ბიომეტრიული და გენეტიკური მონაცემების დამუშავება

ევროპული სტანდარტები

თბილისი
2022

კვლევის ავტორები:

ჟეთევან კუკავა
კანონის უზენაესობისა და ადამიანის უფლებების მიმართულების ხელმძღვანელი, IDFI

სალომე ჩხაიძე
იურისტი/მკვლევარი, IDFI

ნატა ახალაძე
იურისტი, IDFI

კვლევა მომზადდა პროექტის „პერსონალური მონაცემების დაცვის მხარდაჭერა საქართველოში“ ფარგლებში, რომელიც მხარდაჭერილია საქართველოში ნიდერლანდების საელჩოს მიერ. კვლევაში გამოხატული მოსაზრებები შეიძლება არ ასახავდეს ნიდერლანდების საელჩოს პოზიციას.

ISBN 978-9941-8-4136-1

ბიომეტრიული და გენეტიკური მონაცემების დამუშავება

ევროპული სტანდარტები

თბილისი
2022

სარჩევი

1. შესავალი

ბიომეტრიულად მიიჩნევა მონაცემი, რომელიც დაკავშირებულია ადამიანის ფიზიკურ, ბიოლოგიურ ან ფიზიოლოგიურ მახასიათებლებთან, რაც ინდივიდის უნიკალური იდენტიფიცირების შესაძლებლობას იძლევა.[1] ამგვარი მონაცემების გამოყენება ზრდის უსაფრთხოების დონეს, აადვილებს პირის იდენტიფიცირებისა და ვინაობის დადასტურების პროცედურას და უფრო მეტად სწრაფსა და მოსახერხებელს ხდის მათ. ტექნოლოგიურმა პროგრესმა ბიომეტრიული სისტემები უფრო ხელმისაწვდომი გახადა, თუმცა თანმდევ დადებით შედეგებთან ერთად, ახალი საფრთხეებიც წარმოშვა.[2]

ბიომეტრიული ტექნოლოგიების გამოყენების მზარდ პროცესს მონაცემთა დაცვის საზედამხედველო ორგანოები, სამოქალაქო საზოგადოება და სხვა სპეციალისტები კრიტიკის თვალით უყურებენ. ამის ერთ-ერთი მიზეზი ბიომეტრიული იდენტიფიკაციისა და ავტორიზაციის პროგრამების ავტომატიზაციაა.[3] 29-ე მუხლის სამუშაო ჯგუფის[4] სიტყვებით, ეს პროგრამები შეუქცევადად ცვლის სხეულსა და იდენტობას შორის დამოკიდებულებას, რადგან მათი მეშვეობით ადამიანის სხეულის მახასიათებლები „მანქანისთვის კითხვადი" ხდება და შემდგომ გამოყენებას ექვემდებარება.[5]

გარდა ამისა, ბოლო წლებში ადამიანის ბიოლოგიური მასალიდან მრავალი სახის პერსონალური მონაცემების მოპოვებამ უზარმაზარ მასშტაბებს მიაღწია, რაშიც გენომის სეკვენირებამ განსაკუთრებული როლი ითამაშა. კვლევების თუ მკურნალობის ფარგლებში და მათ მიღმა გაიზარდა გენეტიკური ტესტირებების სიზუსტე, ფარგლები, ხოლო მასშტაბების ზრდას გენომის სეკვენირების ღირებულების მკვეთრად შემცირებამ შეუწყო ხელი.[6]

გენეტიკური მონაცემების დამუშავების ტექნოლოგიების მიღწევები მკვლევრებს სხვადასხვა დაავადების უკეთ შესწავლაში, პრევენციისა და მკურნალობის გზების დადგენაში ეხმარება და ადამიანებისა და მათი ჯანმრთელობისთვის სასიცოცხლო მნიშვნელობას იძენს. თითოეული ადამიანის გენეტიკური აგებულება საერთოა მისთვის, მისი ოჯახის წევრებისა და იმ ჯგუფისთვის, რომელსაც ის მიეკუთვნება. შესაბამისად, გენეტიკური ტესტირებებით დაავადების რისკების შეფასება და ბიოლოგიური კავშირების განსაზღვრა გავლენას ახდენს არა მხოლოდ *ინდივიდის* პირადი ცხოვრების ხელშეუხებლობის უფლებაზე, არამედ წამოჭრის *პირთა ჯგუფის* პირადი ცხოვრების ხელშეუხებლობის საკითხსაც. გენეტიკური ინფორმაციის უნიკალურობა და პირის ან პირთა ჯგუფის მიმართ დისკრიმინაციული მოპყრობის რისკები კი ამ მონაცემებს განსაკუთრებულად სენსიტიურს ხდის.[7]

გენეტიკური მონაცემების დამუშავების შედეგად ადამიანების შესახებ უამრავი სხვადასხვა სახის ინფორმაციის მიღების მზარდი შესაძლებლობები და დნმ-ის უნიკალური ხასიათი მათზე სათანადო კონტროლის განხროციელებასა და პირადი ცხოვრების დაცვის ეფექტური მექანიზმების არსებობას აუცილებელს ხდის.

---

[1] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პარ. 58, ხელმისაწვდომია: https://bit.ly/3kF2S6l წვდომის თარიღი: 21.07.2021.

[2] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[3] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 209.

[4] საკონსულტაციო ორგანო, რომელიც მონაცემთა დაცვის დირექტივის საფუძველზე შეიქმნა.

[5] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 209.

[6] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 197.

[7] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, გვ. 85.

მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR)[8], პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის მონაცემთა დაცვის 2016/680 დირექტივის[9] მიღებით, ასევე ევროპის საბჭოს 108-ე კონვენციის მოდერნიზებით[10] გაჩნდა სამართლებრივი ინსტრუმენტები, რომლებიც ევროპის მასშტაბით ბიომეტრიული და გენეტიკური მონაცემების დამუშავებას აწესრიგებს.

მონაცემთა დაცვის ზოგადი რეგულაცია, რომელიც მსოფლიოში მონაცემთა დაცვის ყველაზე კომპლექსურ სამართლებრივ ჩარჩოდ მიიჩნევა, არ ვრცელდება უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებაზე.[11] ამგვარ დამუშავებას 2016/680 დირექტივა არეგულირებს. ამასთან, არც მონაცემთა დაცვის ზოგადი რეგულაცია და არც 2016/680 დირექტივა არ ვრცელდება[12] ეროვნული უსაფრთხოების უზრუნველყოფის მიზნით მონაცემთა შეგროვებაზე, შენახვაზე, დამუშავებასა და მიმოცვლაზე. ევროკავშირს ამ სფეროში პირდაპირი საკანონმდებლო უფლებამოსილება არ აქვს, რადგან ევროკავშირის შესახებ ხელშეკრულების თანახმად, ეროვნული უსაფრთხოების საკითხი თითოეული წევრი სახელმწიფოს პასუხისმგებლობას განეკუთვნება.[13]

რაც შეეხება მოდერნიზებულ 108-ე კონვენციას, ის დაუშვებლად მიიჩნევს ეროვნული უსაფრთხოებისა და თავდაცვის მიზნებისთვის მონაცემთა დამუშავებაზე სრულ გამონაკლისს. გამონაკლისი დაიშვება მხოლოდ ცალკეულ დებულებებთან დაკავშირებით, კანონით გათვალისწინებულ შემთხვევებში, თუ ეს პატივს სცემს ძირითადი უფლებებისა და თავისუფლებების არსს და აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში.[14] გამონაკლისის დაშვების მიუხედავად, კონვენცია ცალსახად ითვალისწინებს სახელმწიფო უსაფრთხოებისა და თავდაცვის მიზნებისათვის პერსონალურ მონაცემთა დამუშავებაზე ეფექტური და დამოუკიდებელი ზედამხედველობის უზრუნველყოფის ვალდებულებას.[15]

წინამდებარე კვლევა განიხილავს ბიომეტრიული და გენეტიკური მონაცემების ცნებას და გამოყენების არეალს, მათ დამუშავებასთან დაკავშირებულ საფრთხეებსა და რისკებს, აანალიზებს ამგვარი მონაცემების დამუშავების პრინციპებსა და საფუძვლებს. კვლევაში ასევე განხილულია ადამიანის უფლებათა ევროპული სასამართლოს და ევროკავშირის მართლმსაჯულების სასამართლოს მიერ მიღებული ცალკეული გადაწყვეტილებები, რაც ბიომეტრიული და გენეტიკური მონაცემების დამუშავებას უკავშირდება.

---

[8] პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის 2016/679 რეგულაცია, ხელმისაწვდომია: https://bit.ly/3C6j2Le წვდომის თარიღი: 20.07.2021.

[9] უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის 2016/680 დირექტივა, ხელმისაწვდომია: https://bit.ly/3kTaS3d წვდომის თარიღი: 20.07.2021.

[10] ხელმისაწვდომია: https://bit.ly/3qqm0Ip წვდომის თარიღი: 20.07.2021.

[11] მონაცემთა დაცვის ზოგადი რეგულაციის მე-2 მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტი.

[12] მონაცემთა დაცვის ზოგადი რეგულაციის მე-2 მუხლის მე-2 პუნქტი. 2016/680 დირექტივის მე-2 მუხლი.

[13] ევროკავშირის შესახებ ხელშეკრულების მე-4 მუხლის მე-2 პუნქტი, ხელმისაწვდომია: https://bit.ly/3cd5mDw წვდომის თარიღი: 14.11.2021.

[14] 108+ კონვენციის მე-11 მუხლი.

[15] The modernised Convention 108: novelties in a nutshell, ხელმისაწვდომია: https://bit.ly/3caNkBX წვდომის თარიღი: 14.11. 2021.

2. ბიომეტრიული მონაცემების დამუშავება

2.1. ბიომეტრიული მონაცემების ცნება

108+ კონვენციის თანახმად, ბიომეტრიულად მიიჩნევა მონაცემი, რომელიც დაკავშირებულია ადამიანის ფიზიკურ, ბიოლოგიურ ან ფიზიოლოგიურ მახასიათებლებთან, რაც ინდივიდის უნიკალური იდენტიფიცირების შესაძლებლობას იძლევა.[16] ბიომეტრიული მონაცემების მაგალითებია: თითის ანაბეჭდები, თვალის ბადურის გამოსახულება, სახის სტრუქტურა, ხმა, ხელის გარშემოწერილობა, ზოგიერთი თანდაყოლილი უნარი ან სხვა ქცევითი მახასიათებელი (მაგალითად, ხელმოწერა, კლავიატურაზე ბეჭდვის, სიარულის ან საუბრის კონკრეტული მანერა და სხვა).[17] კონკრეტულ ადამიანთან უნიკალური კავშირის გამო, ბიომეტრიული მონაცემები შესაძლოა გამოყენებულ იქნას ინდივიდის იდენტიფიცირებისთვის.[18]

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია ბიომეტრიულ მონაცემებს, რომლის მიზანი ფიზიკური პირის უნიკალური იდენტიფიცირებაა, განსაკუთრებული კატეგორიის მონაცემის სტატუსს ანიჭებს.[19] ამ რეგულაციის მსგავსად, განსაკუთრებული კატეგორიის მონაცემის ცნების გაფართოებულ ნუსხას გვთავაზობს მოდერნიზებული 108-ე კონვენცია[20] და 2016/680 დირექტივა[21] და მასში მოიაზრება ბიომეტრიული მონაცემებიც, რომლითაც პიროვნების იდენტიფიცირება ხდება.

ბიომეტრიული მონაცემები შეიძლება რამდენიმე კატეგორიად დაიყოს, მაგალითად, „ძლიერ“, „სუსტ" და „მსუბუქ" იდენტიფიკატორებად. ძლიერი იდენტიფიკატორები ფიზიკური პირის უნიკალური იდენტიფიცირების შესაძლებლობას იძლევა, მაგალითად, თითის ანაბეჭდი, თვალის ბადურა და ფერადი გარსი. სუსტ კატეგორიას მიეკუთვნება ის მახასიათებლები, რომლებიც „ნაკლებად უნიკალური" ან „ნაკლებად სტაბილურია," მაგალითად, სხეულის ფორმა, ქცევის მანერა, ხმა და სხვა. მსუბუქ ბიომეტრიულ მახასიათებლებს ზოგადი ბუნება აქვთ და პირთან უნიკალური კავშირი არ გააჩნიათ, მაგალითად, ასაკი და სქესი.[22] GDPR-ში ასახული „უნიკალური იდენტიფიცირების“ კომპონენტი, შესაძლოა, კანონმდებლის მიერ მსუბუქი ბიომეტრიული მახასიათებლების იგნორირებას ნიშნავდეს.[23]

მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, „ბიომეტრიული მონაცემი” სპეციალური ტენიკური დამუშავების შედეგად მოპოვებული პერსონალური მონაცემია, რომელიც დაკავშირებულია ადამიანის ფიზიკურ, ფიზიოლოგიურ ან ქცევით მახასიათებლებთან, რაც იძლევა ამ ფიზიკური პირის უნიკალური იდენტიფიკაციის შესაძლებლობას ან ადასტურებს მის ვინაობას, მაგალითად, სახის

[16] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პარ. 58, ხელმისაწვდომია: https://bit.ly/3kF2S6l წვდომის თარიღი: 21.07.2021.

[17] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, ხელმისაწვდომია: https://bit.ly/3kET3W4 წვდომის თარიღი: 21.07.2021.

[18] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, ხელმისაწვდომია: https://bit.ly/3kET3W4 წვდომის თარიღი: 21.07.2021.

[19] მონაცემთა დაცვის ზოგადი რეგულაცია, მე-9 მუხლი, ხელმისაწვდომია: https://bit.ly/3Bn9Vqh წვდომის თარიღი: 21.07.2021.

[20] 108+ კონვენცია, მუხლი 6 (1).

[21] 2016/680 დირექტივის მე-10 მუხლი.

[22] Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, გვ. 13. ხელმისაწვდომია: https://bit.ly/30QyFKd წვდომის თარიღი: 24.12.2021.

[23] Tamas Bisztray, Nils Gruschka, Thirimachos Bourlai, Lothar Fritsch, Emerging biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks, 2021, ხელმისაწვდომია: https://bit.ly/3yTCKcY წვდომის თარიღი: 24.12.2021.

გამოსახულება ან დაქტილოსკოპიური მონაცემები.[24]

მონაცემთა დაცვის ზოგადი რეგულაციის მე-4 მუხლის მე-14 პუნქტი არ განსაზღვრავს ბიომეტრიული მონაცემების გენერირების ან დამუშავების პროცესებს. ის მიუთითებს, რომ მონაცემი სპეციალური ტექნიკური დამუშვების შედეგად არის მიღებული, თუმცა არ განმარტავს კონკრეტულად რაში გამოიხატება ტექნიკური დამუშავება, რაც ცნების ფორმულირებას ბუნდოვანებას სძენს.[25] მაგალითად, დნმ GDPR-ის მე-4(13) მუხლის მიხედვით გენეტიკური მონაცემის დეფინიციაშიც შედის, მე-4(14) მუხლის შესაბამისად ბიომეტრიული მონაცემიც შეიძლება იყოს (სპეციალური ტექნიკური დამუშავების ფარგლებში) და მე-4(15) მუხლის თანახმად ადამიანის ჯანმრთელობასთან დაკავშირებულ ინფორმაციასაც წარმოადგენს. თუმცა, მსგავსი გადაფარვები GDPR-ის გავრცელებასთან მიმართებით სირთულეებს არ ქმნის. ამ კუთხით ჩანს, რომ GDPR-ის მე-9(4) მუხლი წევრ სახელმწიფოებს უტოვებს მნიშვნელოვან თავისუფალ სივრცეს, შეხედულებისამებრ დაარეგულირონ გენეტიკური, ბიომეტრიული და ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავება.[26]

მონაცემთა დაცვის ზოგადი რეგულაციის მე-4(14) და მე-9 მუხლების შესაბამისად, ბიომეტრიული მონაცემის ცნება შემდეგ სამ კომპონენტს მოიცავს:

მონაცემის ბუნება: მონაცემი დაკავშირებულია ადამიანის ფიზიკურ, ფიზიოლოგიურ ან ქცევით მახასიათებელთან;

დამუშავების საშუალება და მეთოდი: მონაცემი მოპოვებულია სპეციალური ტექნიკური დამუშავების შედეგად;

დამუშავების მიზანი: მონაცემი გამოყენებულია ფიზიკური პირის უნიკალური იდენტიფიკაციისთვის. [27]

ფოტოსურათი ბიომეტრიული მონაცემის ცნების ქვეშ ექცევა მაშინ, როცა ის სპეციალური ტექნიკური საშუალების გამოყენებით მუშავდება და ფიზიკური პირის უნიკალური იდენტიფიკაცია ან აუთენტიფიკაცია ხდება.[28] მონაცემთა დაცვის ზოგად რეგულაციასა და 2016/680 დირექტივაში[29] მოცემული ბიომეტრიული მონაცემის განმარტება „სპეციალური ტექნიკური დამუშავების" კომპონენტს მოითხოვს. შესაბამისად, ცალკე აღებული ვიდეომასალა, ფოტოსურათი ან ხმოვანი ჩანაწერები ვერ ჩაითვლება GDPR-ის მე-9 მუხლით გათვალისწინებულ ბიომეტრიულ მონაცემად და მასზე ვერ გავრცელდება უფრო ძლიერი დაცვის გარანტიები. დეფინიციის მიხედვით, სწორედ დამუშავების ხასიათი აქცევს მონაცემს ბიომეტრიულად.[30]

---

[24] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4(14).

[25] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 212.

[26] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 213.

[27] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. პარ. 76, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[28] მონაცემთა დაცვის ზოგადი რეგულაციის პრეამბულის 51-ე პუნქტი; Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. პარ. 74, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[29] 2016/680 დირექტივის მე-3 მუხლის მე-13 პუნქტი.

[30] Els Kindt, A First Attempt at Regulating Biometric Data in the European Union, 2020, ხელმისაწვდომია: https://bit.ly/3iNntmH წვდომის თარიღი: 21.07.2021.

2.2. ბიომეტრიული მონაცემების გამოყენების არეალი

ბიომეტრიული სისტემები ინფორმაციის (მაგალითად, მონაცემთა ბაზებში არსებული ინფორმაცია) ავტომატიზებული შედარების საფუძველზე ადამიანების იდენტიფიცირებას ან მათი ვინაობის დადასტურებას ახორციელებენ.[31] თუმცა, აუცილებელია აღინიშნოს, რომ იდენტიფიცირების მიღმა, ბიომეტრიულ მონაცემებს შეუძლია მოგვაწოდოს დეტალური ინფორმაცია ადამიანების შესახებ (მაგალითად, ჯანმრთელობის მდგომარეობის შესახებ), რამდენადაც ბიომეტრიული ტექნოლოგიის სენსორები ადამიანის სხეულის ნიშან-თვისებებს ეყრდნობა.[32]

ხელოვნურ ინტელექტთან კომბინაციაში, ბიომეტრიულ ტექნოლოგიებს სადიაგნოსტიკო როლის შესრულებაც შეუძლიათ. მაგალითად, გაერთიანებულ სამეფოში განავითარეს ინსტრუმენტი, რაც თვალის ბადურის სკანირების მეშვეობით თვალის დაავადებების ნიშნების იდენტიფიცირების შესაძლებლობას იძლევა.[33]

ბიომეტრიული მახასიათებლების ავტომატიზებული გამოყენების მნიშვნელოვანი პოტენციალის, ასევე იდენტიფიცირებისა და ვინაობის დადასტურების სანდოობის გამო, ამგვარი სისტემები ფართოდ გამოიყენება როგორც საჯარო, ისე კერძო სექტორში.[34] თუკი თავდაპირველად ბიომეტრიულ ტექნოლოგიებს ძირითადად სახელმწიფო უწყებები იყენებდნენ, ბოლო პერიოდში კომერციული ორგანიზაციებიც მნიშვნელოვან როლს ასრულებენ ამ ტექნოლოგიების გამოყენებასა და ახალი პროდუქტების შექმნაში.[35] ამგვარი ცვლილება ტექნოლოგიების განვითარებამ და დახვეწამ განაპირობა. ბიომეტრიული სისტემები ანაცვლებენ ან აუმჯობესებენ ტრადიციულ საიდენტიფიკაციო მეთოდებს, რომლებიც ძლიერი სისტემების უზრუნველსაყოფად მრავლობით საიდენტიფიკაციო ფაქტორებს მოითხოვდა.[36]

საჯარო სექტორში ბიომეტრიულ სისტემებს აქტიურად იყენებენ დოკუმენტების აუთენტურობისა და პირის ვინაობის დასადასტურებლად (მაგალითად, პირადობის დამადასტურებელი მოწმობა).[37] გარდა ამისა, სამართალდამცავი ორგანოები ფართოდ იყენებენ ავტომატიზებულ ბიომეტრიულ მონაცემთა ბაზებს, კერძოდ, თითის ანაბეჭდებს, ხშირად სხვა ქვეყნების სამართალდამცავ ორგანოებთან თანაშრომლობით. რაც შეეხება კერძო სექტორს, ბიომეტრიული სისტემები ემსახურება ცალკეულ ადგილებზე, ქსელებსა და ინფორმაციაზე დაშვების კონტროლის უსაფრთხოებას, ადმინისტრაციულ და სხვა მიზნებს.[38]

---

[31] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 19.

[32] Digital identity and biometrics: When your face reveals your vaccination status ... and more, ხელმისაწვდომია: https://bit.ly/3yQM5Cj წვდომის თარიღი: 22.12.2021.

[33] Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, გვ.18, ხელმისაწვდომია: https://bit.ly/30QyFKd წვდომის თარიღი: 22.12.2021.

[34] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 64.

[35] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[36] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[37] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 64.

[38] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 65.

