreign literature and international case law using a comparative legal method. The paper specially focuses on the new Georgian law on Personal Data Protection, which came into force a few months ago and provides specific rules for videomonitoring/video surveillance.

There is no any judgements or decisions by the Georgian general courts on the regulation established by the new law and its problematic issues. Therefore, the present article analyzes the EU's experience and the trends of its implementation in the Georgian reality.

There are several decision of ECtHR concernin the processing of personal data through video monitoring of the employee's workspace. These decisions are so important that they are mentioned in almost all modern legal literature. Therefore, the article overviews them and discusses Georgian legislation and legal practice in the light of the ECtHR's case law.

Keywords: Personal Data, Video Surveillance, Data processing, Store the Data, Consent.