გარდა ამისა, თითის ანაბეჭდისა და სახის ამომცნობი პროგრამები ხშირად ჩაშენებულია თანამედროვე სმარტფონებში, ტაბლეტებში/პლანშეტებსა და ლეპტოპებში.[39] ზოგიერთი კომპანია სახის ამომცნობ ტექნოლოგიას დასაქმებულთა სამუშაო საათების კონტროლის მიზნითაც იყენებს.[40]

პაროლის ან მოწმობის გამოყენებისგან განსხვავებით, ბიომეტრიული აუთენტიფიკაციის დროს შეგროვებული მონაცემები ან იდენტიფიკაციის პროცედურა უფრო მეტ ინფორმაციას ავლენს ადამიანის შესახებ.[41] ბიომეტრიულ მონაცემებზე დაყრდნობით შესაძლებელია პირის რასის ან სქესის (მათ შორის, თითის ანაბეჭდიდან), ემოციური მდგომარეობის, გენეტიკური თავისებურებების, დაავადებებისა და სხვა მახასიათებლების შესახებ მონაცემების მოპოვება. ვინაიდან ეს ინფორმაცია „ჩაშენებულია" მონაცემთა სუბიექტში, მას არ შეუძლია ამგვარი დამატებითი ინფორმაციის შეგროვების თავიდან აცილება.[42]

ბიომეტრიული სისტემით ინდივიდის **იდენტიფიკაცია** გულისხმობს მისი ბიომეტრიული მონაცემების შედარებას მონაცემთა ბაზაში არსებულ ბიომეტრიულ ნიმუშებთან, ხოლო ინდივიდის **ვერიფიკაცია/დადასტურება** არის მისი ბიომეტრიული მონაცემების შედარება მოწყობილობაში არსებულ კონკრეტულ ბიომეტრიულ ნიმუშთან.

ტექნოლოგიური გავნითარების შედეგად, შესაძლებელია ბიომეტრიული სისტემების გამოყენება **კატეგორიზაციის/სეგრეგაციის მიზნით**. ეს გულისხმობს იმის დადგენას, ადამიანის ბიომეტრიული მონაცემები მიეკუთვნება თუ არა წინასწარ განსაზღვრული ნიშნის მქონე ჯგუფს, მაგალითად, კონკრეტული ასაკის ან სქესის ადამიანებს. ამ შემთხვევაში, ინდივიდის იდენტიფიკაცია და ვერიფიკაცია არ არის მნიშვნელოვანი, რადგან ამ პროცესის შედეგად ის ავტომატურად ადამიანთა კონკრეტულ კატეგორიას მიეკუთვნება. მაგალითად, ადამიანები შესაძლოა განსხვავებულ რეკლამებს ხედავდნენ მათი ასაკის ან სქესის გათვალისწინებით. როდესაც მონაცემთა დამუშავების მიზანია განასხვავოს ადამიანთა ერთი ჯგუფი მეორისგან, მაგრამ არა ინდივიდის უნიკალური იდენტიფიცირება, ამგვარი დამუშავება არ ექცევა GDPR-ის მე-9 მუხლის ფარგლებში.

მაგალითი: მაღაზიის მფლობელს სურს რეკლამის დამზადება, რომელიც დაეყრდნობა და გაითვალისწინებს ვიდეო მეთვალყურეობის სისტემით გადაღებული კლიენტის სქესისა და ასაკის მახასიათებლებს. თუ ეს სისტემა არ გამოიმუშავებს ბიომეტრიულ ნიმუშს პირების უნიკალური იდენტიფიცირებისათვის, არამედ გამოავლენს პიროვნების ფიზიკურ მახასიათებლებს პირთა კლასიფიცირების მიზნით, ამ შემთხვევაში, დამუშავება არ მოექცევა მე-9 მუხლის მოქმედების სფეროში (რადგან სხვა სახის განსაკუთრებული კატეგორიის მონაცემები არ მუშავდება).[43]

თუ მონაცემთა დამმუშავებელს სურს გაიგოს, მომხმარებელი ხელახლა სტუმრობს თუ არა იმავე ან

[39] National Cyber Security Centre of UK, Using Biometrics, ხელმისაწვდომია: https://bit.ly/3msYfMP წვდომის თარიღი: 22.12.2021.

[40] Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, გვ. 15, ხელმისაწვდომია: https://bit.ly/30QyFKd წვდომის თარიღი: 22.12.2021.

[41] EDPS and AEPD Joint Paper, 14 Misunderstandings with Regard to Identification and Authentication, June 2020.

[42] EDPS and AEPD Joint Paper, 14 Misunderstandings with Regard to Identification and Authentication, June 2020. დამატებითი ინფორმაციისთვის იხ. სტატია The Hidden Data in Your Fingerprints, ხელმისაწვდომია: https://bit.ly/38w7XH2 წვდომის თარიღი: 01.09.2021.

[43] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. პარ. 80, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

სხვა არეალს და შემდგომ ამ მონაცემებს ინდივიდუალიზებული მარკეტინგის მიზნით იყენებს, მაშინ მისი მიზანი მომხმარებლის უნიკალური იდენტიფიცირებაა. შესაბამისად, ეს შემთხვევა GDPR-ის მე-9 მუხლის ფარგლებში მოექცევა.[44]

თუ მაღაზიის მფლობელმა, რეკლამის ინდივიდუალურ პირებზე მორგების მიზნით, მაღაზიის შიგნით სახის ამომცნობი სისტემა დააამონტაჟა, მან ამ ბიომეტრიული სისტემის გამოყენებამდე მონაცემთა სუბიექტების მკაფიო და ინფორმირებული თანხმობა უნდა მიიღოს. ეს სისტემა უკანონოდ ჩაითვლება, თუ ის ისეთ ვიზიტორს ან გამვლელს გადაიღებს, ვისაც თავისი ბიომეტრიული ნიმუშის შექმნაზე თანხმობა არ განუცხადებია, თუნდაც ის უმოკლეს ვადაში წაიშალოს.[45]

მულტიმოდალური ბიომეტრია[46] შეიძლება განიმარტოს, როგორც სხვადასხვა ბიომეტრიული ტექნოლოგიის კომბინაცია, რომელიც სისტემის მუშაობის სიზუსტეს აუმჯობესებს (მას ასევე მოიხსენიებენ, როგორც მრავალდონიან ბიომეტრიას). თანხვედრის პროცესში ბიომეტრიული სისტემები ერთი ინდივიდის ორ ან მეტ ბიომეტრიულ მახასიათებელს იყენებენ. ამ სისტემებს სხვადასხვანაირად ფუნქციონირება შეუძლიათ, მაგალითად, სხვადასხვა ბიომეტრიული მონაცემის სხვადასხვა სენსორით შეგროვება ან ერთი ბიომეტრიული მონაცემის სხვა ნაწილების/მახასიათებლების შეგროვება. ზოგიერთი კვლევა აჩვენებს, რომ არსებობს სისტემები, რომლებსაც ერთი ბიომეტრიული მონაცემის მრავალჯერადი წაკითხვა შეუძლია ან ისეთი სისტემები, რომლებიც სხვადასხვა ალგორითმს იყენებენ, რათა იგივე ბიომეტრიული მონაცემიდან სასურველი დამახასიათებელი შტრიხი ამოჭრან. მულტიმოდალურ სისტემებს შეუძლიათ მინიმუმამდე დაიყვანონ თაღლითობის საფრთხე და ხელი შეუწყონ მონაცემთა დაბალი ხარისხით ან დაკარგვით გამოწვეული სირთულეების გადალახვას, თუმცა ასევე წარმოშობენ ეთიკურ პრობლემებს, რამდენადაც ისინი საზოგადოების უფრო ეფექტური მეთვალყურეობის საშუალებას იძლევიან.[47]

2.3. ბიომეტრიული მონაცემების დამუშავებასთან დაკავშირებული რისკები და საფრთხეები

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებამ შეიძლება მოიტანოს მნიშვნელოვანი სარგებელი და ამავე დროს, საფრთხე შეუქმნას ადამიანის ძირითად უფლებებსა და თავისუფლებებს. ტექნოლოგიის სწრაფი განვითარება სენსიტიური მონაცემების დამუშავების მიმართულებით სერიოზულ რისკებს უკავშირდება.[48] ბიომეტრიული მონაცემი შესაძლოა ამჟღავნებდეს ადამიანის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციას ან მის რასობრივ ან

[44] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. პარ. 82, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[45] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. პარ. 83, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[46] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[47] Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, გვ.14. ხელმისაწვდომია: https://bit.ly/30QyFKd წვდომის თარიღი: 22.12.2021.

[48] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 370.

ეთნიკურ კუთვნილებას, ასევე შესაძლოა წარმოშვას ვინაობის მოპარვის რისკებიც.[49] შესაბამისად, ამგვარი მონაცემები გაძლიერებულ დაცვას საჭიროებს.[50]

მაგალითისთვის, სისტემა, რომელიც პიროვნების სახის გამოსახულებას ან მის დნმ-ს აანალიზებს, მნიშვნელოვნად უწყობს ხელს დანაშაულთან ბრძოლას და ეფექტიანად ამჟღავნებს დანაშაულის ჩამდენი სავარაუდო პირის ვინაობას. თუმცა, ამგვარი სისტემების ფართომასშტაბიან გამოყენებას გვერდითი ეფექტებიც აქვს. სახის ამომცნობი სისტემის ფართო გამოყენება, როდესაც ბიომეტრიული მონაცემები შესაძლოა მოპოვებულ იქნას მონაცემთა სუბიექტის ინფორმირების გარეშე, საჯარო სივრცეში ანონიმურობას სპობს და ინდივიდის მუდმივი თვალყურის დევნების შესაძლებლობას იძლევა.[51]

იმის გათვალისწინებით, რომ ბიომეტრიული ტექნოლოგიები სრულ სიზუსტეს ვერ უზრუნველყოფს, არსებობს არასწორი იდენტიფიცირების პოტენციური რისკიც. შედეგად, შესაძლოა მიღებულ იქნას იმგვარი გადაწყვეტილება, რაც გავლენას ახდენს ინდივიდუალურ უფლებებზე.[52] გარდა ამისა, ერთ-ერთი ყველაზე სერიოზული რისკი ბიომეტრიულ მონაცემთა ბაზის მოპარვა ან არაუფლებამოსილი პირ(ებ)ის მიერ მონაცემებზე წვდომის მოპოვებაა, რამაც შესაძლოა მნიშვნელოვანი ზიანი გამოიწვიოს.

პირადი ცხოვრების კუთხით არსებული საფრთხეების გარდა, არსებობს რისკები, რომლებიც დაკავშირებულია მოწყობილობების შესაძლო გაუმართაობასთან, ასევე ტენდენციურობასთან, რაც მათ შეიძლება გამოიწვიონ.[53] სახის ამოცნობის პროცესში ასაკის, სქესისა და ეთნიკური ნიშნით ტენდენციურობამ შესაძლოა საზოგადოებაში არსებული წინასწარ შექმნილი უარყოფითი განწყობები გააძლიეროს.[54]

აღსანიშნავია პროფილირების[55] საკითხიც, ავტომატიზებული გადაწყვეტილებების მიღების ან კონკრეტულ სიტუაციაში ადამიანის ქცევის პროგნოზირების კონტექსტში. ინდივიდის შესახებ ინფორმაცია შესაძლოა გამოყენებულ იქნას პროფილირების მიზნით, თუმცა ამავე დროს შეიძლება დისკრიმინაცია ან სტიგმატიზება გამოიწვიოს.[56]

---

[49] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 2.

[50] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 110-111, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[51] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[52] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[53] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. გვ.5, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 02.09.2021.

[54] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. გვ.6, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 02.09.2021.

[55] მონაცემთა დაცვის ზოგადი რეგულაციის მე-4 მუხლის მე-4 პუნქტის მიხედვით, პროფილირება ნიშნავს პერსონალური მონაცემების ნებისმიერი ავტომატური ფორმით დამუშავებას, რომელიც მოიცავს პერსონალური მონაცემების გამოყენებას ფიზიკურ პირთან დაკავშირებული გარკვეული პიროვნული მახასიათებლების შესაფასებლად, კერძოდ, იმ მახასიათებლების ანალიზსა და პროგნოზირებას, რომლებიც შეეხება ფიზიკური პირის მიერ სამუშაოს შესრულების ხარისხს, ეკონომიკურ მდგომარეობას, ჯანმრთელობას, პირად უპირატესობებს, ინტერესებს, სანდოობას, ქცევას, ადგილმდებარეობას ან გადაადგილებას.

[56] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

2.4. ბიომეტრიული მონაცემების დამუშავების სტანდარტები

ევროპის საბჭოს სამართლებრივი ჩარჩო განსაკუთრებული კატეგორიის მონაცემთა გამოყენებისათვის სათანადო დაცვის ზომების განსაზღვრას ეროვნულ კანონმდებლობას ანდობს.[57] ასეთ შემთხვევაში, დაცული უნდა იყოს მოდერნიზებული 108-ე კონვენციის მოთხოვნები. კერძოდ, ეროვნული კანონმდებლობით გათვალისწინებული უსაფრთხოების სათანადო ზომები კონვენციის სხვა დებულებებს უნდა შეესაბამებოდეს. რაც შეეხება ევროკავშირის სამართალს, მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლი განსაკუთრებული კატეგორიის მონაცემთა დამუშავების დეტალურ რეჟიმსა და კანონიერ საფუძვლებს განსაზღვრავს.[58]

2016/680 დირექტივის მიხედვით, პირის უნიკალური იდენტიფიცირებისთვის ბიომეტრიული მონაცემების დამუშავება დასაშვებია მხოლოდ მაშინ, როდესაც არსებობს ამის მკაცრი აუცილებლობა, უზრუნველყოფილია მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო გარანტიები და სახეზეა ერთ-ერთი შემდეგი შემთხვევა: ა) დამუშავება გათვალისწინებულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით; ბ) დამუშავება ემსახურება მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვას; გ) დამუშავება ეხება მონაცემებს, რომლებიც მონაცემთა სუბიექტმა აშკარად საჯარო გახადა.[59]

2.4.1. დამუშავების კანონიერების, სამართლიანობისა და გამჭვირვალობის პრინციპი

ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობა ადგენს პერსონალურ მონაცემთა დამუშავების კანონიერების, სამართლიანობისა და გამჭვირვალობის მოთხოვნას.[60]

მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, ბიომეტრიული მონაცემების დამუშავება საჭიროებს მონაცემთა სუბიექტის მკაფიო თანხმობას[61] ან სხვა კანონიერი საფუძვლის არსებობას. მაგალითად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება დასაშვებია, თუკი ეს აუცილებელია მნიშვნელოვანი საჯარო ინტერესიდან გამომდინარე, გათვალისწინებულია ევროპული ან ეროვნული კანონმდებლობით, რომელიც პროპორციულია, პატივს სცემს მონაცემთა დაცვის უფლებას და ითვალისწინებს სათანადო და კონკრეტულ ღონისძიებებს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და ინტერესების დასაცავად.[62]

რაც შეეხება სამართლიანი დამუშავების პრინციპს, ის ძირითადად, აწესრიგებს ურთიერთობას მონა-

[57] 108+ კონვენციის მე-6 მუხლი.

[58] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 181, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[59] 2016/680 დირექტივის მე-10 მუხლი.

[60] 108+ კონვენცია, მუხლი 5 (3); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ა). 2016/680 დირექტივა, პრეამბულის 26-ე პუნქტი და მე-4 მუხლის 1-ლი პუნქტის „ა“ ქვეპუნქტი.

[61] მონაცემთა დაცვის ზოგადი რეგულაცია, მე-9 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტი.

[62] მონაცემთა დაცვის ზოგადი რეგულაცია, მე-9 მუხლის მე-2 პუნქტის „ზ“ ქვეპუნქტი.

ცემთა დამმუშავებელსა და მონაცემთა სუბიექტს შორის და შეიძლება ითქვას, რომ უკავშირდება პერსონალურ მონაცემთა ეთიკური პრინციპებით დამუშავებას.[63] გამჭვირვალობის პრინციპი კი ადგენს მონაცემთა დამმუშავებლის ვალდებულებას, მიიღოს სათანადო ზომები მონაცემთა სუბიექტების ინფორმირებისათვის მათი მონაცემების გამოყენებაზე.[64]

ხშირ შემთხვევაში, როდესაც ბიომეტრიული მონაცემები მუშავდება ვალიდური ალტერნატივის გარეშე, როგორიც არის პაროლი ან გასატარებელი ბარათი, მონაცემთა სუბიექტის თანხმობა არ შეიძლება თავისუფლად გაცემულად ჩაითვალოს. მაგალითად, სისტემა, რომელიც მონაცემთა სუბიექტებს ხელს შეუშლის მათ გამოყენებაში (მაგალითად, მომხმარებლის ძალიან ბევრი დრო იკარგება ან ეს პროცესი ზედმეტად გართულებულია) არ შეიძლება ჩაითვალოს სათანადო ალტერნატივად და შედეგად, სახეზე არ იქნება ნამდვილი თანხმობა.[65]

თანხმობა ნამდვილია მხოლოდ მაშინ, როდესაც გაცემულია საკმარისი ინფორმაცია ბიომეტრიული მონაცემების გამოყენების შესახებ. რამდენადაც ბიომეტრიული მონაცემები შეიძლება გამოყენებულ იქნას, როგორც უნიკალური და უნივერსალური იდენტიფიკატორი, მკაფიო და მარტივად გასაგები ინფორმაციის მიწოდება იმის შესახებ, თუ როგორ გამოიყენება კონკრეტული მონაცემები, აუცილებელია მონაცემთა სამართლიანი დამუშავების უზრუნველსაყოფად. შესაბამისად, ეს არის ბიომეტრიული მონაცემების გამოყენებისთვის ვალიდური თანხმობის არსებითი წინაპირობა.[66]

როდესაც GDPR-ის მე-9 მუხლის შესაბამისად მონაცემთა დამუშავებისათვის სუბიექტის თანხმობა აუცილებელია, მონაცემთა დამმუშავებელი მის სერვისებზე წვდომის წინაპირობად ბიომეტრიული მონაცემების დამუშავებაზე თანხმობის გაცემას ვერ დააწესებს. სხვა სიტყვებით რომ ვთქვათ, ბიომეტრიული მონაცემების აუთენტიფიკაციის მიზნით დამუშავებისას, დამმუშავებელმა მონაცემთა სუბიექტს შეზღუდვების ან დამატებითი ხარჯის გარეშე უნდა შესთავაზოს ალტერნატიული გადაწყვეტა, რომელიც ბიომეტრიულ მონაცემთა დამუშავებას არ მოიცავს. ეს ალტერნატივა საჭიროა ასევე იმ პირთათვის, ვინც ვერ აკმაყოფილებს ბიომეტრიული მოწყობილობის მოთხოვნებს (ბიომეტრიული მონაცემების დატანა ან წაკითხვა შეუძლებელია, შეზღუდული შესაძლებლობის გამო რთულია მისი გამოყენება და ა. შ.).[67]

2.4.2. მიზნის შეზღუდვის პრინციპი

ბიომეტრიული მონაცემების გამოყენების აუცილებელი წინაპირობა იმ მიზნის მკაფიოდ და ნათლად განსაზღვრაა, რისთვისაც ისინი გროვდება და მუშავდება. მაგალითისთვის, ბიომეტრიული მონაცემები შეიძლება შეგროვდეს სისტემების უსაფრთხოების გასაზრდელად ან უზრუნველსაყოფად, არაავტორიზებული წვდომისგან პერსონალური მონაცემების დასაცავად სათანადო ზომების

[63] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 135-136, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[64] მონაცემთა დაცვის ზოგადი რეგულაცია, მე-12 მუხლი.

[65] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[66] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[67] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 86, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

მიღებით.[68]

მიზნის შეზღუდვა მონაცემთა დაცვის ევროპულ სამართალში ერთ-ერთი ფუნდამენტური პრინციპია. მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, მონაცემები უნდა შეგროვდეს კონკრეტული, მკაფიო და ლეგიტიმური მიზნით და დაუშვებელია მათი შემდგომი დამუშავება იმგვარად, რომ არ შეესაბამებოდეს დამუშავების თავდაპირველ მიზანს.[69] ანალოგიურ ჩანაწერს ითვალისწინებს მოდერნიზებული 108-ე კონვენციაც.[70] ორივე დოკუმენტი ითავლისწინებს გარკვეულ გამონაკლის შემთხვევებს, საჯარო ან სამეცნიერო/ისტორიული კვლევის ინტერესებიდან ან სტატისტიკური მიზნებიდან გამომდინარე.

ინტერნეტში, სოციალურ მედიაში ან აპლიკაციებში არსებული ფოტო არ შეიძლება შემდგომ დამუშავდეს ბიომეტრიული ნიმუშების მოსაპოვებლად ან ბიომეტრიულ სისტემებში განსათავსებლად, თუკი ამ ახალი მიზნისთვის კონკრეტული სამართლებრივი საფუძველი (მაგალითად, თანხმობა) სახეზე არ არის. მეორეული მიზნით დამუშავების სამართლებრივი საფუძვლის არსებობისას, დამუშავება უნდა იყოს ადეკვატური, რელევანტური და არ უნდა აჭარბებდეს დამუშავების მიზანს.[71]

მიზნის შეზღუდვის პრინციპს ითვალისწინებს 2016/680 დირექტივაც.[72] ამასთან, იმავე ან სხვა დამმუშავებლის მიერ თავდაპირველი მიზნისგან განსხვავებული, თუმცა ამ დირექტივის პირველი მუხლით გათვალისწინებული ერთ-ერთი მიზნით[73] მონაცემთა დამუშავება დასაშვებია, თუკი:

ა) ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით დამმუშავებელი უფლებამოსილია ამგვარი მონაცემები ამ მიზნით დაამუშავოს და

ბ) ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით ამგვარი დამუშავება აუცილებელი და ამ მიზნის პროპორციულია.[74]

მიზნის შეზღუდვის პრინციპი მჭიდროდ უკავშირდება გამჭვირვალობასა და განჭვრეტადობას: თუ დამუშავების მიზანი საკმარისად კონკრეტული და მკაფიოა, შესაბამის პირებს ექმნებათ წარმოდგენა, თუ რას უნდა ელოდონ. ამასთან, უმჯობესდება გამჭვირვალობისა და სამართლებრივი განჭვრეტადობის დონე. მეორე მხრივ, მიზნების მკაფიოდ განსაზღვრა მნიშვნელოვანია იმისთვის, რომ მონაცემთა სუბიექტებმა შეძლონ თავიანთი უფლებების ეფექტიანად განხორციელება (მაგალითად, დამუშავების შეწყვეტის მოთხოვნა).[75]

---

[68] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[69] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ბ).

[70] 108+ კონვენცია, მუხლი 5(4)(ბ).

[71] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[72] 2016/680 დირექტივა, მუხლი 4(1)(ბ).

[73] ეს მიზნებია: დანაშაულის პრევენცია, გამოძიება, გამოვლენა, სისხლისსამართლებრივი დევნა ან სასჯელის აღსრულება, მათ შორის საზოგადოებრივი უსაფრთხოების უზრუნველყოფა.

[74] 2016/680 დირექტივა, მუხლი 4(2).

[75] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 140, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021; ARTICLE 29 Data Protection Working Party, Opinion 3/2013 on purpose limitation, WP 203, 2 April 2013, ხელმისაწვდომია: https://bit.ly/32fLyhI წვდომის თარიღი: 21.07.2021.

პერსონალურ მონაცემთა დამუშავება კონკრეტული მიზნის გარეშე, მხოლოდ იმ გათვლით, რომ ეს მონაცემები შესაძლოა მომავალში სასარგებლო აღმოჩნდეს, კანონმდებლობის დარღვევაა. დამუშავების კანონიერება დამოკიდებულია მის მიზანზე, რომელიც უნდა იყოს მკაფიო, კონკრეტული და კანონის შესაბამისი.[76]

2.4.3. მონაცემთა მინიმიზაციის პრინციპი

მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რაც საჭიროა ლეგიტიმური მიზნის მისაღწევად და მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, სხვა საშუალებებით შეუძლებელია. მონაცემთა დამუშავება არ უნდა იყოს არაპროპორციული ჩარევა კონკრეტულ ინტერესებში, უფლებებსა და თავისუფლებებში.[77]

სირთულე შეიძლება წარმოიშვას მაშინ, როდესაც ბიომეტრიული მონაცემები შეიცავს იმაზე მეტ ინფორმაციას, ვიდრე ეს აუცილებელია შესაბამისობის დასადგენად. მონაცემთა დამმუშავებელმა უნდა იხელმძღვანელოს მონაცემთა მინიმიზაციის პრინციპით, რაც პირველ რიგში, გულისხმობს იმას, რომ მხოლოდ აუცილებელი ინფორმაციის დამუშავება, გადაცემა და შენახვა უნდა მოხდეს, ასევე კონფიგურაციამ პირველად პარამეტრად მონაცემთა დაცვა უნდა უზრუნველყოს.[78]

უნდა დამუშავდეს მხოლოდ ისეთი მონაცემები, რომლებიც „შესაბამისი და რელევანტურია, მოცულობა კი არ აჭარბებდეს მიზანს, რისთვისაც ისინი შეგროვდა და/ან დამუშავდა.“[79] დამუშავებისთვის შერჩეული მონაცემთა კატეგორიები საჭირო უნდა იყოს დამუშავების ოპერაციების გაცხადებული მიზნის მისაღწევად, ხოლო დამმუშავებელი მკაცრად შეიზღუდოს მხოლოდ იმ მონაცემთა შეგროვებით, რომლებიც პირდაპირ შეესაბამება კონკრეტულ მიზანს.[80]

2.4.4. მონაცემთა სიზუსტის პრინციპი

მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, პერსონალური მონაცემები უნდა იყოს ზუსტი და საჭიროებისამებრ განახლდეს. აუცილებელია ყველა გონივრული ზომის მიღება არაზუსტი პერსონალური მონაცემების დაუყოვნებლივ წასაშლელად ან შესასწორებლად მათი დამუშავების მიზნების გათვალისწინებით.[81] მონაცემთა სიზუსტის პრინციპს განამტკიცებს მოდერნიზებული 108-ე კონვენცია[82] და 2016/680 დირექტივაც.[83]

---

[76] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 140, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[77] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 143, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[78] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[79] 108+ კონვენცია, მუხლი 5 (4) (გ); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(გ). 2016/680 დირექტივა, მუხლი 4(1)(გ).

[80] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 143, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[81] მონაცემთა დაცვის ზოგადი რეგულაციის მე-5 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტი.

[82] 108+კონვენცია, მე-5 მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტი.

[83] 2016/680 დირექტივა, მუხლი 4(1)(დ).

2.4.5. ბიომეტრიულ მონაცემთა შენახვის ვადის შეზღუდვა

მონაცემთა დაცვის ზოგადი რეგულაციის, 2016/680 დირექტივისა და მოდერნიზებული 108-ე კონვენციის თანახმად, პერსონალური მონაცემები „უნდა შეინახონ ისეთი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას არაუმეტეს იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნებისთვის.“[84] პერსონალურ მონაცემთა დამუშავება განუსაზღვრელი ან/და შეუზღუდავი ვადით კანონდარღვევაა.[85]

მონაცემთა დამმუშავებელმა უნდა განსაზღვროს ბიომეტრიულ მონაცემთა შენახვის ვადა, რაც არ უნდა აღემატებოდეს იმ ვადას, რაც აუცილებელია იმ მიზნის მისაღწევად, რისთვისაც მონაცემები შეგროვდა და მუშავდება. დამმუშავებელმა უნდა უზრუნველყოს, რომ მონაცემები ან ამ მონაცემებიდან მიღებული პროფილები ამ ვადის გასვლის შემდეგ სამუდამოდ წაიშალოს.[86]

მაგალითად: დამსაქმებელი იყენებს ბიომეტრიულ სისტემას შეზღუდულ არეალში პირთა დაშვების კონტროლისთვის. დასაქმებულის როლი აღარ ითვალისწინებს მის დაშვებას ამ არეალში (სამსახურის ან პასუხისმგებლობების ცვლილების გამო). ასეთ შემთხვევაში, ბიომეტრიული მონაცემები უნდა წაიშალოს, რადგან მიზანი, რისთვისაც ისინი შეგროვდა, აღარ არსებობს.[87]

2.4.6. ბიომეტრიული მონაცემების უსაფრთხოების უზრუნველყოფა

ბიომეტრიულ მონაცემებთან მიმართებით უპირველესი საზრუნავი მათი უსაფრთხოება უნდა იყოს, რადგან საქმე ეხება შეუცვლელ მონაცემებს. ბიომეტრიული მონაცემების ერთხელ გამჟღავნებით საფრთხე ექმნება იდენტიფიკატორად მათ შემდგომ გამოყენებას და შესაბამისი პირების მონაცემთა დაცვას. ამგვარი დარღვევის შედეგების შემსუბუქების შესაძლებლობა არ არსებობს.[88] რისკები იზრდება იმ აპლიკაციების რაოდენობასთან ერთად, რომლებიც იდენტიფიკაციისათვის ბიომეტრიულ მონაცემებს იყენებენ. რაც უფრო მეტად გამოიყენება ამგვარი მონაცემები, მით უფრო მაღალია ქურდობის გზით მათი მოპოვების ალბათობა.[89]

იმის გათვალისწინებით, რომ ბიომეტრიული ტექნოლოგიით აუთენტიფიკაცია ბევრ სხვადასხვა ანგარიშზე ერთი და იმავე პაროლის გამოყენებას ჰგავს, რომლის შეცვლაც შეუძლებელია (სახის გამოსახულება, ანაბეჭდი და აშ.), მონაცემთა უსაფრთხოების ერთხელ დარღვევა სერიოზულ რისკს წარმოადგენს, რადგან მონაცემთა დამმუშავებელი შეძლებს სხვა ამ ტიპის აუთენტიფიკაციის მქონე სისტემებში შეღწევას.[90] შეიძლება ითქვას, რომ მსგავსი მაგალითები უკვე მრავლად არის.[91]

---

[84] მონაცემთა დაცვის ზოგადი რეგულაციის მე-5 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტი. 108+ კონვენციის მე-5 მუხლის მე-4 პუნქტის „ე“ ქვეპუნქტი. 2016/680 დირექტივის მე-4 მუხლის 1 პუნქტის „ე“ ქვეპუნქტი.

[85] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 140, ხელმისაწვდომია: https://bit.ly/3Bt94Em წვდომის თარიღი: 21.07.2021.

[86] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[87] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[88] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[89] Opinion 3/2012 on developments in biometric technologies, ხელმისაწვდომია: https://bit.ly/2W6MtgT წვდომის თარიღი: 21.07.2021.

[90] EDPS and AEPD Joint Paper, 14 Misunderstandings with Regard to Identification and Authentication, June 2020.

[91] დამატებით იხ. სტატია, ხელმისაწვდომია: https://bit.ly/2WzlFqi წვდომის თარიღი: 31.08.2021.

მონაცემთა უსაფრთხოების პრინციპი მოითხოვს სათანადო ტექნიკური ან ორგანიზაციული ღონისძიებების გატარებას პერსონალურ მონაცემთა დამუშავების პროცესში, რათა ისინი დაცული იყოს შემთხვევითი, არაავტორიზებული ან უკანონო წვდომის, გამოყენების, შეცვლის, გამჟღავნების, განადგურების ან დაზიანებისაგან.[92] უახლესი ტექნოლოგიების, დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების, ასევე მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დარღვევის სავარაუდო რისკების გათვალისწინებით, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები.[93]

მონაცემთა უსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას ("privacy by design") და მონაცემთა დაცვა პირველად პარამეტრად ("privacy by default"). მონაცემთა დამმუშავებელმა უნდა უზრუნველყოს ისეთი ტექნიკური და ორგანიზაციული ზომების გატარება, რომ ავტომატურად დამუშავდეს მხოლოდ ის მონაცემები, რომლებიც დამუშავების კონკრეტული მიზნისთვის აუცილებელია. ეს ვალდებულება ვრცელდება შეგროვებული მონაცემების რაოდენობაზე, მონაცემთა დამუშავების მასშტაბებზე, შენახვის ვადებსა და წვდომაზე.[94]

მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, თუ მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების კონტექსტისა და მიზნების გათვალისწინებით, განსაკუთრებით კი ახალი ტექნოლოგიების გამოყენებით, ადამიანის უფლებებისა და თავისუფლებების დარღვევის მაღალი რისკი იქმნება, მონაცემთა დამმუშავებელი ვალდებულია წინასწარ განახორციელოს მონაცემთა დამუშავების გავლენის შეფასება.[95] ანალოგიურ ჩანაწერს ითვალისწინებს 2016/680 დირექტივაც.[96]

GDPR-ის თანახმად, მონაცემთა დამუშავების გავლენის შეფასება სავალდებულოა განსაკუთრებით მაშინ, როდესაც მონაცემების ავტომატური დამუშავების, მათ შორის პროფილირების საფუძველზე, მონაცემთა სუბიექტისათვის სამართლებრივი შედეგის ან სხვა მხრივ მნიშვნელოვანი გავლენის მქონე გადაწყვეტილება მიიღება; საჯარო სივრცეში ხორციელდება სისტემატური და მასშტაბური მონიტორინგი; ასევე მაშინ, როდესაც დიდი რაოდენობით განსაკუთრებული კატეგორიის მონაცემები მუშავდება.[97]

იდენტიფიკაცია და აუთენტიფიკაცია/ვერიფიკაცია უმეტესად მოითხოვს ნიმუშის შენახვას, რათა ის შემდგომ შესადარებლად გამოუყენონ. მონაცემთა დამმუშავებელმა მონაცემთა შენახვის ყველაზე შესაფერისი ადგილი უნდა შეარჩიოს.[98] კონტროლის ქვეშ მყოფ გარემოში (შემოსაზღვრული დერეფნები ან გამშვები პუნქტები), ნიმუში უნდა ინახებოდეს ინდივიდუალურ მოწყობილობაზე, რომელზე კონტროლიც მხოლოდ მომხმარებელს აქვს და ის მასთან ინახება (სმარტფონში ან პირადობის მოწმობის ბარათში) ან კონკრეტული მიზნებისთვის ობიექტური საჭიროების არსებობისას, მათი

[92] მონაცემთა დაცვის ზოგადი რეგულაციის მე-5 მუხლის 1-ლი პუნქტის „ვ" ქვეპუნქტი. 108+ კონვენციის მე-7 მუხლი. 2016/680 დირექტივის მე-4 მუხლის 1-ლი პუნქტის „ვ" ქვეპუნქტი.

[93] მონაცემთა დაცვის ზოგადი რეგულაციის 32-ე მუხლის 1-ლი პუნქტი.

[94] მონაცემთა დაცვის ზოგადი რეგულაციის 25-ე მუხლის მე-2 პუნქტი.

[95] მონაცემთა დაცვის ზოგადი რეგულაციის 35-ე მუხლი.

[96] 2016/680 დირექტივის 27-ე მუხლი.

[97] იქვე, 35-ე მუხლის მე-3 პუნქტი.

[98] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 88, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

შენახვა შეიძლება ცენტრალიზებულ მონაცემთა ბაზაში დაშიფრული სახით, რომლის გასაღები/კოდი ნიმუშზე უნებართვო წვდომის თავიდან ასაცილებლად მხოლოდ ამ პირის ხელში უნდა იყოს. თუ მონაცემთა დამმუშავებელს არ შეუძლია თავიდან აიცილოს ნიმუშზე წვდომა, მან უნდა მიიღოს შესაბამისი ზომები შენახული მონაცემების უსაფრთხოების უზრუნველსაყოფად. ეს შეიძლება გულისხმობდეს შაბლონის დაშიფვრას კრიპტოგრაფიული ალგორითმის გამოყენებით.[99]

ნებისმიერ შემთხვევაში, დამმუშავებელმა უნდა მიიღოს ყველა აუცილებელი ზომა, რათა შეინარჩუნოს დამუშავებული მონაცემების გამოსადეგობა, მთლიანობა და კონფიდენციალურობა. ამ მიზნით, დამმუშავებელმა უნდა გაატაროს შემდეგი ღონისძიებები: მოახდინოს მონაცემთა კატეგორიზაცია მათი შენახვისას და გადაცემისას, სხვადასხვა ბაზაში შეინახოს ბიომეტრიული ნიმუშები და ნედლი მონაცემები ან პირის ვინაობასთან დაკავშირებული მონაცემები, დაშიფროს ბიომეტრიული მონაცემები, განსაკუთრებით ბიომეტრიული ნიმუშები, განსაზღვროს მათი დაშიფვრისა და ძირითადი მართვის პოლიტიკა, დანერგოს თაღლითობის გამოვლენის ორგანიზაციული და ტექნიკური ზომები, მონაცემებთან დააკავშიროს კოდი (მაგალითად, ხელმოწერა) და აკრძალოს ყოველგვარი გარე წვდომა ბიომეტრიულ მონაცემებზე. ეს ღონისძიებები საჭიროებს ტექნოლოგიის განვითარების კვალდაკვალ განახლებას.[100]

გარდა ამისა, თუ დამუშავების კანონიერი საფუძველი აღარ არსებობს, ნედლი მონაცემები უნდა წაიშალოს.[101] იმდენად, რამდენადაც ბიომეტრიული ნიმუშები ასეთი მონაცემებიდან მიიღება, მონაცემთა ბაზების შექმნა შეიძლება დიდი საფრთხე იყოს. ბიომეტრიული ნიმუშის წაკითხვა ყოველთვის ადვილი არ არის, თუ პირმა არ იცის, როგორ მოხდა მისი დაპროგრამება, ხოლო ნედლი მონაცემები ნებისმიერი ნიმუშის „სამშენებლო მასალაა". დამმუშავებელმა უნდა წაშალოს ბიომეტრიული მონაცემები და ნიმუშები წაკითხვის/შედარების ტერმინალზე ან შენახვის სერვერზე არაავტორიზებული წვდომის შემთხვევაში, ასევე წაშალოს ნებისმიერი მონაცემი, რომელიც შემდგომი დამუშავებისთვის სასარგებლო არ არის.[102]

მოდერნიზებული 108-ე კონვენცია, 2016/680 დირექტივა და GDPR მონაცემთა დამმუშავებელს უწესებს მოთხოვნას, რომ უფლებამოსილ საზედამხედველო ორგანოს შეატყობინოს მონაცემთა უსაფრთხოების ისეთი დარღვევის შესახებ, რომელმაც შეიძლება შელახოს ფიზიკურ პირთა უფლებები და თავისუფლებები.[103] შეტყობინების ვალდებულება დაწესებულია მონაცემთა სუბიექტთან დაკავშირებითაც, თუკი პერსონალურ მონაცემთა უსაფრთხოების დარღვევა, სავარაუდოდ, მაღალ რისკს შეუქმნის მის უფლებებსა და თავისუფლებებს.[104]

---

[99] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 88, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[100] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 89, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[101] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 90, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[102] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 90, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

[103] 108+ კონვენცია, მუხლი 7(2); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 33 (1). 2016/680 დირექტივა, მუხლი 30(1).

[104] 108+ კონვენცია, მუხლი 7 (2); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 34 (1). 2016/680 დირექტივის 31-ე მუხლი.

2.4.7. ანგარიშვალდებულების პრინციპი

ანგარიშვალდებულება მოითხოვს მონაცემთა დამმუშავებლის მიერ იმ ზომების აქტიურად და მუდმივად გატარებას, რომლებიც ხელს შეუწყობს და განამტკიცებს მონაცემთა დაცვას დამუშავების პროცესში.[105] ეს პრინციპი ასახულია GDPR-ში[106], 2016/680 დირექტივასა[107] და მოდერნიზებულ 108-ე კონვენციაში.[108]

29-ე მუხლის სამუშაო ჯგუფის მოსაზრებით, ანგარიშვალდებულების არსი განისაზღვრება მონაცემთა დამმუშავებლის მოვალეობით:

- გაატაროს ღონისძიებები, რომლებიც, ჩვეულებრივ პირობებში, უზრუნველყოფს მონაცემთა დაცვის წესების შესრულებას დამუშავების ოპერაციების კონტექსტში; და
- მზად იქონიოს დოკუმენტაცია, რომელიც მონაცემთა სუბიექტებსა და საზედამხედველო ორგანოებს დაუდასტურებს, რომ გატარდა ღონისძიებები მონაცემთა დაცვის წესების შესასრულებლად.[109]

2.5. მონაცემების დამუშავება ცალსახად პირადი ან საოჯახო საქმიანობის ფარგლებში

მონაცემების ცალსახად პირადი ან საოჯახო საქმიანობის ფარგლებში დამუშავებისას, კერძო პირზე არ ვრცელდება GDPR-ითა და მოდერნიზებული 108-ე კონვენციით გათვალისწინებული წესები და ის მონაცემთა დამმუშავებლად არ მიიჩნევა.[110]

მონაცემების ამგვარი დამუშავების მაგალითია, როდესაც მესაკუთრე ბიომეტრიულ სისტემას იყენებს კერძო სახლში მისი, ოჯახის წევრებისა და სავარაუდო მესამე პირების შესვლის კონტროლისთვის. ასეთ შემთხვევაში, მონაცემთა დამუშავების საშუალებასა (სისტემის შერჩევა) და მიზნებს ქონების მესაკუთრე განსაზღვრავს. თუმცა, თუ ბიომეტრიული სისტემა ცენტრალურ მოწყობილობას უკავშირდება, რომელსაც უსაფრთხოების სამსახურები მართავენ, გადაწყვეტილებას იღებს არა მხოლოდ მესაკუთრე, არამედ ასევე მესამე პირებიც.[111] შესაბამისად, ამგვარი შემთხვევა არ ჩაითვლება ცალსახად პირადი ან საოჯახო საქმიანობის ფარგლებში მონაცემთა დამუშავებად და მასზე გავრცელდება მონაცემთა დაცვის წესები.

---

[105] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 152.

[106] მონაცემთა დაცვის ზოგადი რეგულაცია, მე-5 მუხლის მე-2 პუნქტი.

[107] 2016/680 დირექტივა, მუხლი 4(4).

[108] 108+ კონვენცია, მე-10 მუხლის პირველი პუნქტი.

[109] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 155.
ARTICLE 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability, ხელმისაწვდომია: https://bit.ly/3wLR46j წვდომის თარიღი: 13.11.2021.

[110] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 18 და მუხლი 2(2)(გ); 108+ კონვენცია, მუხლი 3 (2).

[111] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 120.

როდესაც ბიომეტრიული სისტემა ინსტალირებულია მანქანაში, რომელსაც პირადი საქმიანობის ფარგლებში ექსკლუზიურად ფლობს და იყენებს ფიზიკური პირი, ბიომეტრიული მონაცემების შეგროვება და გამოყენება ზემოაღნიშნულ გამონაკლისს განეკუთვნება. თუმცა, თუ კონტროლის ბიომეტრიული სისტემით აღჭურვილ ავტომობილებს კომპანია ფლობს და მათ დასაქმებულებს გადასცემს, ეს გამონაკლისი არ გავრცელდება. ანალოგიურად, როდესაც თითის ანაბეჭდის სისტემა ჩაშენებულია პირად ლეპტოპში ან მობილურ ტელეფონში, ეს გამონაკლის შემთხვევად განიხილება. თუმცა, თუ ამგვარ ლეპტოპს ან მობილურ ტელეფონს დამსაქმებელი გადასცემს დასაქმებულს, ეს არ ჩაითვლება პირადი ან საოჯახო საქმიანობის ფარგლებში გამოყენებად[112] და მასზე მონაცემთა დაცვის წესები სრულად გავრცელდება.

[112] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, გვ. 120-121.

3. გენეტიკური მონაცემების დამუშავება

3.1. გენეტიკური მონაცემების ცნება

სამედიცინო მონაცემების დაცვის შესახებ ევროპის საბჭოს 1997 წლის N° R(97)5 რეკომენდაცია[113] გენეტიკურ მონაცემებს შემდეგნაირად განმარტავდა: *„ნებისმიერი მონაცემი, ჰომეღიც პიჰის მემკვიდჩეობით მახასიათებლებს ან პიჰთა მონათესავე ჯგუფში ამგვაჩი მახასიათებლების მემკვიდჩეობით გადაცემის შედეგად მიღებუღ სახესხვაობას შეეხება.“*

29-ე მუხლის სამუშაო ჯგუფმა 2004 წელს მიიღო დოკუმენტი,[114] სადაც გენეტიკური მონაცემების ძირითადი მახასიათებლები ჩამოაყალიბა და მათი სამართლებრივი დაცვის განსაკუთებულ მნიშვნელობას გაუსვა ხაზი. იმ დროს მოქმედი პერსონალურ მონაცემთა დაცვის 95/46 დირექტივა[115] გენეტიკურ მონაცემებს არ ახსენებდა და მას სხვა მონაცემებისგან არ განაცალკევებდა.[116] მოგვიანებით, გენეტიკური მონაცემები განსაკუთრებული კატეგორიის მონაცემებს შორის აისახა ევროკავშირის მონაცემთა დაცვის ზოგად რეგულაციაში, რომელიც ძალაში 2018 წელს შევიდა და ზემოხსენებული დირექტივა ჩაანაცვლა. მოდერნიზებული 108-ე კონვენციაც გენეტიკურ მონაცემებს განსაკუთრებულ კატეგორიას მიაკუთვნებს.[117]

მონაცემთა დაცვის ზოგად რეგულაციაში გენეტიკური მონაცემების განმარტება არა მხოლოდ მემკვიდრეობით, არამედ შეძენილ გენეტიკურ მახასიათებლებსაც მოიცავს. კერძოდ, რეგულაციის მე-4 მუხლის თანახმად, გენეტიკურ მონაცემებს წარმოადგენს ფიზიკური პირის მემკვიდრეობით მიღებულ ან შეძენილ გენეტიკურ მახასიათებლებთან დაკავშირებული პერსონალური მონაცემები, რომლებიც პირის ფიზიოლოგიის ან ჯანმრთელობის შესახებ უნიკალურ ინფორმაციას იძლევა და ფიზიკური პირისგან აღებული ბიოლოგიური ნიმუშის ანალიზის შედეგად მიიღება.[118] რეგულაციის პრეამბულის თანახმად, გენეტიკური მონაცემი მიიღება ბიოლოგიური ნიმუშის, კერძოდ, ქრომოსომული, დეზოქსირიბონუკლეინის მჟავის (DNA) და რიბონუკლეინის მჟავის (RNA) ანალიზის ან სხვა ელემენტის ანალიზის შედეგად, რომლებიც იმავე ინფორმაციის მიღების შესაძლებლობას იძლევა.[119]

გენეტიკური მონაცემების ამგვარი განმარტება დეტალურია, თუმცა ზოგად ტერმინებს ეფუძნება, რათა ტექნოლოგიური განვითარების პირობებში არ მოძველდეს და მოქნილობა შეინარჩუნოს. ვინაიდან სახის ამსახველი სურათის ანალიზის საფუძველზე კომპიუტერული გამოსახულებისა და ღრმა სწავლების ალგორითმების გამოყენებით გენეტიკური დარღვევების დიაგნოზირება უკვე შესაძლებელი გახდა, მე-4 მუხლში მოცემული განმარტების ბოლო წინადადება, რომელიც გენეტიკურ მონაცემებად მხოლოდ ფიზიკური პირის ბიოლოგიური ნიმუშის ანალიზის შედეგად მიღებულ

---

[113] ხელმისაწვდომია: https://bit.ly/3wswqIl წვდომის თარიღი: 09.11.2021.

[114] ხელმისაწვდომია: https://bit.ly/3bTFsVd წვდომის თარიღი: 09.11.2021.

[115] ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ.

[116] განსაკუთრებულ კატეგორიას მიეკუთვნებოდა ჯანმრთელობის შესახებ მონაცემები, რომელიც გენეტიკურ მონაცემებს მნიშვნელოვანწილად ფარავს, თუმცა ეს უკანასკნელი გარკვეული ასპექტებით და მისთვის დამახასიათებელი თავისებურებებიდან გამომდინარე, ჯანმრთელობის შესახებ მონაცემებისგან მაინც განსხვავდება (მაგალითად, მომავალში მისი მნიშვნელობის თვალსაზრისით).

[117] 108+ კონვენცია, მუხლი 6 (1).

[118] მონაცემთა დაცვის ზოგადი რეგულაციის მე-4 მუხლის მე-13 პუნქტი.

[119] მონაცემთა დაცვის ზოგადი რეგულაციის პრეამბულის 34-ე პუნქტი.

პერსონალურ მონაცემებს განსაზღვრავს, ზუსტი არ არის.[120] ამ შემთხვევაში, მე-4 მუხლის უფრო ფართოდ გამოყენების საშუალებას პრეამბულის 34-ე პუნქტი უზრუნველყოფს, რომლის თანახმად, გენეტიკური მონაცემები ასევე სხვა ელემენტის ანალიზის შედეგად მიიღება.[121]

გენეტიკურ მონაცემებს მონაცემთა დაცვის ზოგადი რეგულაციის მსგავსად განმარტავს[122] ევრო-კავშირის 2016/680 დირექტივა, რომელიც სამართალდამცავი ორგანოების მიერ პერსონალური მონაცემების დამუშავებას შეეხება.

29-ე მუხლის სამუშაო ჯგუფმა გენეტიკური მონაცემების სპეციალური მახასიათებლების განსაზღვრისას შემდეგი მნიშვნელოვანი თავისებურებები გამოყო:

- თითოეული პირის გენეტიკური მონაცემი უნიკალურია და ერთი ინდივიდის მეორისგან გარჩევის შესაძლებლობას იძლევა;
- ის ადამიანის ბიოლოგიური ოჯახის წევრების შესახებ ინფორმაციას ამჟღავნებს (როგორც აღმავალი, ისე დაღმავალი შტო);
- გენეტიკურ მონაცემებს შეუძლია პირთა ჯგუფების განსხვავება (მაგალითად, ეთნიკური ჯგუფები);
- გენეტიკური ინფორმაცია მისი მატარებლისთვის უცნობია და მისი ცვლილება შეუძლებელია;
- გენეტიკური მონაცემების დაუმუშავებელი მასალიდან მიღება და მოპოვება ადვილია, თუმცა ეს მონაცემები შესაძლოა ზოგჯერ სანდო არ იყოს.[123]

ამ განმარტების ზოგიერთი ნაწილი ზუსტი არ არის. განაცხადი, რომ გენეტიკური ინფორმაცია უნიკალურია, რამდენადმე აკნინებს იმ ფაქტს, რომ ადამიანის გენების დიდი უმრავლესობა იდენტურია, განსხვავება მხოლოდ მცირედ ნაწილშია. თუმცა, ის ერთი ადამიანის მეორესგან გამოსარჩევად სრულიად საკმარისია. ასევე, გენეტიკური მონაცემის არაცვალებად ხასიათზე მითითება ყურადღების მიღმა ტოვებს გენომში ცვლილებების შეტანის მიმართულებით ბოლოდროინდელ პროგრესს და იმ ფაქტს, რომ დაავადებებს და მათ მკურნალობას ხშირად დნმ-ის მახასიათებლების შეცვლა შეუძლია.[124]

---

[120] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 201.

[121] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 201.

[122] 2016/680 დირექტივის პრეამბულის 23-ე პუნქტი, მე-3 მუხლის მე-12 პუნქტი.

[123] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004, გვ 4-5, ხელმისაწვდომია: https://bit.ly/3yRs26O ნვდომის თარიღი: 18.10.2021

[124] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, გვ. 198.

ჯანმრთელობასთან დაკავშირებული მონაცემების შესახებ ევროპის საბჭოს რეკომენდაციისა[125] და მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათის[126] თანახმად, გენეტიკური მონაცემები პირის მემკვიდრეობით ან პრენატალური[127] განვითარების ეტაპზე მიღებულ გენეტიკურ მახასიათებლებს უკავშირდება. აღსანიშნავია, რომ მონაცემთა დაცვის ზოგად რეგულაციაში გენეტიკური მონაცემების განსაზღვრების შემუშავებისას, პრენატალური განვითარების ეტაპზე მიღებული გენეტიკური მახასიათებლების ნაცვლად, შეძენილი გენეტიკური მახასიათებლები შეირჩა სწორედ იმ მიზეზით, რომ დაბადების შემდგომ გენეტიკური მონაცემების ცვლილება შესაძლებელია.[128]

მონაცემთა დაცვის ზოგადი რეგულაციით განსაზღვრული გენეტიკური მონაცემი მოიცავს ინდივიდის მხოლოდ იმ გენეტიკურ მახასიათებლებს, რომლებიც პირის ჯანმრთელობასა და ფიზიოლოგიაზე უნიკალურ ინფორმაციას იძლევა. შესაბამისად, განსაზღვრების ქვეშ ბიოლოგიური ნიმუშის ანალიზიდან მიღებული ყველა ტიპის ინფორმაცია არ ხვდება. დეფინიციის ქვეშ შესაძლოა არ მოექცეს ადამიანის ფენოტიპური მახასიათებლები (მაგალითად, თმის ან თვალის ფერი) ან მახასიათებლები, რომლებიც ჯანმრთელობის მდგომარეობის გათვალისწინებით ან ფიზიოლოგიურად ერთ ინდივიდს მეორესგან გამოარჩევს.[129]

ფიზიოლოგიური მახასიათებლები ექცევა თუ არა გენეტიკური მონაცემების დეფინიციის ქვეშ მთლიანად არის დამოკიდებული იმაზე, თუ როგორ განიმარტება „გენეტიკური მახასიათებლები," რომელიც ძირითადად გაიგივებულია ტერმინთან „გენეტიკური მემკვიდრეობა" და ის ჩვეულებრივ ინდივიდის ქრომოსომებსა და გენს მიემართება.[130] მხოლოდ ფენოტიპური მახასიათებლების შესახებ არსებული მონაცემების დამუშავება (მაგალითად, პირისთვის სურათის გადაღება ან შენახვა) ჩვეულებრივ მონაცემთა დაცვის რეგულაციით განსაზღვრული გენეტიკური მონაცემების დამუშავების ქვეშ არ ექცევა. ამას ასევე ადასტურებს ამ რეგულაციის პრეამბულის 51-ე პუნქტი, რომლის მიხედვით ფოტოსურათის დამუშავება შეიძლება არ ჩაითვალოს განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავებად.[131] ამასთან, თავად ბიოლოგიური ნიმუში, რომლიდანაც გენეტიკური მონაცემები მიიღება, პერსონალურ მონაცემებს არ წარმოდგენს.[132]

ზოგადად, გენეტიკური და ჯანმრთელობასთან დაკავშირებული მონაცემები ერთმანეთს მნიშვნელოვნად ფარავს, თუმცა განსხვავება მდგომარეობს იმაში, რომ გენეტიკური ინფორმაცია შეიძლება პირის ჯანმრთელობის მომავალ მდგომარეობას შეეხებოდეს. გენეტიკური მონაცემების განსაკუთრებულ თავისებურებას წარმოადგენს ასევე ის ფაქტი, რომ ეს მონაცემები შეიძლება მონაცემთა სუბიექტის მთელი ოჯახისა და მისი შთამომავლობის შესახებ ინფორმაციას ამჟღავნებდეს. სწორედ ამ მახასიათებლების გამო იქცა გენეტიკური მონაცემები დროთა განმავლობაში ცალკე დაცვის საგნად.

---

[125] ხელმისაწვდომია: https://bit.ly/3D7TQW0 წვდომის თარიღი: 09.11.2021.

[126] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პარ. 57, ხელმისაწვდომია: https://bit.ly/3oi32B4 წვდომის თარიღი: 09.11.2021.

[127] გ. გოგიჩაძე, ა. გედენიძე, ჯ. ჭუმბურიძე, ნაყოფის დაბადების წინა პერიოდი, სამედიცინო ტერმინოლოგიის ქართულ-ინგლისურ-რუსულ-ლათინური განმარტებითი ლექსიკონი, თბილისი, 2009, გვ. 496.

[128] Lee A. Bygrave, Luca Tosoni, Genetic Data, The EU General Data Protection Regulation, A Commentary, Oxford University Press, 2020, გვ. 199.

[129] იქვე, გვ 202.

[130] იქვე, გვ. 203.

[131] იქვე.

[132] იქვე, გვ. 202.

3.2. გენეტიკური მონაცემების გამოყენების არეალი, მათ დამუშავებასთან დაკავშირებული რისკები და საფრთხეები

გენეტიკური მონაცემების გამოყენების არეალი საკმაოდ ფართოა და ტექნოლოგიურ პროგრესთან ერთად უფრო და უფრო იზრდება. გენეტიკური მონაცემები პირის შესახებ უამრავ ინფორმაციას ამჟღავნებს, მათ შორის, პირის გენეტიკური დაავადებისადმი მიდრეკილებას, რაც იშვიათი გენეტიკური დაავადებების შესახებ კვლევებსა და მათი მკურნალობის გზების პოვნაში დიდ როლს ასრულებს.[133] კვლევითი საქმიანობის გარდა, გენეტიკური მონაცემების გამოყენება ჯანდაცვის სფეროში განუზომლად დიდი მნიშვნელობის არის: შესაძლებელია ცალკეულ დაავადებათა პრევენციის, დიაგნოზირებისა და მკურნალობის გაუმჯობესება, ზოგიერთი წამლის გვერდით ეფექტებთან დაკავშირებული რისკების იდენტიფიცირება და ორგანიზმზე საზიანო გავლენების პრევენცია.[134]

გენეტიკური მონაცემები ასევე გამოიყენება სისხლის სამართლის საქმის გამოძიებისას (მაგალითად, დამნაშავის იდენტიფიცირებისთვის), საოჯახო დავებში, როცა საქმე ეხება შვილად აყვანას, მამობის/დედობის დადგენას ან მეურვეობასა და მზრუნველობასთან დაკავშირებულ დავებს. სახელმწიფოები გენეტიკურ მონაცემებს იმიგრაციის საკითხებში ოჯახის გაერთიანებასთან დაკავშირებულ საქმეებზე ნათესაური კავშირის დასადასტურებლად იყენებენ.[135]

ამასთან, უძრავი ქონებისა და კომერციული ტრანზაქციების სფეროში გენეტიკური ნიშნით დისკრიმინაციის საფრთხეები უფრო და უფრო იზრდება. არსებობს რისკები, რომ სხვადასხვა კომპანიები, მაგალითად, ალცაიმერის დაავადების გენეტიკური განწყობის მქონე პირებს უარი ეტყვიან ქონების მიქირავებაზე ან უძრავი ქონების სანაცვლოდ თანხის გაცემაზე.[136]

პირთა დნმ-ის შესახებ ინფორმაცია არსებობს ეროვნულ მონაცემთა ბაზებშიც, რასაც უმეტესწილად სამართალდამცავი უწყებები, ხშირად, მოსამართლეთა კონტროლის ქვეშ აწარმოებენ. თავდაპირველად ამგვარი ბაზები იმ პირთა იდენტიფიცირების მიზნით შეიქმნა, რომლებსაც ბავშვთა მიმართ სექსუალური ხასიათის დანაშაული ჰქონდათ ჩადენილი. თუმცა, პირთა წრე ნელ-ნელა გაფართოვდა და ხშირად ამ ბაზებში ასახულია სხვა მძიმე, მათ შორის ტერორიზმთან, ხანდახან მსუბუქ დანაშაულთან შემხებლობაში მყოფ პირთა დნმ-ის შესახებ ინფორმაციაც.[137]

გენეტიკური მონაცემების დამუშავების მიზანი შეიძლება იყოს ასევე ჰუმანიტარული კრიზისის დროს ან ჰუმანიტარული საქმიანობის ფარგლებში მონაცემების დამუშავება, როდესაც სათანადო საკანონმდებლო გარანტიები არსებობს. ჰუმანიტარული კრიზისი გულისხმობს მოვლენებს, რომლებიც კრიტიკულ საფრთხეს უქმნის საზოგადოების ან მისი დიდი ნაწილის ჯანმრთელობას,

---

[133] John Paul M. Gaba, Joan Janneth M. Estremadura, Data Protection of Biometric Data and Genetic Data, Ateneo Law Journal 64, no. 3, February 2020, გვ. 967.

[134] Kristi Harbord, *Genetic data privacy solutions in the GDPR*, 7 Tex. A&M L. Rev. 269 (2019), გვ. 276.

[135] Ellen W. Clayton, Barbara J. Evans, James W. Hazel, Mark A. Rothstein, *The law of genetic privacy: applications, implications, and limitations,* Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, გვ. 22-24.

[136] იქვე, გვ. 26.

[137] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications,* Springer Dordrecht Heidelberg New York London, 2013, პარ. 371, გვ. 208.

უსაფრთხოებას ან კეთილდღეობას, რა დროსაც ჰუმანიტარულ ორგანიზაციებს ან სახელმწიფოს შეიძლება ესაჭიროებოდეს ოჯახური კავშირის აღდგენის ან ადამიანის ნეშტების იდენტიფიცირების მიზნით გენეტიკური მონაცემების დამუშავება.[138]

გენეტიკური მონაცემები გამოიყენება კერძო სექტორში, მაგალითად, კერძო კომპანიების მიერ მომხმარებელთა გენეტიკური ტესტირებისას. ამ შემთხვევაში, მომხმარებლები დნმ-ის ნიმუშებს პირდაპირ კომპანიებთან აგზავნიან, რომლებიც ვებგვერდის მეშვეობით ან წერილობითი სახით მათი გენეტიკური ინფორმაციის შესახებ ატყობინებენ. მომხმარებელმა გენეტიკური ტესტირებისთვის ამ ტიპის კერძო კომპანიებს სხვადასხვა მიზეზის გამო შეიძლება მიმართოს. ყველაზე ხშირად მოთხოვნა საკუთარი ჯანმრთელობის, წარმომავლობისა და გენეოლოგიის შესახებ ინფორმაციის გამოკვლევას უკავშირდება; ზოგიერთ ადამიანს სისხლით ნათესავების პოვნის იმედი ამოძრავებს ან შვილად აყვანილი ბავშვის ბიოლოგიური მშობლების გარკვევის სურვილი აქვს.[139]

გარდა ამისა, კერძო სექტორში გენეტიკური მონაცემების გამოყენება შესაძლებელია დასაქმებისა და დაზღვევის სფეროებში, რაც გენეტიკური ნიშნით დისკრიმინაციის სერიოზულ საფრთხეს ქმნის. ამ რისკებიდან გამომდინარე, დაზღვევის და დასაქმების შესახებ გადაწყვეტილების მიღების მიზნით გენეტიკური მონაცემების გამოყენება დაუშვებელია.

გენეტიკური მონაცემების დამუშავებისას მონაცემთა სუბიექტები სერიოზული საფრთხის წინაშე შეიძლება აღმოჩნდნენ, რაც სუბიექტის სათანადო დაცვის გარანტიებით აღჭურვას აუცილებელს ხდის. გენეტიკური ტექნოლოგიების სწრაფ განვითარებასთან, ამ პროცესში მიმდინარე ცვლილებებთან, გენეტიკური მონაცემების ანალიზის ფასის შემცირებასთან ერთად, გენომის სეკვენირება ჩვეულებრივი მოვლენა გახდა და დიდი მონაცემების ბაზების რაოდენობა იზრდება. ყოველივე ეს მეტყველებს იმაზე, რომ ტექნოლოგიების გამოყენება მონაცემთა დაცვის სფეროს მნიშვნელოვანი გამოწვევების წინაშე აყენებს და უწყვეტ მონიტორინგს საჭიროებს.[140]

[138] Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, პარ. 75.

[139] Ellen W. Clayton, Barbara J. Evans, James W. Hazel, Mark A. Rothstein, *The law of genetic privacy: applications, implications, and limitations*, Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, გვ. 16.

[140] Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, პარ. 69.

3.3. გენეტიკური ნიშნით დისკრიმინაციისა და სტიგმატიზაციის აკრძალვის პრინციპი

გენეტიკური მონაცემების დამუშავებისას დისკრიმინაციის ან/და სტიგმატიზაციის აკრძალვის პრინციპს არაერთი მნიშვნელოვანი საერთაშორისო სამართლებრივი დოკუმენტი განამტკიცებს. მონაცემთა დაცვის ზოგადი რეგულაციის პრეამბულა ყურადღებას ამახვილებს დისკრიმინაციის საფრთხეებზე.[141] მოდერნიზებული 108-ე კონვენცია განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას მხოლოდ კანონმდებლობით სათანადო გარანტიების არსებობისას უშვებს, რაც, თავის მხრივ, ადამიანის უფლებებისა და ძირითადი თავისუფლებების შელახვის, განსაკუთრებით კი *დისკრიმინაციის* რისკებისგან დაცვას უნდა უზრუნველყოფდეს.[142]

ადამიანის უფლებებისა და ბიომედიცინის შესახებ ევროპის საბჭოს კონვენცია არის პირველი საერთაშორისო დოკუმენტი, რომელიც ბიოლოგიური და სამედიცინო მიღწევების ბოროტად გამოყენების აკრძალვის გზით ადამიანის ღირსების, უფლებებისა და თავისუფლებების დასაცავად შეიქმნა. კონვენცია ადგენს, რომ საზოგადოებისა და მეცნიერების ინტერესებსა და ადამიანის კეთილდღეობასა და ინტერესებს შორის არჩევანი აუცილებლად ამ უკანასკნელის სასარგებლოდ უნდა გაკეთდეს. გენეტიკური ტესტირება, რომელიც გენეტიკური დაავადების ან ამ უკანასკნელისადმი წინასწარგანწყობის ან მიდრეკილების შესახებ ინფორმაციას ამჟღავნებს, შესაძლოა დისკრიმინაციისა და სელექციის საშუალება აღმოჩნდეს, რის გამოც კონვენცია ადამიანის გენომის საფუძველზე ნებისმიერი სახის დისკრიმინაციის აკრძალვის პრინციპს ადგენს.[143]

კონვენციის დამატებითი ოქმი, რომელიც მხოლოდ ჯანმრთელობის მიზნით ჩატარებულ გენეტიკურ ტესტირებებზე ვრცელდება, ასევე კრძალავს პირის ან პირთა ჯგუფის გენეტიკური ნიშნით დისკრიმინაციას და გენეტიკურ მახასიათებლებთან დაკავშირებული სტიგმატიზაციის თავიდან ასარიდებლად სათანადო ზომების მიღების აუცილებლობაზე მიუთითებს.[144] დამატებითი ოქმი სტიგმატიზაციასა და დისკრიმინაციას ერთმანეთისგან მიჯნავს. როგორც განმარტებით ბარათშია მითითებული, სტიგმატიზაცია აუცილებლად პირის უფლების რეალიზებას არ უკავშირდება და პირის ან პირთა ჯგუფის შესახებ გენეტიკური მახასიათებლებთან დაკავშირებით გავრცელებულ შეხედულებებს გულისხმობს. ეს შეხედულებები შესაძლოა სიმართლესაც ასახავდეს, თუმცა ისინი პირს ან პირთა ჯგუფს ნეგატიურ იარლიყს აკრავს. სტიგმატიზაციის თავიდან ასარიდებელი ზომები, რომლის გატარებასაც დამატებითი ოქმი სახელმწიფოებისგან მოითხოვს, შესაძლებელია იყოს საინფორმაციო ხასიათის კამპანიები, რომელიც ადამიანის გენეტიკისა და ამ მხრივ არსებული მიღწევების შესახებ ცოდნის გაღრმავებას ემსახურება.[145]

გენეტიკური ნიშნით დისკრიმინაციის განსაკუთრებული საფრთხეები შეიძლება წარმოიშვას დასაქმების ან დაზღვევის კონტექსტში. დასაქმებისას პერსონალურ მონაცემთა დამუშავების შესახებ ევროპის საბჭოს რეკომენდაცია ხაზგასმით მიუთითებს, რომ იმ შემთხვევაშიც კი, თუ არსებობს მონაცემთა სუბიექტის თანხმობა, დასაქმებულის ან კანდიდატის სამუშაო პოზიციასთან

[141] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 75 და 85.

[142] 108+ კონვენციის მე-6 მუხლი.

[143] ადამიანის უფლებებისა და ბიომედიცის შესახებ ევროპის საბჭოს კონვენციის მე-11 მუხლი.

[144] კონვენციის ჯანდაცვის მიზნებით ჩატარებული გენეტიკური ტესტირების შესახებ დამატებითი ოქმის მე-4 მუხლი.

[145] დამატებითი ოქმის განმარტებითი ბარათი, პარ. 42.

შესაბამისობის დადგენის მიზნით გენეტიკური მონაცემების დამუშავება დაუშვებელია.[146]

დასაქმების კონტექსტში გენეტიკური მონაცემების დამუშავება დასაშვებია კანონით გათვალისწინებულ შემთხვევებში მხოლოდ სათანადო გარანტიების არსებობისას. საგამონაკლისო შემთხვევებს წარმოადგენს, მაგალითად, გენეტიკური მონაცემების დამუშავება მონაცემთა სუბიექტის ან მესამე პირების ჯანმრთელობასთან დაკავშირებული ნებისმიერი წინასწარგანწყობის თავიდან არიდების მიზნით.[147] კიდევ ერთი მაგალითია გენეტიკური ინფორმაციის დამუშავება, როცა გენეტიკური მონიტორინგის პროგრამა სამუშაო ადგილზე ტოქსიკური ნივთიერებების ბიოლოგიურ ზემოქმედებას ამოწმებს, თუკი ამგვარი მონიტორინგის აუცილებლობა კანონით არის დადგენილი ან სათანადო, მკაფიოდ განსაზღვრული პირობების არსებობისას პროგრამაში მონაწილეობა მოხალისეობრივად შეიძლება.[148]

სადაზღვევო მიზნით გენეტიკური მონაცემების დამუშავებისას დისკრიმინაციას წარმოადგენს, მაგალითად, იმ პირთათვის უფრო მეტი სადაზღვევო გადასახადის დაკისრება, რომელთაც გარკვეული დაავადებების განვითარების მომეტებული რისკი აქვთ. სადაზღვევო პროცესში გენეტიკური დისკრიმინაციის თავიდან არიდებისათვის კონკრეტულ წესებს ადგენს სადაზღვევო მიზნებით პერსონალური მონაცემების დამუშავების შესახებ ევროპის საბჭოს რეკომენდაცია, რომლითაც იკრძალება პროგნოზული გენეტიკური ტესტის სადაზღვევო მიზნებით ჩატარება.[149]

გენეტიკური ტესტებიდან მიღებული უკვე არსებული პროგნოზული მონაცემები სადაზღვევო მიზნებით არ მუშავდება, თუ ეს კონკრეტულად არ არის მითითებული კანონში.[150] ამ შემთხვევაში დამუშავება შესაძლებელია მხოლოდ მას შემდეგ, რაც შეფასდება მისი ცალკეულ პირობებთან შესაბამისობა. კერძოდ, დამუშავება შესაძლებელია, თუ მას კონკრეტული მიზანი აქვს, მონაცემების მიზანთან შესაბამისობა სათანადოდ დასაბუთებულია, მონაცემების ხარისხი და სისწორე შეესაბამება საზოგადოდ მიღებულ სამეცნიერო და კლინიკურ სტადანარტებს, პროგნოზული გამოკვლევის შედეგად მიღებულ მონაცემებს აქვს მაღალი დადებითი პროგნოზული ღირებულება და პროპორციულობის პრინციპის შუქზე, მოცემული რისკის მნიშვნელობისა და ბუნების გათვალისწინებით, დამუშავების საჭიროება სათანადოდ არის დასაბუთებული.[151] პირის ოჯახის წევრების შესახებ გენეტიკური ტესტირებიდან მიღებული უკვე არსებული მონაცემების დაზღვევის მიზნით დამუშავება ყველა შემთხვევაში აკრძალულია. [152]

---

[146] დასაქმებისას პერსონალურ მონაცემთა დამუშავების შესახებ ევროპის საბჭოს რეკომენდაციის მე-9 მუხლის მე-3 პუნქტი.

[147] იქვე.

[148] დასაქმებისას პერსონალურ მონაცემთა დამუშავების შესახებ ევროპის საბჭოს რეკომენდაციის განმარტებითი ბარათი, პარ. 81.

[149] Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, principle 4.

[150] იქვე.

[151] იქვე, მე-5 და მე-16 პუნქტები.

[152] იქვე, მე-17 პუნქტი.

3.4. გენეტიკური მონაცემების დამუშავების ფარგლები, პრინციპები და საფუძვლები

მოდერნიზებულ 108-ე კონვენციასა და მონაცემთა დაცვის ზოგად რეგულაციაში განმტკიცებული წესები არ ვრცელდება ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებაზე. მოქმედებების ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებისადმი მიკუთვნება დამოკიდებულია საქმის გარემოებებზე.[153] ცალსახად პირად დამუშავებად ვერ ჩაითვლება მონაცემთა გამჟღავნება ადამიანთა დიდი რაოდენობის ან აშკარად კერძო სფეროს მიღმა მყოფი პირებისათვის (მაგალითად, მონაცემების საჯაროდ ხელმისაწვდომ ვებგვერდზე განთავსება). [154]

მოდერნიზებული 108-ე კონვენცია და მონაცემთა დაცვის ზოგადი რეგულაცია მხოლოდ ცოცხალ ადამიანებზე ვრცელდება.[155] თუმცა, გენეტიკური მონაცემების სპეციფიკურობიდან გამომდინარე, გარდაცვლილი ადამიანის გენეტიკური მონაცემების დამუშავებაზე პერსონალურ მონაცემთა დაცვის კანონმდებლობა შეიძლება გავრცელდეს, რადგან ამ მონაცემებმა შესაძლოა მისი ცოცხალი ოჯახის წევრების შესახებ ინფორმაცია გაამჟღავნოს.

3.4.1. გენეტიკური მონაცემების დამუშავების პრინციპები

მონაცემთა დამუშავების ძირითადი პრინციპები თავმოყრილია მოდერნიზებულ 108-ე კონვენციასა და მონაცემთა დაცვის ზოგად რეგულაციაში: მონაცემთა კანონიერი, გამჭვირვალე და სამართლიანი დამუშავების პრინციპი, მიზნის შეზღუდვის, მონაცემთა მინიმიზაციის, სიზუსტის, შენახვის ვადის შეზღუდვის, უსაფრთხოებისა და ანგარიშვალდებულების პრინციპები.[156]

კანონიერების პრინციპი გულისხმობს, რომ მონაცემთა დამუშავების სამართლებრივი საფუძველი არსებობს და ის ლეგიტიმურ მიზნებს ემსახურება. როდესაც მონაცემთა სუბიექტი გენეტიკური მონაცემების დამუშავებაზე თანხმობას აცხადებს და კანონმდებლობა არ კრძალავს პირის თანხმობის შემთხვევაში ამ მონაცემთა დამუშავებას, მაშინ მათი დამუშავება შეიძლება კანონიერად ჩაითვალოს. კანონიერი დამუშავება ასევე გულისხმობს, რომ დამუშავებული მონაცემები სხვა მიზნებით არ იქნეს გამოყენებული, დამუშავება უნდა შეესაბამებოდეს კანონმდებლობას, ემსახურებოდეს ლეგიტიმური მიზნების მიღწევას და იყოს მიზნის მიღწევის აუცილებელი და პროპორციული საშუალება.[157] მაგალითისთვის, ესპანეთში მონაცემთა დაცვაზე პასუხისმგებელმა ორგანომ არაპროპორციულობის პრინციპთან შეუსაბამოდ ჩათვალა ახალშობილთა იდენტიფიცირებისა და დედა-შვილის ერთმანეთისგან აცდენის თავიდან არიდების მიზნით გენეტიკური ნიმუშების ფაილის შექმნა, ვინაიდან ამავე მიზნის მიღწევა სხვა (მაგალითად, სამაჯურის) საშუალებითაც შეიძლებოდა.[158]

---

[153] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პარ. 28.

[154] იქვე.

[155] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პარ. 30. მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის 27-ე პუნქტი.

[156] 108+ კონვენციის მე-5, მე-6, მე-7 და მე-8 მუხლები. მონაცემთა დაცვის ზოგადი რეგულაციის მე-5 მუხლი.

[157] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation, A Commentary, Oxford University Press, 2020, გვ. 314.

[158] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

სამართლიანი დამუშავება მოითხოვს, რომ მონაცემები მონაცემთა სუბიექტის მოლოდინების შესაბამისად დამუშავდეს. ამავდროულად, სუბიექტი პოტენციური რისკების შესახებ გაფრთხილებული უნდა იყოს. გენეტიკური მონაცემების დამუშავებისას ეს საკითხი განსაკუთრებით მნიშვნელოვანია. პირის ინფორმირებას მჭიდროდ უკავშირდება **მონაცემთა გამჭვირვალედ დამუშავების პრინციპი.** დამუშავება მონაცემთა სუბიექტისთვის ნათელი და გასაგები იყოს. მას არამხოლოდ გენეტიკური მონაცემების დამუშავების რისკების, არამედ დამუშავების მიზნების, თანხმობის გამოთხოვის უფლების შესახებაც უნდა ეცნობოს.

მიზნის შეზღუდვის პრინციპის შესაბამისად, გენეტიკური მონაცემები კონკრეტული, შესაბამისი, სათანადო ლეგიტიმური მიზნების მისაღწევად უნდა დამუშავდეს ისე, რომ მონაცემების შემდგომი დამუშავება თავდაპირველ მიზანს არ ასცდეს.[159] გენეტიკური მონაცემების რთული და სენსიტიური ბუნების გათვალისწინებით, მათი ხელახლა გამოყენების ან/და ბიოლოგიური ნიმუშის დამატებითი ანალიზის შედეგად, ამგვარი მონაცემების ბოროტად ან სხვა მიზნებით გამოყენების სერიოზული რისკები არსებობს.[160] მონაცემების შემდგომ ახალი მიზნის მისაღწევად დამუშავებისთვის სამართლებრივი საფუძვლის არსებობა აუცილებელია. თუმცა, ამ წესიდან არსებობს გამონაკლისი - მონაცემების საჯარო ინტერესის, სამეცნიერო, ისტორიული თუ სტატისტიკური მიზნით მონაცემთა შემდგომი დამუშავება არ უნდა ჩაითვალოს მონაცემთა თავდაპირველ მიზნებთან შეუსაბამოდ, თუ არსებობს შესაბამისი გარანტიები, რომ ადამიანის უფლებები დაცული იქნება.[161] ამ შემთხვევაში, როცა დამუშავების მიზნები ამის შესაძლებლობას იძლევა, მონაცემთა სუბიექტი იდენტიფიცირებადი არ უნდა იყოს. მოდერნიზებული 108-ე კონვენციის თანახმად, სტატისტიკურ მონაცემებში ასახული გენეტიკური ინფორმაცია აუცილებლად ანონიმური უნდა იყოს, თუმცა, თუ შეგროვების მიზნისთვის მონაცემთა სუბიექტის ვინაობას არსებითი მნიშვნელობა აქვს, მაშინ ამ წესიდან გამონაკლისი დასაშვებია.[162]

გენეტიკური მონაცემების გამოყენება, რომელიც თავდაპირველად პრევენციული, მონაცემთა სუბიექტის ან ამ უკანასკნელის ბიოლოგიური ოჯახის წევრის დიაგნოზირების, მკურნალობის ან სამეცნიერო კვლევის მიზნებისთვის დამუშავდა, შეიძლება მხოლოდ ამ ან შესაბამის პირებთან დაკავშირებით ამ საკითხებზე ინფორმირებული გადაწყვეტილების მისაღებად.[163]

მიზნის შეზღუდვის პრინციპი ვრცელდება სამართალწარმოების ან გამოძიების მიზნებისთვის გენეტიკური მონაცემების დამუშავებაზეც. მაგალითად, როდესაც გენეტიკური მონაცემები მამობის დასადგენად მუშავდება, ეს ინფორმაცია მხოლოდ ბავშვსა და მამას შორის გენეტიკური კავშირის დასადგენად უნდა იქნეს გამოყენებული.[164]

მონაცემთა მინიმაზაციის პრინციპი მოითხოვს, რომ მხოლოდ ისეთი მონაცემები დამუშავდეს, რომლებიც „შესაბამისი და რელევანტურია, მოცულობა კი არ აჭარბებდეს მიზანს, რისთვისაც ისინი

[159] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation, A Commentary, Oxford University Press, 2020, გვ. 315.

[160] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

[161] მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლის მე-2 პუნქტის “კ“ ქვეპუნქტი.

[162] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პარ. 61.

[163] Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data, პუნქტი 7.2.

[164] Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, პარ. 74.

შეგროვდა და/ან დამუშავდა".[165] ამ მხრივ პრობლემურია, რომ გამოძიებისას მიღებული გენეტიკური ინფორმაცია ხშირად პირის უდანაშაულოდ ცნობის შემდგომაც ინახება.[166]

მონაცემთა სიზუსტის პრინციპი ითვალისწინებს მონაცემების საჭიროებისამებრ განახლებას. გენეტიკური ტესტირებების შედეგები შეიძლება გარკვეულ ცდომილებებს შეიცავდეს, თუმცა თუ ეს შედეგები ცდომილების ფარგლებს განსაზღვრავს და ეს მონაცემთა სუბიექტისათვის ახსნილია, მაშინ შეიძლება ჩაითვალოს, რომ ეს მონაცემები ზუსტია.[167] თუ შედეგების შესახებ დასკვნა მოსაზრებას ეფუძნება, ეს ასევე უნდა იყოს ახსნილი, ხოლო როცა მონაცემები განახლდება, შეცდომები ადრეულ მონაცემებში შესაძლებელია შეინახოს, როგორც გადაწყვეტილების მიღებისა და ანალიტიკური პროცესის ამსახველი ზუსტი ჩანაწერი.[168]

შენახვის ვადის შეზღუდვის პრინციპის თანახმად, პერსონალური მონაცემები აუცილებელზე მეტი ვადით არ უნდა ინახებოდეს. თუმცა, ამ პრინციპთან შესაბამისად ითვლება, როცა მონაცემები ანონიმური სახით ან სამეცნიერო კვლევის მიზნებით ინახება. როგორც წესი, კვლევის მიზნით შეგროვებული გენეტიკური მონაცემები ანონიმური უნდა იყოს, თუ ეს ამ მიზნებს არ ეწინააღმდეგება.

შენახვის ვადის შეზღუდვის პრინციპს უკავშირდება ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება, სადაც სასამართლომ დაადგინა, რომ თითის ანაბეჭდების, უჯრედული ნიმუშებისა და დნმ-ის პროფილების განუსაზღვრელი ვადით შენახვა მას შემდეგ, რაც ერთი მონაცემთა სუბიექტის მიმართ სისხლის სამართლებრივი დევნა შეწყდა, ხოლო მეორე გამართლდა, დემოკრატიულ საზოგადოებაში პროპორციულ და სათანადო საშუალებას არ წარმოადგენდა.[169] მართალია, მოდერნიზებული 108-ე კონვენცია ამ პრინციპიდან გამონაკლისის დაწესებას უშვებს, თუმცა, გამონაკლისი კანონით დაწესებული მიზნების მიღწევის აუცილებელი და პროპორციული საშუალება უნდა იყოს.[170]

სისხლის სამართლის საქმის წარმოებისას დნმ ანალიზის შედეგები და მიღებული ინფორმაცია უნდა წაიშალოს მას შემდეგ, რაც მიზანი, რომლისთვისაც ის ინახებოდა, მიღწეულია. თუმცა, ეს ინფორმაცია შეიძლება შეინახოს, თუ პირი მსჯავრდებულია მძიმე დანაშაულში, რომელიც მიმართულია ადამიანის სიცოცხლის ან ადამიანების უსაფრთხოების წინააღმდეგ. თუმცა, შენახვის ზუსტი ვადის განსაზღვრა ყველა შემთხვევაში აუცილებელია.[171]

მონაცემთა დამუშავებისას უსაფრთხოებისა და კონფიდენციალურობის დაცვის ვალდებულებას ადგენს **უსაფრთხოების პრინციპი.**[172] ეს ნიშნავს, რომ მონაცემთა დამმუშავებელმა უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები, რაც შეიძლება მოიცავდეს ფსევდონიმიზაციასა და დაშიფვრას, გარკვეული მონაცემების ცალკე შენახვის ვალდებულებას, უფლებამოსილი საზედამ-

[165] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 143.

[166] Privacy International, DNA and Genetic Data, ხელმისაწვდომია: https://bit.ly/3H8IJPf წვდომის თარიღი: 19.10.2021.

[167] PHG Foundation, GDPR and Genomic Data, გვ. 94.

[168] იქვე.

[169] ადამიანის უფლებათა ევროპული სასამართლოს 2008 წლის 4 დეკემბრის გადაწყვეტილება საქმეზე S. and Marper v. United Kingdom.

[170] 108+ კონვენციის მე-11 მუხლის პირველი პუნქტი.

[171] COM Recommendation 1992A: Committee of Ministers of the Council of Europe, 'Recommendation on the Use of Analysis of Deoxyribonucleic Acid (DNA) within the Framework of the Criminal Justice System' (R (92)1, 10 February 1992), მე-8 პუნქტი.

[172] 108+ კონვენციის მე-7 მუხლი; მონაცემთა დაცვის ზოგადი რეგულაციის მე-5 მუხლის 1-ლი პუნქტის „ვ" ქვეპუნქტი.

ხედველო ორგანოებისა და მონაცემთა სუბიექტის შეტყობინებას, როცა არსებობს უფლებების შელახვის საფრთხე.

დასაქმებისას პერსონალური მონაცემების დამუშავების შესახებ ევროპის საბჭოს რეკომენდაცია გენეტიკურ მონაცემებთან დაკავშირებით განმარტავს, რომ გენეტიკური მონაცემები, როცა მათ დამუშავებას კანონი ითვალისწინებს და როცა ეს მიზანშეწონილია, დამსაქმებელთან დაკავშირებული პერსონალური მონაცემების სხვა კატეგორიებისგან განცალკევებით უნდა იქნეს შენახული. მნიშვნელოვანია ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების მიღება, რათა სხვა თანამშრომლებს ამ მონაცემებზე ხელი არ მიუწვდებოდეთ.[173] ასევე, კონფიდენციალური უნდა იყოს პერსონალური ხასიათის ინფორმაცია, რომელიც ბიოლოგიური მასალის კვლევებისას შეგროვდა.[174] მკვლევრებს მხოლოდ ანონიმიზებულ ან დაშიფრულ ბიოლოგიურ ნიმუშებსა და მონაცემებზე უნდა ჰქონდეთ წვდომა და აეკრძალოთ მონაწილეთა იდენტიფიცირება, გამონაკლისი შემთხვევების გარდა.[175] გენეტიკური მონაცემების ცალკე შენახვის ვალდებულება უნდა არსებობდეს ჯანდაცვის მიზნებისთვის გენეტიკური ტესტირების ჩატარების შემთხვევებში. თუმცა, პროფესიული საიდუმლოების დაცვისა და კონფიდენციალურობის ვალდებულება შეიძლება შეიზღუდოს, თუ პირის ოჯახის წევრები გენეტიკური დაავადების სერიოზული რისკების წინაშე დგანან.[176]

ევროკავშირის დირექტივა, რომელიც სამართალმდაცავი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავების წესებს ადგენს, ასევე ავალდებულებს წევრ სახელმწიფოებს პერსონალური მონაცემების, განსაკუთრებით კი, განსაკუთრებული კატეგორიის პერსონალური მონაცემების გამჟღავნების რისკებთან შესაბამისი უსაფრთხოების დონის უზრუნველსაყოფად სათანადო ტექნიკური და ორგანიზაციული ზომების მიღებას.[177]

ანგარიშვალდებულების პრინციპის მიხედვით, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი პასუხისმგებელნი არიან დამუშავების ოპერაციების შესაბამისობაზე მონაცემთა დაცვის კანონმდებლობასა და საკუთარ ვალდებულებებთან. ეს პრინციპი მოიაზრებს დამუშავების ოპერაციების აღრიცხვას, რისკების შეფასებას, ახალი პროდუქტის ან მომსახურების შექმნისას მონაცემთა დაცვის სტანდარტების გათვალისწინებას (privacy by design), პირველად პარამეტრად მონაცემთა დაცვის განსაზღვრას (privacy by default) და სხვა ზომების მიღებას.[178]

29-ე მუხლის სამუშაო ჯგუფმა ბიო ბანკების გამოყენებასთან დაკავშირებით განმარტა, რომ მონაცემთა დამმუშავებლებმა უსაფრთხოების მაღალი დონის უზრუნველსაყოფად შეიძლება ჩაატარონ კვლევები პოტენციურ რისკებთან დაკავშირებით, განსაზღვრონ უსაფრთხოების პოლიტიკა, ინფორმაცია მიაწოდონ მომსახურე პერსონალს და ჩაუტარონ ტრენინგები.[179]

---

[173] Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, განმარტებითი ბარათი, პუნქტი 9.6.

[174] Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, განმარტებითი ბარათი, პუნქტი 37.

[175] OECD Guidelines on Human Biobanks and Genetic Research Databases 7.D p.14

[176] RECOMMENDATION No. R (92) 3 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON GENETIC TESTING AND SCREENING FOR HEALTH CARE PURPOSES, მე-9 და მე-10 პრინციპი.

[177] 2016/680 დირექტივის 29-ე მუხლი.

[178] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 153-154.

[179] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004, გვ. 11.

მაგალითისთვის, 2016/680 დირექტივის თანახმად, წევრმა სახელმწიფოებმა უნდა განსაზღვრონ მონაცემთა დამმუშავებლის ვალდებულება, აღრიცხონ დამუშავების ოპერაციები, მათ შორის, დამმუშავებლის, დამუშავების მიზნის, მონაცემთა სუბიექტის კატეგორიისა და მონაცემთა კატეგორიის შესახებ ინფორმაცია; სამართლებრივი საფუძველი; როცა ეს შესაძლებელია, სხვადასხვა კატეგორიის მონაცემთა წაშლის ვადები; პროფილირების შემთხვევები და სხვა.[180] მსგავს ვალდებულებას მონაცემთა დაცვის ზოგადი რეგულაციაც ითვალისწინებს.[181]

3.4.2. გენეტიკური მონაცემების დამუშავების საფუძვლები

მოდერნიზებული 108-ე კონვენცია ადგენს, რომ მონაცემები უნდა დამუშავდეს მონაცემთა სუბიექტის ნებაყოფლობითი, კონკრეტული, ინფორმირებული და მკაფიო თანხმობის ან კანონით დადგენილი ლეგიტიმური საფუძვლის არსებობის შემთხვევაში.[182] კონვენციისგან განსხვავებით, მონაცემთა დაცვის ზოგადი რეგულაცია განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძვლებს ჩამოთვლის. რეგულაციით დადგენილი ზოგადი წესით, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დაუშვებელია, თუ არ არსებობს რეგულაციით განსაზღვრული კონკრეტული გამონაკლისი. თუმცა, გამონაკლისის არსებობის შემთხვევაშიც, მონაცემები აუცილებლად კანონის საფუძველზე უნდა დამუშავდეს. ერთ-ერთი გამონაკლისია მონაცემთა სუბიექტის თანხმობა.[183] სწორედ მონაცემთა სუბიექტის თანხმობას ეფუძნება კერძო კომპანიების მიერ ჯანმრთელობასთან დაკავშირებული გენეტიკური რისკების თუ წარმომავლობის საკითხების გარკვევის მიზნით გენეტიკური ტესტების ჩატარება.

გენეტიკური მონაცემების დამუშავებაზე თანხმობა საჭირო არ არის, როცა ის სისხლის სამართლის საქმის გამოძიებისას სავარაუდო დამნაშვის იდენტიფიცირების ან უგზო-უკვლოდ დაკარგული პირის ძებნისას გამოიყენება. ამ უკანასკნელ შემთხვევაში, დამუშავების საფუძველი მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვაა.[184] 2016/680 დირექტივა განსაკუთრებული კატეგორიის მონაცემების დამუშავების ერთ-ერთ საფუძვლად სწორედ მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვას ითვალისწინებს.[185] თუმცა, თანხმობა აუცილებელია სამოქალაქო საქმის წარმოებისას, როცა გენეტიკური მონაცემები მშობლის ან სხვა ოჯახური კავშირის დადგენის მიზნით მუშავდება.[186] დაუშვებელია გენეტიკური მასალის მოპარვა და სუბიექტისგან ფარულად მონაცემის დამუშავება (მაგალითად, ბავშვის მამის დადგენის მიზნით გენეტიკური ტესტირების ჩატარება მამისგან ფარულად აღებული თმის მასალით).[187]

შესაძლებელია კანონმდებლობა კრძალავდეს კონკრეტული მონაცემის დამუშავებას იმ შემთხვევაშიც კი, როცა მონაცემთა სუბიექტი თანხმობას აცხადებს. როგორც უკვე აღინიშნა, გენეტიკურ

[180] 2016/680 დირექტივის 24-ე მუხლის პირველი პუნქტი.

[181] მონაცემთა დაცვის ზოგადი რეგულაციის 30-ე მუხლი.

[182] 108+ კონვენცია, მე-5 მუხლის მე-2 პუნქტი.

[183] მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლი.

[184] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

[185] სამართალდამცავი ორგანოების შესახებ დირექტივის მე-10 მუხლი.

[186] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004, გვ. 12;

[187] იქვე.

მონაცემებთან დაკავშირებით ამგვარი აკრძალვა შეიძლება უკავშირდებოდეს დასაქმების ან დაზღვევის მიზნებისთვის გენეტიკური პროგნოზირების ტესტების გაკეთებას.

გენეტიკური მონაცემების დამუშავების მნიშვნელოვანი საფუძველია მათი დამუშავება სამედიცინო და საზოგადოებრივ ჯანმრთელობასთან დაკავშირებული მიზნებით.[188] როგორც უკვე აღინიშნა, გენეტიკური მონაცემები ხშირად გამოიყენება დაავადებათა დიაგნოსტირებისა თუ მკურნალობის მიზნით. ამასთან, საზოგადოებრივ ჯანმრთელობასთან დაკავშირებული მიზნებით დამუშავება შესაძლებელია, როცა სხვადასხვა დაავადების აფეთქებისას ადამიანის დნმ-სგან ვირუსის დნმ-ის გამოყოფა ხდება პათოგენის სეკვენირების პროცესში, რისი მიზანიც სხვადასხვა ინფექციური დაავადების კვლევა და უკეთ მართვაა.

გამონაკლისია დაწესებული არქივირების, სამეცნიერო/ისტორიული კვლევის ან სტატისტიკის წარმოების მიზნებით მონაცემთა დამუშავებაზეც. პერსონალური მონაცემების დაცვის უზრუნველსაყოფად, სამედიცინო ან სხვა მეცნიერულ კვლევებში გამოყენებული გენეტიკური მონაცემები ანონიმური უნდა იყოს. ამავდროულად, თუ კვლევის მიზნებისთვის აუცილებელია, შესაძლებელია იდენტიფიცირებადი პირი ან პირთა ჯგუფის გენეტიკური მონაცემების დამუშავებაც. ჯანმრთელობასთან დაკავშირებული გენეტიკური მონაცემების სამეცნიერო კვლევის მიზნებისთვის დამუშავების საჭიროება უნდა შეფასდეს კვლევის პროექტის მიზნების, მონაცემთა სუბიექტისათვის საფრთხის შექმნის, ასევე მის ბიოლოგიურ ოჯახთან მიმართებით არსებული რისკების გათვალისწინებით.[189]

განსაკუთრებული კატეგორიის მონაცემების დამუშავების რეგულაციით განსაზღვრული სხვა საფუძვლებია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვა, საქველმოქმედო ან არაკომერციული ორგანიზაციების მიერ მათი საქმიანობის ფარგლებში ამ მონაცემთა გამოყენება, მონაცემთა სუბიექტის მიერ მათი გასაჯაროება, სამართლებრივი მოთხოვნების შესრულება და მნიშვნელოვანი საჯარო ინტერესის დაცვა.

სამართლებრივი მოთხოვნების შესასრულებლად გენეტიკური მონაცემების დამუშავების მაგალითად შეგვიძლია განვიხილოთ გენეტიკურ მონაცემთა სასამართლოში საქმისწარმოების მიზნით დამუშავება. გენეტიკური მონაცემები ამ შემთხვევაში შეიძლება გამოიყენონ როგორც სამოქალაქო (საოჯახო დავებში, მამობის/დედობის დადგენისას), ისე სისხლის სამართლის საქმეებზე (მაგალითად, პირის იდენტიფიკაციისთვის).

ასევე, შესაძლებელია, რომ მონაცემთა სუბიექტმა გენეტიკური მონაცემები ვებგვერდზე გამოაქვეყნოს, მაგალითად, წარმომავლობასთან დაკავშირებულ მონაცემთა ბაზაში და ამგვარად ყველა პირისთვის ხელმისაწვდომი გახადოს.[190] მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად გენეტიკური მონაცემების გამოყენება შესაძლებელია, მაგალითად, ბუნებრივი კატასტროფების დროს, როცა პირს თანხმობის გაცხადება არ შეუძლია და გენომის სეკვენირება აუცილებელია სიცოცხლისთვის საშიში დაავადების გამოსაკვლევად.[191]

---

[188] მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლის „თ“ და “ი“ ქვეპუნქტები;

[189] Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, პუნქტი 15.2.

[190] Colin Mitchell, Johan Ordish, Emma Johnson, Tanya Brigden and Alison Hal, *GDPR and genomic data*, 2020, გვ. 76.

[191] იქვე, გვ. 77.

დამატებით, მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლის მე-4 პუნქტი სახელმწიფოებს მიუთითებს გენეტიკური, ბიომეტრიული და ჯანმრთელობის შესახებ მონაცემთა დამუშავების დამატებითი წესების და პირობების, მათ შორის, შეზღუდვების საკუთარ კანონმდებლობაში ჩამოყალიბების შესაძლებლობაზე.

3.4.2.1. მონაცემთა სუბიექტის თანხმობა

გენეტიკური მონაცემების დამუშავება ხშირად მონაცემთა სუბიექტის თანხმობას ეფუძნება. გარდა გენეტიკური ტესტირებებისა, არც ისე იშვიათად, სამეცნიერო კვლევებში გენეტიკური მონაცემების გამოყენება თანხმობის შედეგია. მონაცემთა დაცვის ზოგადი რეგულაციაც პრეამბულაში მიუთითებს, რომ სამეცნიერო კვლევის მიზნით მონაცემთა შეგროვების ეტაპზე დამუშავების მიზნის სრულყოფილად განსაზღვრა ხანდახან შეუძლებელია, სწორედ ამიტომ მონაცემთა სუბიექტს თანხმობის გაცემის შესაძლებლობა უნდა მიეცეს.[192]

მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, თანხმობა ნებაყოფლობითი, მკაფიოდ გამოხატული, თავისუფალი და ინფორმირებული უნდა იყოს.[193] ამავდროულად, მონაცემთა სუბიექტი უფლებამოსილია გამოითხოვოს ეს თანხმობა, რის შესახებაც მისი ინფორმირება აუცილებელია.[194] განსაკუთრებული კატეგორიის მონაცემების დამუშავებისას თანხმობა მკაფიოდ, ზეპირი ან წერილობითი ფორმით უნდა გამოიხატოს.[195] მოდერნიზებული 108-ე კონვენცია მიუთითებს, რომ თანხმობა განცხადებით ან აქტიური ქმედებით უნდა იყოს გამოხატული.[196] შესაბამისად, უმოქმედობა, წინასწარ შევსებული ფორმები ან მონიშნული გრაფები თანხმობას ვერ წარმოშობს.[197]

გენეტიკური მონაცემების შესახებ იუნესკოს დეკლარაციაც ადგენს, რომ პირი მკაფიოდ, სათანადოდ და წინასწარ უნდა იყოს ინფორმირებული, მათ შორის, უნდა ეცნობოს გენეტიკური მონაცემების გამოყენებისა და შენახვის მიზნები, აუცილებლობის შემთხვევაში, დამუშავების რისკები და შედეგები, ასევე, თანხმობის გამოთხოვის უფლება.[198] გენეტიკური მონაცემების შეგროვებაზე პირის წინასწარი, ინფორმირებული თანხმობა აუცილებელია, თუმცა, გარკვეული გამონაკლისების დაწესება კანონმდებლობით შეიძლება. თავისუფალი თანხმობა გულისხმობს, რომ ის გაცემულია ფინანსური ან სხვა პირადი სარგებლის მიღების ინტერესებისგან დამოუკიდებლად.[199] ამასთან, როდესაც პირი გამოითხოვს თანხმობას, შენახული გენეტიკური მონაცემები უნდა განადგურდეს. ასევე, უნდა განადგურდეს დანაშაულის გამოძიების, სასამართლო ექსპერტიზის ჩატარებისა და სამოქალაქო დავის მიზნებისთვის შენახული გენეტიკური მონაცემები, როცა მიზნები, რის გამოც მონაცემები ინახებოდა, მიღწეულია.[200]

---

[192] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, 33-ე პუნქტი.

[193] იქვე, მე-4 მუხლის მე-11 პუნქტი.

[194] იქვე, მე-7 მუხლის მე-3 პუნქტი.

[195] იქვე, პრეამბულა, 32-ე პუნქტი.

[196] 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, პუნქტი 42.

[197] იქვე.

[198] გენეტიკური მონაცემების დამუშავების შესახებ იუნესკოს დეკლარაციის მე-6 მუხლი.

[199] იქვე, მე-8 მუხლი.

[200] იქვე, 21-ე მუხლი.

მნიშვნელოვანია აღინიშნოს, რომ გენეტიკური ტესტირების ჩატარებისას მნიშვნელოვანია მონაცემთა სუბიექტს სათანადო კონსულტაცია გაეწიოს სამედიცინო ფაქტების, ტესტირების შედეგებისა და გასაკეთებელი არჩევანის თაობაზე.[201]

3.5. ინფორმაციის მიღებისა და მიღებაზე უარის თქმის უფლება

ევროპის საბჭოსა და ევროკავშირის კანონმდებლობით[202], დამმუშავებლებს ეკისრებათ ვალდებულება, რომ პერსონალური მონაცემების შეგროვებისას მონაცემთა სუბიექტს მიაწოდონ ინფორმაცია დაგეგმილი დამუშავების შესახებ. გენეტიკური ინფორმაციის დამუშავებისას ინფორმაციის მიღების უფლება შეიძლება მონაცემთა სუბიექტის ოჯახის წევრებზეც გავრცელდეს. ინფორმაციის მიწოდების ვალდებულება დამმუშავებელმა პროაქტიულად უნდა შეასრულოს, მიუხედავად იმისა, მონაცემთა სუბიექტი გამოავლენს თუ არა ინტერესს ამ ინფორმაციის მიმართ.[203] თუმცა, გენეტიკური მონაცემების დამუშავებისას, შესაძლებელია, მონაცემთა სუბიექტმა უარი განაცხადოს ინფორმაციის მიღებაზე.

2016/680 დირექტივა მონაცემთა სუბიექტის ინფორმირების და მის მონაცემებზე ხელმისაწვდომობის უფლებას ადგენს, თუმცა უშვებს კონკრეტულ შემთხვევებში ხელმისაწვდომობის უფლების შეზღუდვის შესაძლებლობას.[204] ამ დროს აუცილებელია მონაცემთა სუბიექტს განემარტოს უარის მიზეზები და საფუძვლები.[205]

ადამიანის უფლებებისა და ბიომედიცინის შესახებ ევროპის საბჭოს კონვენცია განსაზღვრავს პაციენტების ჯანმრთელობისა და გენეტიკური ტესტირების შედეგების შესახებ ინფორმაციის მიღების უფლებას და ითვალისწინებს პაციენტის უფლებასაც, უარი განაცხადოს ამ ინფორმაციის მიღებაზე.[206] ჯანმრთელობის დაცვის მიზნით შესრულებულმა გენეტიკურმა ტესტმა შესაძლოა პირის ან მისი ოჯახის წევრების შესახებ იმგვარი ინფორმაცია გამოამჟღავნოს, რაც ჯანმრთელობას არ უკავშირდება (მაგალითად, მოულოდნელი ბიოლოგიური კავშირის არსებობა). კონვენცია ეროვნული კანონმდებლობის მიხედულების ფარგლებში აქცევს დაინტერესებული პირებისათვის ამგვარი მოულოდნელი ინფორმაციის გამჟღავნების საკითხის რეგულირებას და შესაბამისი პირობების ჩამოყალიბებას.[207] გადაწყვეტილების მიღებისას მხედველობაში მიიღება პირის სურვილი, ასევე პირისა და მისი ოჯახის წევრებისთვის ზიანის მიყენების საფრთხეები.[208]

---

[201] RECOMMENDATION No. R (92) 3 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON GENETIC TESTING AND SCREENING FOR HEALTH CARE PURPOSES, მე-3 პრინციპი.

[202] 108+ კონვენციის მე-8 მუხლი; მონაცემთა დაცვის ზოგადი რეგულაციის პრეამბული 39-ე პუნქტი, მე-12-14 მუხლები.

[203] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 236.

[204] მაგალითად, როცა ხელმისაწვდომობა ხელს უშლის გამოძიების ინტერესებს, აუცილებელია საზოგადოებრივი უსაფრთხოების ან სხვათა უფლებების ან თავისუფლებების დასაცავად და სხვა.

[205] 2016/680 დირექტივა, მუხლი 15.

[206] ადამიანის უფლებებისა და ბიომედიცის შესახებ კონვენციის მე-10 მუხლი.

[207] ადამიანის უფლებებისა და ბიომედიცის შესახებ კონვენციის განმარტებითი ბარათი, პარ. 130.

[208] იქვე.

ჯანმრთელობასთან დაკავშირებული მონაცემების შესახებ ევროპის საბჭოს რეკომენდაცია ითვალისწინებს პირის უფლებას, უარი განაცხადოს ინფორმაციის მიღებაზე, როცა კვლევებმა შეიძლება მოულოდნელი შედეგები აჩვენოს ან მას არ სურს საკუთარ ჯანმრთელობასთან დაკავშირებული კონკრეტული საკითხების ცოდნა, რის შესახებაც მას გამოკვლევებამდე უნდა ეცნობოს. მაგალითისთვის, ეს ვითარება შეიძლება მაშინ დადგეს, როდესაც მონაცემთა სუბიექტს არ სურს გამოარკვიოს, ატარებს თუ არა კონკრეტული განუკურნებელი გენეტიკური დაავადების გენებს. თუმცა, განსაკუთრებულ შემთხვევებში, ეს უფლება შეიძლება შეიზღუდოს მონაცემთა სუბიექტის ინტერესების ან პაციენტის მოვლაზე ექიმის ვალდებულების გათვალისწინებით.[209]

მონაცემთა სუბიექტსა და მის ბიოლოგიურ ოჯახის წევრებს გენეტიკური მახასიათებლები საერთო აქვთ. შესაბამისად, გენეტიკური ტესტირების შედეგებს მათთვისაც დიდი მნიშვნელობა შეიძლება ჰქონდეს. მონაცემთა სუბიექტის შესახებ გენეტიკური ინფორმაციის მისი ბიოლოგიური ნათესავებისათვის გაზიარების საკითხი წამოიჭრება მაშინ, როდესაც ეს მონაცემები მათი ჯანმრთელობისა და მომავლისთვისაც რელევანტურია. ამ დროს შესაძლებელია მონაცემთა სუბიექტის თანხმობის არარსებობისას, ოჯახის წევრებს ინფორმაციაზე წვდომის უფლება მიენიჭოთ. ეს შეიძლება ორი გზით განხორციელდეს:

- ოჯახის წევრებიც მონაცემთა სუბიექტებად უნდა ჩაითვალონ ან
- ოჯახის წევრებს მათი ინტერესების შელახვის საფრთხის გამო ამ ინფორმაციის მიღების უფლება მიენიჭოთ.[210]

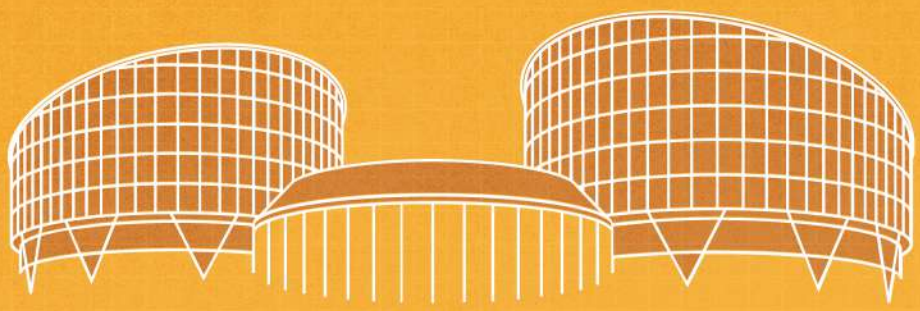
მაგალითად, 1999 წელს იტალიაში, მამის პირადი ცხოვრების ხელშეუხებლობის უფლება გადაწონა შვილის ჯანმრთელობის უფლებამ. მიუხედავად იმისა, რომ მამამ უარი განაცხადა მის შესახებ გენეტიკური ინფორმაციის შვილისთვის გამჟღავნებაზე, ამ უკანასკნელს მაინც მიენიჭა ამ ინფორმაციაზე წვდომის უფლება.[211] აღსანიშნავია, რომ პირის უფლება, არ მიიღოს გენეტიკური ინფორმაცია, ოჯახის წევრებზეც ვრცელდება, რაც მხედველობაში უნდა იქნეს მიღებული განსაკუთრებით მაშინ, როცა არ არსებობს დაავადების მკურნალობისა და პრევენციის შესაძლებლობა, ხოლო დაავადება განსაკუთრებით საშიშია.[212]

[209] 7.6 პუნქტი, ხელმისაწვდომია: https://bit.ly/3qqnulR წვდომის თარიღი: 11.11.2021.

[210] ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

[211] იქვე, გვ. 9.

[212] იქვე.



4. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები

ამ თავში განხილულია ადამიანის უფლებათა ევროპული სასამართლოს მიერ მიღებული რამდენიმე გადაწყვეტილება, რაც უკავშირდება ბიომეტრიული და გენეტიკური მონაცემების დამუშავებას.

4.1. ს. და მარფერი გაერთიანებული სამეფოს წინააღმდეგ (2008)

საქმეზე ***ს. და მარფერი გაერთიანებული სამეფოს წინააღმდეგ***[213] ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ იმ პირების დნმ-ს ნიმუშებისა და ანაბეჭდების შენახვა, რომლებიც გამართლდნენ ან ბრალდება მოეხსნათ, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევას იწვევს.

ფაქტობრივი გარემოებები

პირველი მომჩივანი 11 წლის ასაკში დააკავეს ძარცვის მცდელობისათვის და ამ ბრალდების გამო მისი ანაბეჭდები და დნმ-ის ნიმუშები აიღეს, თუმცა საბოლოოდ ის გამართლდა. მეორე მომჩივანი - მარფერი დააკავეს პარტნიორზე ძალადობისათვის. მისი ანაბეჭდებისა და დნმ-ს ნიმუშებიც პირველი შემთხვევის მსგავსად აიღეს. წინა სასამართლო სხდომის ჩატარებამდე მარფერი და მისი პარტნიორი მორიგდნენ. შესაბამისად, პროკურორმა ბრალდებას მხარი არ დაუჭირა და საქმე ოფიციალურად შეწყდა. ორივე მომჩივანმა მოითხოვა შენახული ანაბეჭდებისა და დნმ-ს ნიმუშების განადგურება, თუმცა პოლიციამ წარდგენილ მოთხოვნაზე უარი განუცხადა.

პოლიციის გადაწყვეტილების განხილვის მიზნით, მომჩივნებმა სასამართლოს მიმართეს. თუმცა, 2002 წლის მარტში ადმინისტრაციულმა სასამართლომ მათი საჩივარი არ დააკმაყოფილა. იმავე წლის სექტემბერში სააპელაციო სასამართლომ ძალაში დატოვა ადმინისტრაციული სასამართლოს გადაწყვეტილება, ხოლო 2004 წელს ლორდთა პალატამ მომჩივანთა საჩივარი არ დააკმაყოფილა.

საბოლოოდ, მომჩივნებმა ადამიანის უფლებათა ევროპულ სასამართლოში წარადგინეს საჩივარი და განაცხადეს, რომ მათი ნების საწინააღმდეგოდ დნმ-ს ნიმუშებისა და ანაბეჭდების შენახვით კონვენციის მე-8 და მე-14 მუხლები ირღვეოდა.

სასამართლოს შეფასება

2008 წლის 4 დეკემბრის გადაწყვეტილებით სასამართლომ განმარტა, რომ ანაბეჭდების, დნმ-ისა და უჯრედოვანი ქსოვილის ნიმუშების პირის ნების საწინააღმდეგო შენახვა მომჩივნების პირადი და ოჯახური ცხოვრების პატივისცემის უფლებას არღვევდა. შეფასებისას სასამართლომ გაითვალისწინა მოპასუხე ქვეყნის პოზიცია, რომ დნმ-ისა და ანაბეჭდების აღება დანაშაულის აღკვეთის ლეგიტიმურ მიზანს ემსახურება, თუმცა დასძინა, რომ უფლებაში ჩარევა უნდა გამომდინარეობდეს „მწვავე

[213] ხელმისაწვდომია: https://bit.ly/3n8AUB1 წვდომის თარიღი: 12.11.2021

სოციალური საჭიროებიდან,“ იყოს პროპორციული და აუცილებელი დემოკრატიულ საზოგადოებაში.

უჯრედოვან ქსოვილთან დაკავშირებით სასამართლომ განმარტა, რომ ის შეიცავს უაღრესად პირადი ხასიათის ინფორმაციას, მათ შორის, ჯანმრთელობის მდგომარეობის შესახებ მონაცემებს. ამასთან, აღებულ ნიმუშებში შედის ადამიანის უნიკალური გენეტიკური კოდი, რომელიც ინფორმაციას ამჟღავნებს არა მხოლოდ კონკრეტული პირის, არამედ ასევე მისი ნათესავების შესახებ. დნმ-ში არსებული ინფორმაციის დიდი მოცულობის გათვალისწინებით, ამ ტიპის მონაცემების შენახვა თავისთავად ნიშნავს კონვენციის მე-8 მუხლით გათვალისწინებულ უფლებაში ჩარევას. ის გარემოება, რომ პოლიცია მას შეზღუდული ოდენობით იყენებს, ამ ფაქტს არ ცვლის.

ამასთან, შესაძლებელია, იდენტიფიცირებული პირის დნმ-ის ნიმუშებსა და ანაბეჭდებს შორის განსხვავებებზე მსჯელობა საჭირო იყოს, თუმცა ორივე მათგანის შენახვა პირადი ცხოვრების უფლებაში ჩარევას წარმოადგენს. სასამართლომ დასძინა, რომ ის იზიარებს დანაშაულთან ბრძოლის ფარგლებში დნმ-ის ნიმუშების გამოყენების მნიშვნელობას და ხედავს ამ კუთხით ბოლო წლებში მიღწეულ პროგრესს, თუმცა აუცილებელია დადგინდეს ამ მონაცემების გამოყენების ზღვარი.

სასამართლოს შეფასებით, მე-8 მუხლით გათვალისწინებული დაცვის გარანტიების დონე დასაშვებზე მეტად შესუსტდება, თუ კომპეტენტური ორგანოები ნებისმიერ ფასად, ინტერესების დაბალანსების გარეშე გამოიყენებენ სამეცნიერო ტექნიკის მიღწევებს. გადაწყვეტილების მიხედვით, ჩარევა უნდა ემსახურებოდეს ლეგიტიმურ მიზანს და ხორციელდებოდეს კანონის შესაბამისად, კანონი კი უნდა იყოს მარტივად გასაგები, განჭვრეტადი და იმ სიზუსტით ჩამოყალიბებული, რაც პირს შესაძლებლობას აძლევს დაარეგულიროს საკუთარი ქმედება. ეროვნული კანონმდებლობა უნდა შეიცავდეს თვითნებობისგან დაცვის ადეკვატურ სამართლებრივ ბერკეტებს და საკმარისი სიცხადით უთითებდეს კომპეტენტური ორგანოების დისკრეციის ფარგლებსა და მისი განხორციელების წესს.

საგულისხმოა, რომ სასამართლომ გადაწყვეტილებაში მსჯელობა განავითარა იმ პირებთან მიმართებით, ვინც ეჭვმიტანილი იყო დანაშაულის ჩადენაში და შემდგომ ბრალი არ დაუმტკიცდა. ევროპულმა სასამართლომ მხედველობაში მიიღო ის გარემოება, რომ გაერთიანებულ სამეფოში არსებული კანონმდებლობა ნიმუშის აღებისას არ ითვალისწინებდა სამართალდარღვევის ხასიათსა და სიმძიმეს, არც ეჭვმიტანილის ასაკს. ამასთან, აღებული ნიმუშების შენახვა დაშვებული იყო განუსაზღვრელი ვადით, ხოლო გამართლებული პირის ნიმუშების განადგურება ან მონაცემების სახელმწიფო ბაზიდან წაშლა შეზღუდულ შემთხვევებში შეიძლებოდა. სასამართლომ მიუთითა, რომ იმ პირების ბიოლოგიური ნიმუშების შენახვა, რომლებიც არ იყვნენ დამნაშავეებად ცნობილნი, ვერ გამართლდებოდა დანაშაულის პრევენციის ლეგიტიმურ მიზანზე აპელირებით. გადაწყვეტილების თანახმად, ამ შემთხვევაში, გაერთიანებული სამეფო გასცდა მინიჭებულ მიხედულების ფარგლებს, რამაც მომჩივნების პირადი და ოჯახური ცხოვრების პატივისცემის უფლებაში არაპროპორციული ჩარევა გამოიწვია.

4.2. მ.კ. საფრანგეთის წინააღმდეგ (2013)

საქმეზე ***მ.კ. საფრანგეთის წინააღმდეგ***[214] ადამიანის უფლებათა ევროპულმა სასამართლომ ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევა დაადგინა, რადგან უდანაშაულო ადამიანის პერსონალური მონაცემების 25 წლით შენახვა არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში.

ფაქტობრივი გარემოებები

პოლიციამ მ.კ. წიგნის ქურდობისათვის დააკავა, რის გამოც აიღეს მისი ანაბეჭდები. პარიზის სააპელაციო სასამართლოს 2005 წლის გადაწყვეტილებით, მომჩივანი გამართლდა. 2005 წლის 28 სექტემბერს, მომჩივანი ისევ წიგნის ქურდობისთვის დააკავეს და კვლავ აიღეს მისი თითის ანაბეჭდები. 2006 წლის 2 თებერვალს, პროკურორმა სისხლისსამართლებრივი დევნა შეწყვიტა. ამ პროცესის ფარგლებში აღებული ანაბეჭდები შეიტანეს ანაბეჭდების სახელმწიფო მონაცემთა ბაზაში. მომჩივანმა მოითხოვა მისი ანაბეჭდების ბაზიდან წაშლა. პროკურორმა მხოლოდ პროცესის პირველ ეტაპზე აღებული ანაბეჭდების წაშლის გადაწყვეტილება მიიღო. ის ამტკიცებდა, რომ მომჩივნის თითის ანაბეჭდების ერთი ნიმუშის შენახვა გამართლებული იყო ამ უკანასკნელის ინტერესებიდან გამომდინარე, რადგან ეს შესაძლებლობას იძლეოდა მესამე პირის ჩადენილ ქმედებებში მისი მონაწილეობა გამოერიცხათ, თუ მესამე პირი მის ვინაობას მიითვისებდა/მოიპარავდა. პარიზის ტრიბუნალმა დაადგინა, რომ მ. კ.-ს შესახებ ინფორმაცია მონაცემთა ბაზაში უნდა დარჩენილიყო. პარიზის სააპელაციო სასამართლოს საგამოძიებო განყოფილების თავმჯდომარემ მხარი დაუჭირა ამ გადაწყვეტილებას, ხოლო საკასაციო სასამართლომ საჩივარი არ დააკმაყოფილა.

მომჩივანმა ადამიანის უფლებათა ევროპულ სასამართლოში საჩივარი შეიტანა და განაცხადა, რომ დაირღვა კონვენციის მე-8 და მე-6 მუხლები.

სასამართლოს შეფასება

ევროპულმა სასამართლომ განმარტა, რომ იდენტიფიცირებული პირის ანაბეჭდების შენახვა მე-8 მუხლში ჩარევაა და ის უნდა ხდებოდეს კანონის შესაბამისად. კანონი კი უნდა იყოს მარტივად გასაგები, განჭვრეტადი და იმ სიზუსტით ჩამოყალიბებული, რომ ინდივიდს შესაძლებლობა მისცეს, დაარეგულიროს საკუთარი ქცევა. სასამართლოს პოზიციით, მსგავსად საქმისა ***ს. და მარფეი გაერთიანებული სამეფოს წინააღმდეგ***, მოცემულ შემთხვევაშიც, მსჯელობის საგანს წარმოადგენდა, კანონის საფუძველზე პირად ცხოვრებაში ჩარევა რამდენად იყო აუცილებელი დემოკრატიულ საზოგადოებაში. პერსონალურ მონაცემთა შეგროვების, გამოყენებისა და შენახვის ლეგიტიმური მიზანი დანაშულის გამოაშკარავებაა. უფლებაში ჩარევა უნდა იყოს ლეგიტიმური მიზნის პროპორციული და არსებობდეს ამის მწვავე სოციალური საჭიროება.

[214] ხელმისაწვდომია: https://bit.ly/3kyp6pX წვდომის თარიღი: 12.11.2021

ევროპული სასამართლოს გადაწყვეტილების თანახმად, პერსონალურ მონაცემთა დაცვას ფუნდამენტური მნიშვნელობა აქვს პირის პირადი და ოჯახური ცხოვრების პატივისცემის უფლებით სარგებლობისათვის. შესაბამისად, სახელმწიფო უწყებებმა პირადი ცხოვრების დაცვის სათანადო გარანტიების არსებობა უნდა უზრუნველყონ. შენახული ინფორმაცია არ უნდა სცდებოდეს იმ მიზანს, რისთვისაც ის დამუშავდა და არ უნდა ინახებოდეს იმაზე მეტი ვადით, ვიდრე ეს საჭიროა. სასამართლომ ასევე ხაზი გაუსვა უდანაშაულო პირების სტიგმატიზაციის რისკსაც, რადგან მათი მონაცემების შენახვა ზუსტად ისევე ხორციელდება, როგორც მსჯავრდებული პირების. იმ არგუმენტს, რომ ანაბეჭდების შენახვით პოლიცია შეძლებდა მ.კ. დაეცვა სხვა დამნაშავის მიერ მისი იდენტობის მითვისებისაგან, სასამართლომ უპასუხა, რომ ამ მიდგომით პოლიციას მოუწევდა ბაზაში შეეტანა მთელი საფრანგეთის მოსახლეობის პერსონალური მონაცემები, რაც ნამდვილად გადაჭარბებული და არარელევანტური ზომა იქნებოდა.

ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ დაირღვა კონვენციის მე-8 მუხლი და განმარტა, რომ უდანაშაულო ადამიანის პერსონალური მონაცემების 25 წლით შენახვა არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში.

4.3. გორენი გაერთიანებული სამეფოს წინააღმდეგ (2020)

საქმეზე ***გორენი გაეიტიანებული სამეფოს წინააღმდეგ***[215] პირის დნმ-ის პროფილი, ანაბეჭდები და ფოტოსურათი პოლიციის საინფორმაციო ბაზაში ინახებოდა სამართალდარღვევის სიმძიმესა და განუსაზღვრელი ვადით შენახვის საჭიროებაზე მითითების, ასევე, შენახვის რეალური გადახედვის შესაძლებლობის გარეშე. ადამიანის უფლებათა ევროპულმა სასამართლომ ევროპული კონვენციის მე-8 მუხლის დარღვევა დაადგინა.

ფაქტობრივი გარემოებები

2008 წლის ოქტომბერში, მომჩივანი ავტომანქანას მართავდა ალკოჰოლური თრობის ქვეშ, რისთვისაც მას მაგისტრატმა სასამართლომ 50 გირვანქა სტერლინგის ოდენობით ჯარიმა დააკისრა და ერთი წლის განმავლობაში მართვის უფლება ჩამოართვა. ამასთან, მსგავსი სამართალდარღვევისთვის კანონი ასევე ითვალისწინებდა თავისუფლების აღკვეთას. მომჩივნის მიმართ ეს ზომა არ გამოყენებულა, თუმცა მას ნასამართლევის სტატუსი მიენიჭა (ნასამართლობა 2013 წელს გაქარწყლდა).

2009 წელს, მომჩივნის წარმომადგენელმა ჩრდილოეთ ირლანდიის პოლიციის სამსახურს მიმართა და მისი დაცვის ქვეშ მყოფის დნმ-ს ნიმუშის, ანაბეჭდებისა და ფოტოსურათის განადგურება ან მომჩივნისთვის დაბრუნება მოითხოვა. 2015 წელს, მისი მოთხოვნის საფუძველზე, დნმ-ს ნიმუში განადგურდა, თუმცა დნმ-ის პროფილი, ანაბეჭდები და ფოტოსურათი ბაზაში ისევ ინახებოდა.

[215] ხელმისაწვდომია: https://bit.ly/3HrOXd5 წვდომის თარიღი: 12.11.2021

პერსონალური მონაცემების წაშლაზე უარის ეროვნულ დონეზე გასაჩივრებით გორენმა ვერ მიიღო სასურველი შედეგი. კონვენციის მე-8 მუხლის დარღვევაზე მითითებით, მან ადამიანის უფლებათა ევროპულ სასამართლოს მიმართა.

სასამართლოს შეფასება

ადამიანის უფლებათა ევროპული სასამართლოს 2020 წლის 13 ივნისის გადაწყვეტილების თანახმად, მოცემულ საქმეში, დანაშაულის აღკვეთის ლეგიტიმური მიზნით მომჩივნის პერსონალური მონაცემების შენახვამ პირადი და ოჯახური ცხოვრების პატივისცემის უფლების დარღვევა გამოიწვია. მსგავსად ზემოთ განხილული საქმეებისა, სასამართლომ მოცემულ გადაწყვეტილებაშიც განმარტა, რომ პერსონალური მონაცემების შენახვა უფლებაში ჩარევას წარმოადგენდა, რაც ემსახურებოდა დანაშაულის აღკვეთის ლეგიტიმურ მიზანს. ამგვარი ჩარევა უნდა ყოფილიყო პროპორციული და აუცილებელი დემოკრატიულ საზოგადოებაში.

ევროპის საბჭოს წევრი ქვეყნების უმრავლესობა ნასამართლევი პირების მონაცემების შენახვას განსაზღვრული ვადით ითვალისწინებდა. გაერთიანებული სამეფო კი იმ მცირე ქვეყნების რიცხვში შედიოდა, რომელთა კანონმდებლობა უვადო შენახვის შესაძლებლობას იძლეოდა. შესაბამისად, მას უნდა დაესაბუთებინა ეფექტური დაცვის გარანტიების არსებობა. სასამართლოს განმარტებით, იმის გათვალისწინებით, რომ სახელმწიფოს უფლებამოსილებები იყო ბუნდოვანი და ხელმისაწვდომი ტექნოლოგიები კი - უფრო და უფრო კომპლექსური, პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზება განსაკუთრებულ მნიშვნელობას იძენდა.

გადაწყვეტილებაში აღნიშნულია, რომ საქმე ***ს. და მახფეხი გაერთიანებული სამეფოს წინააღმდეგ*** განსხვავდებოდა მოცემული შემთხვევისგან და ამ საქმეში, ნასამართლობიდან გამომდინარე, მომჩივნის სტიგმატიზაციის იდენტური რისკი არ არსებობდა. სასამართლოს შეფასებით, გორენის ბიომეტრიული მონაცემები ინახებოდა მის მიერ ჩადენილი სამართალდარღვევის სიმძიმის ხარისხსა და განუსაზღვრელი ვადით მათი შენახვის განგრძობად (უწყვეტ) საჭიროებაზე მითითების გარეშე. მომჩივანს არ ჰქონდა შესაძლებლობა, მოეთხოვა მონაცემების შენახვის გადახედვა, რამდენადაც არ არსებობდა ნორმა, რომელიც მას მონაცემების წაშლის მოთხოვნის შესაძლებლობას მისცემდა, მათი შენახვის საჭიროების არარსებობის, მომჩივნის ასაკის, გასული დროის ან მომჩივნის ამჟამინდელი პიროვნული მდგომარეობის გამო.

გადაწყვეტილების მიხედვით, გაერთიანებული სამეფო გასცდა მისთვის მინიჭებულ მიხედულების ფარგლებს და ვერ დაიცვა ბალანსი დაპირისპირებულ საჯარო და კერძო ინტერესებს შორის, შესაბამისად, დაირღვა კონვენციის მე-8 მუხლი.

4.4. პ.გ. და ჯ.ჰ. გაერთიანებული სამეფოს წინააღმდეგ (2001)

საქმეზე ***პ.გ. და ჯ.ჰ. გაერთიანებული სამეფოს წინააღმდეგ***[216] ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ გამოძიებისას სამართალდამცავთა მიერ განხორციელებული ფარული მოსმენითა და ხმის ნიმუშების მოპოვების მიზნით პოლიციის განყოფილებაში მომჩივანთა თანხმობის გარეშე მოსასმენი აპარატის დამონტაჟებით კონვენციით გარანტირებული პირადი ცხოვრებისა და მიმოწერის ხელშეუხებლობის უფლება დაირღვა.

ფაქტობრივი გარემოებები

პოლიციამ შეტყობინება მიიღო იმის თაობაზე, რომ პირველი მომჩივანი და ბ. მომდევნო დღეებში ფულის ამგროვებელი ფურგონის დაყაჩაღებას გეგმავდნენ და დამატებითი დეტალების გამოსარკვევად, ბ.-ს ბინაში მოსასმენი აპარატი დააყენა. პოლიცია ფარული მოსმენების განხორციელებისას ხელმძღვანელობდა მეთოდური რეკომენდაციებით (ე.წ. „გაიდლაინებით“), ხოლო ნორმატიულად ეს პროცესი მოწესრიგებული არ იყო. ამავდროულად, პოლიციამ სატელეკომუნიკაციო კომპანიიდან გამოითხოვა ბინიდან განხორციელებული ზარებისა და აბონენტის საუბრების ხანგრძლივობის აღმრიცხველი ამონაწერი. საბოლოოდ, დანაშაული არ მომხდარა - ეჭვმიტანილები ჯგუფური ყაჩაღობის დაგეგმვის ბრალდებით დააკავეს. სამართალდამცავებს სურდათ ეჭვმიტანილის ხმის ნიმუშები მათ ხელთ არსებული ჩანაწერებისთვის შეედარებინათ, თუმცა დაკავებულებმა ხმის ნიმუშების მიცემაზე უარი განაცხადეს, რის გამოც მათ საკანში ფარული მოსასმენი აპარატი დამონტაჟდა. საქმის განხილვისას სასამართლომ ყველა მტკიცებულება დასაშვებად ცნო, ხოლო დანაშაულის სიმძიმიდან გამომდინარე, პირის პირად ცხოვრებაში ჩარევა გამართლებულად მიიჩნია. სააპელაციო სასამართლომ საქმის განხილვაზე უარი თქვა იმ მიზეზით, რომ ამის საფუძველი არ არსებობდა.

სასამართლოს შეფასება

ადამიანის უფლებათა ევროპულმა სასამართლომ ბინაში მოსასმენი აპარატის დაყენება ფარული მოსმენების მომწესრიგებელი კანონმდებლობის არსებობის გარეშე პირადი ცხოვრების უფლების დარღვევად მიიჩნია. სამართალდამცავები ხელმძღვანელობდნენ ე.წ. „გაიდლაინებით“, თუმცა მათ სავალდებულო ძალა არ გააჩნდა და საჯაროდ ხელმისაწვდომიც არ იყო. შედეგად, სასამართლომ დაადგინა, რომ პირადი ცხოვრების უფლებაში ჩარევა „კანონმდებლობის შესაბამისად“ არ განხორციელებულა.

მომჩივნები მიუთითებდნენ, რომ ბ.-ს ბინაში არსებული ტელეფონით განხორციელებული ზარების შესახებ ინფორმაციის პოლიციის მიერ მოპოვება კონვენციის მე-8 მუხლით გათვალისწინებულ უფლებაში ჩარევას წარმოადგენდა. თუმცა სასამართლომ განმარტა, რომ კანონმდებლობაში

[216] ხელმისაწვდომია: https://bit.ly/3kw16DX წვდომის თარიღი: 12.11.2021.

ინფორმაციის შენახვისა და განადგურების მარეგულირებელი ნორმების არარსებობის მიუხედავად, განხორციელებული ზომები მაინც „კანონის შესაბამისად“ ითვლებოდა, რადგან დეტალური რეგულირების ნაკლებობა თვითნებობის რისკს არ წარმოშობდა. მონაცემებით არ ხდებოდა არც საუბრის შინაარსის და არც ზარების მიმღები/განმახორციელებელი პირების იდენტიფიცირება.

რაც შეეხება სამართალდამცავთა მიერ ხმის ნიმუშების თანხმობის გარეშე მოპოვებას, სასამართლომ კიდევ ერთხელ გაუსვა ხაზი, რომ ადამიანის პირადი ურთიერთობები, მათ შორის, საჯარო ადგილას სხვებთან ინტერაქცია, შესაძლებელია, პირადი ცხოვრების უფლების დაცვის ქვეშ მოექცეს. მიუხედავად იმისა, რომ ფარული ჩაწერა ხმის ნიმუშების ასაღებად იყო გამიზნული და საუბრის შინაარს არ შეეხებოდა, ჩაწერა მიმდინარეობდა განუწყვეტლივ, შესაძლებელი იყო მონაცემების გაანალიზება და მისი მიზანი პირდაპირ უკავშირდებოდა პირის იდენტიფიცირებას, რის გამოც ადგილი ჰქონდა მომჩივნების პერსონალური მონაცემების დამუშავებას და პირადი ცხოვრების უფლებაში ჩარევას.

სასამართლომ მიუთითა, რომ არ არსებობდა კანონმდებლობით დადგენილი საფუძველი, რაც სამართალდამცავებს მომჩივნის თანხმობის გარეშე ხმის ჩაწერის უფლებას მისცემდა, მათ შორის, პოლიციის განყოფილებაში. პრინციპი, რომელიც მოითხოვს, შიდა კანონმდებლობამ უზრუნველყოს თვითნებობისა და ფარული საგამოძიებო ღონისძიებების ბოროტად გამოყენებისგან დაცვის გარანტიები, ყველა შემთხვევაზე ვრცელდება, მათ შორის, პოლიციის განყოფილებაში ხმის ჩაწერაზე. ამდენად, სასამართლომ განმარტა, რომ ხმის ნიმუშების ასაღებად პირთა თანხმობის გარეშე საუბრის ჩაწერა არ განხორციელებულა „კანონის შესაბამისად“ და შედეგად, კონვენციის მე-8 მუხლის დარღვევა დაადგინა.

4.5. ეიქაგერი საფრანგეთის წინააღმდეგ (2017)

საქმეზე ***ეიქაგერი საფრანგეთის წინააღმდეგ,***[217] ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ ბიოლოგიური ნიმუშების ხანგრძლივი ვადით შენახვის, ასევე მათი განადგურების შესაძლებლობის არარსებობის გამო, დნმ-ის პროფილების შენახვის მომწესრიგებელი რეგულაციები, რომლებსაც მომჩივანი ნიმუშის აღებაზე უარის თქმით აპროტესტებდა, მონაცემთა სუბიექტს დაცვის საკმარისი გარანტიებით ვერ უზრუნველყოფდა. შესაბამისად, დნმ-ის ნიმუშის აღებაზე უარის თქმის გამო მომჩივნისათვის პასუხისმგებლობის დაკისრება მისი პირადი ცხოვრების პატივისცემის უფლებას არღვევდა. აქედან გამომდინარე, სასამართლომ დაადგინა, რომ დაირღვა კონვენციის მე-8 მუხლი.

ფაქტობრივი გარემოებები

მომჩივანი მონაწილეობდა პროფკავშირების მიერ ორგანიზებულ მიტინგში, სადაც მან წინააღმდე-

[217] ხელმისაწვდომია: https://bit.ly/3n8wg5K წვდომის თარიღი: 12.11.2021

გობა გაუწია ჟანდარმერიას და მათ ქოლგით დარტყმები მიაყენა. ის დააკავეს და სასამართლომ მისი საქმე დაჩქარებული, გამარტივებული წესით განიხილა და 2 თვით თავისუფლების აღკვეთა მიუსაჯა. კანონით გათვალისწინებული წესით, პროკურორმა მისგან დნმ-ის ნიმუშის აღება მოითხოვა, რაზეც მან უარი განაცხადა. სასამართლომ ის დააჯარიმა, ხოლო სააპელაციო სასამართლომ ეს გადაწყვეტილება ძალაში დატოვა. უზენაესმა სასამართლომ საქმე განსახილველად არ მიიღო და მიუთითა, რომ ქვემდგომმა სასამართლომ დამაჯერებლად და დასაბუთებულად უპასუხა საჩივარს.

სასამართლოს შეფასება

სასამართლომ კიდევ ერთხელ აღნიშნა, რომ ინდივიდის პირადი მონაცემების შენახვის ფაქტი მისი პირადი ცხოვრების პატივისცემის უფლებაში ჩარევას თავისთავად უტოლდება, მიუხედავად იმისა, შემდგომ ეს მონაცემები გამოიყენება თუ არა. ამავდროულად, მოსახლეობის დასაცავად, დანაშაულის პრევენციისა თუ დამნაშავეთა დასჯის მიზნით, სახელმწიფო ორგანოებს შეუძლიათ მონაცემთა ბაზები შექმნან. თუმცა, ასეთი მონაცემი არ უნდა შეგროვდეს იმგვარად, რომ გამოიწვიოს მაქსიმალურად დიდი რაოდენობისა და ხანგრძლივი ვადით ინფორმაციის შენახვა.

მიუხედავად იმისა, რომ მომჩივნის უარის გამო, FNAEG-ში (საფრანგეთის დნმ-ის ეროვნული მონაცემთა ბაზა) მისი ბიოლოგიური მონაცემები არ ინახებოდა, დაჯარიმების თაობაზე ეროვნული სასამართლოს მიერ მიღებული გადაწვეტილება პირის პირადი ცხოვრების უფლებაში ჩარევას გაუტოლდა. უფლებაში ჩარევა კანონის შესაბამისად განხორციელდა და დანაშაულის პრევენციის ლეგიტიმურ მიზანს ემსახურებოდა. შესაბამისად, ევროპულ სასამართლოს უნდა გამოეკვლია, იყო თუ არა ჩარევა აუცილებელი დემოკრატიულ საზოგადოებაში.

მიუხედავად იმისა, რომ კერძო და საჯარო ინტერესებს შორის სამართლიანი ბალანსის განსაზღვრა სახელმწიფოს მიხედულების ფარგლებში ექცევა, თავისუფალი მოქმედების ფარგლები მრავალ ფაქტორზეა დამოკიდებული, მათ შორის, მზღუდავი ღონისძიების ხასიათსა და მიზანზე. როდესაც საქმე პირის პირადი ცხოვრების ან იდენტობის განსაკუთრებით მნიშვნელოვან ასპექტს შეეხება, სახელმწიფოსთვის მინიჭებული მიხედულების ფარგლები უფრო ვიწროა. ეროვნულმა კანონმდებლობამ უნდა უზრუნველყოს პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების არსებობა, განსაკუთრებით მაშინ, როცა მონაცემები ავტომატურ დამუშავებას ექვემდებარება. ეს კი გულისხმობს, რომ მონაცემები უნდა შეგროვდეს მიზნის პროპორციულად და არ ინახებოდეს იმაზე ხანგრძლივი ვადით, რაც მიზნის მისაღწევად არის საჭირო.

მიუხედავად იმისა, რომ საფრანგეთის სისხლის სამართლის საპროცესო კანონმდებლობით პირის დნმ-ის შენახვის 40 წლიანი ვადა ამ მონაცემების შენახვის მაქსიმალური ხანგრძლივობა იყო (იმ შემთხვევაში, როცა დანაშაული სიმძიმის განსაკუთრებულ ხარისხს აღწევდა), ეროვნულ ხელისუფლებას ეს ჩანაწერი არ დაუკონკრეტებია და არ მიუღია სხვა დამატებითი წესი, რაც სხვადასხვა დანაშაულისთვის განსხვავებულ ვადას დაადგენდა. შედეგად, განსაზღვრული 40 წელი პრაქტიკაში შენახვის არა მაქსიმალურ, არამედ ზოგად ხანგრძლივობას უტოლდებოდა.

ეროვნული კანონმდებლობა განსაზღვრავდა დანაშაულთა ამომწურავ ჩამონათვალს, რომლის ჩადენის შემთხვევაში, პირის ბიოლოგიური მონაცემი შენახვას ექვემდებარებოდა. ეს დანაშაულები

სიმძიმის სხვადასხვა ხარისხით ხასიათდებოდა. მათ შორის იყო ისეთი მძიმე დანაშაულები, როგორიც არის ტერორიზმი, ტრეფიკინგი და სხვა. მიტინგზე ჟანდარმერიისთვის წინააღმდეგობის გაწევა და მათთვის ქოლგით დარტმის მიყენება სიმძიმის ხარისხით მნიშვნელოვნად განსხვავდებოდა ზემოთხსენებული დანაშულებისგან. ამავდროულად, მონაცემთა წაშლის მოთხოვნა შეეძლოთ მხოლოდ დანაშაულში ეჭვმიტანილებს და არა მსჯავრდებულ პირებს. ევროპულმა სასამართლომ მიიჩნია, რომ აუცილებელია მსჯავრდებულ პირებსაც ჰქონდეთ რეგისტრირებული მონაცემების წაშლის მოთხოვნით მიმართვის პრაქტიკული შესაძლებლობა.

ამდენად, სასამართლომ მიიჩნია, რომ პირის დნმ-ის პროფილის შენახვის ხანგრძლივობისა და ამ მონაცემის წაშლის შესაძლებლობის არარსებობის გათვალისწინებით, კანონმდებლობა მომჩივანს საკმარისი დაცვის გარანტიებით ვერ უზრუნველყოფდა. შესაბამისად, საჯარო და კერძო ინტერესებს შორის სამართლიანი ბალანსი დაცული არ იყო. ეს ფაქტები საკმარისი აღმოჩნდა სასამართლოსთვის მიეჩნია, რომ ეროვნული ხელისუფლება მისთვის მინიჭებულ მიხედულების ფარგლებს გასცდა და პირის პირადი ცხოვრების პატივისცემის უფლებაში არაპროპორციულად ჩაერია. ამდენად, ევროპულმა სასამართლომ დაადგინა, რომ მოცემულ შემთხვევაში ჩარევა არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში.

5. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებები

ამ თავში განხილულია ევროკავშირის მართლმსაჯულების სასამართლოს მიერ მიღებული ორი გადაწყვეტილება, რაც უკავშირდება ბიომეტრიული მონაცემების დამუშავებას.

5.1. მაიკე შვარცი ქალაქ ბოხუმის წინააღმდეგ (2013)

საქმე ***მაიკე შვარცი ქალაქ ბოხუმის წინააღმდეგ***[218] შეეხებოდა პასპორტის გასაცემად თითის ანაბეჭდების დამუშავებას. განმცხადებელმა პასპორტის აღების მიზნით შესაბამის ორგანოს მიმართა, თუმცა მან უარი განაცხადა ანაბეჭდების აღების სავალდებულო პროცედურაში მონაწილეობაზე. შედეგად, მან პასპორტის გაცემაზე უარი მიიღო. შვარცმა სასამართლოს მიმართა და თითის ანაბეჭდების აღების გარეშე პასპორტის გაცემა მოითხოვა. ის მიუთითებდა, რომ ანაბეჭდების აღებასთან დაკავშირებულ რეგულაციას არ ჰქონდა სამართლებრივი საფუძველი, წარმოშობდა პროცედურულ ხარვეზს და ლახავდა ევროკავშირის ძირითად უფლებათა ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებულ უფლებებს. ადმინისტრაციულმა სასამართლომ No 2252/2004 რეგულაციის 1(2) მუხლის ვალიდურობის საკითხის გადასაჭრელად ევროკავშირის მართლმსაჯულების სასამართლოს მიმართა.

სასამართლოს შეფასებით, ანაბეჭდების აღებასთან დაკავშირებული ევროკავშირის რეგულაცია საფუძვლიანია ორი მიზეზის გამო: 1) ის მიღებულია სამართლებრივ ბაზაზე დაყრდნობით - საზღვრის კონტროლისთვის; 2) ის ემსახურება დოკუმენტის მფლობელის იდენტიფიცირებისა და პასპორტის ვალიდურობის დადგენის მიზანს.

სასამართლომ გადაწყვეტილებაში მიუთითა, რომ ანაბეჭდები არის პერსონალური მონაცემი და მათი დამუშავება პირად ცხოვრებაში ჩარევაა. მოცემულ შემთხვევაში, შეფასების საგანია, თუ რამდენად გამართლებულია ეს ჩარევა. სასამართლოს პოზიციით, ანაბეჭდების აღების კიდევ ერთი მიზანს ევროკავშირის ტერიტორიაზე არალეგალური შესვლის აღკვეთა წარმოადგენს და შესაბამისად, რეგულაცია ევროკავშირის საერთო საზოგადო ინტერესს შეესატყვისება. გამოსაკვლევია, თუ რამდენად საჭიროა თაღლითობის გამოსავლენად ამ მეთოდის გამოყენება. სასამართლოს შეფასებით, ანაბეჭდების აღება არ ატარებს ინტიმურ ხასიათს, მეტიც ის პირს არ უქმნის იმაზე მეტ ფიზიკურ ან მენტალურ დისკომფორტს, ვიდრე პასპორტისთვის ფოტოსურათის გადაღება. ამასთან, ის წარმოადგენს მიზნის მიღწევის ეფექტურ საშუალებას, რამდენადაც მკვეთრად ამცირებს თაღლითობის რისკს.

სასამართლომ აღნიშნა, რომ ანაბეჭდების აღების ალტერნატივა თვალის ფერადი გარსის სკანირებაა, რაც, საქმეში წარმოდგენილი მტკიცებულებების გათვალისწინებით, არ დასტურდება, რომ ჩარევის ნაკლები ხარისხით ხასიათდება. გარდა ამისა, ანაბეჭდების ამომცნობი ტექნოლოგია უფრო განვითარებული და ნაკლებად ძვირადღირებულია, ვიდრე თვალის ფერადი გარსის მაიდენტიფიცირებელი მოწყობილობები. შესაბამისად, პირველი უფრო გამოსადეგია საყოველთაო გამოყენებისათვის.

გადაწყვეტილებაში ნათქვამია, რომ სასამართლოსთვის არ არის ცნობილი სხვა საშუალების

[218] ხელმისაწვდომია: https://bit.ly/3CfQrTE წვდომის თარიღი: 13.11.2021.

შესახებ, რომელიც ერთი მხრივ, ეფექტურად გამოავლენს გაყალბებული პასპორტის გამოყენების შემთხვევებს და მეორე მხრივ, ნაკლებ საფრთხეს შეუქმნის ქარტიის მე-7 და მე-8 მუხლებით განმტკიცებულ უფლებებს.

სასამართლომ აღნიშნა, რომ ანაბეჭდების გამოყენება არ უნდა გასცდეს იმ ფარგლებს, რაც საჭიროა ლეგიტიმური მიზნის მისაღწევად. კანონმდებლობით გათვალისწინებული უნდა იყოს მონაცემების დაცვის სათანადო გარანტიები, რათა მათი ბოროტად გამოყენება არ მოხდეს. განსახილველ შემთხვევაში, უფლებაში ჩარევა გამართლებულია, რამდენადაც ანაბეჭდების აღება გაყალბებული პასპორტის გამოყენებისგან დაცვის ლეგიტიმური მიზნის მისაღწევად საჭირო და პროპორციული ზომაა.

5.2. ვ.პ. ვიღემსი და სხვები ნეთის მერის და სხვების წინააღმდეგ (2015)

საქმეზე ***ვ.პ. ვიღემსი და სხვები ნეთის მეჰის და სხვების წინააღმდეგ***[219] ევროკავშირის მართლმსაჯულების სასამართლომ დაადგინა, რომ N2252/2004 რეგულაცია არ ქმნიდა სამართლებრივ საფუძველს, რომ წევრ ქვეყნებს რეგულაციის შესაბამისად შეგროვებული ბიომეტრიული მონაცემები პასპორტისა და სხვა სამგზავრო დოკუმენტების გაცემის გარდა სხვა მიზნებით არ გამოეყენებინათ. სასამართლომ განმარტა, რომ ბიომეტრიული მონაცემების შემდგომი შეგროვებისა და გამოყენების რეგულირება წევრი სახელმწიფოების კომპეტენციას მიეკუთვნება.

განმცხადებლებმა უფლებამოსილ ორგანოებს პასპორტისა (3 განმცხადებელი) და პირადობის მოწმობის (1 განმცხადებელი) აღების თხოვნით მიმართეს. თუმცა, მათ უარი ეთქვათ განაცხადის დაკმაყოფილებაზე, ვინაიდან არ სურდათ ციფრული თითის ანაბეჭდის აღება.

მომჩივნები მთავარ სხდომაზე მიუთითებდნენ, რომ უფლებამოსილი ორგანოსთვის ბიომეტრული მონაცემის მიწოდება მათი პირადი ცხოვრების უფლებაში სერიოზული ჩარევა იყო. მათი მონაცემები შეინახებოდა სამ საშუალებაზე და შესაძლოა, საბოლოოდ, სახელმწიფო ცენტრალურ მონაცემთა ბაზაში აღმოჩენილიყო. ამავდროულად, მათთვის ცნობილი არ იყო, ვის მიუწვდებოდა ხელი მათ პერსონალურ მონაცემებზე.

პირველმა ინსტანციამ მათი სარჩელი არ დააკმაყოფილა. ეს გადაწყვეტილება გასაჩივრდა ზემდგომ სასამართლოში, რომელმაც ევროკავშირის მართლმსაჯულების სასამართლოს შემდეგი კითხვებით მიმართა:

1. N2252/2004 რეგულაციის პირველი მუხლის მე-3 პუნქტი[220] უნდა განიმარტოს თუ არა იმგვარად, რომ

[219] ხელმისაწვდომია: https://bit.ly/3kxqlFV წვდომის თარიღი: 13.11.2021

[220] N2252/2004 რეგულაციის პირველი მუხლის მე-2 და მე-3 პუნქტები: პასპორტი და სამგზავრო დოკუმენტები უნდა მოიცავდეს შესანახ საშუალებას, სადაც მოთავსებული იქნება სახის ფოტოსურათი და თითის ანაბეჭდები ოპერაციულად შეთავსებადი ფორმატით. მონაცემები უნდა იყოს დაცული, შესანახი საშუალება უნდა იყოს საკმარისად ტევადი, რათა შეძლოს მონაცემების კონფიდენციალურობის, ნამდვილობისა და ერთიანობის უზრუნველყოფა. რეგულაცია არ ვრცელდება პირადობის დამადასტურებელ მოწმობებზე ან დროებით პასპორტებსა და სამგზავრო დოკუმენტებზე, რომელთა ძალაში ყოფნის პერიოდი 12 თვე ან ნაკლებია.

ეს რეგულაცია არ ვრცელდება წევრი ქვეყნების მიერ მათ მოქალაქეებზე გაცემულ პირადობის დამადასტურებელ მოწმობებზე, მათი მოქმედების ვადისა და სამგზავრო დოკუმენტად მათი გამოყენების შესაძლებლობის მიუხედავად?

2. N2252/2004 რეგულაციის მე-4 მუხლის მე-3 პუნქტი უნდა განიმარტოს თუ არა იმგვარად, რომ წევრი ქვეყნები ვალდებულნი არიან უზრუნველყონ, რომ რეგულაციის შესაბამისად შეგროვებული და შენახული ბიომეტრიული მონაცემების შეგროვება, დამუშავება და გამოყენება არ მოხდება პასპორტისა და სხვა სამგზავრო დოკუმენტების გაცემის გარდა სხვა მიზნებით?

ევროკავშირის მართლმსაჯულების სასამართლომ პირველ შეკითხვასთან მიმართებით აღნიშნა, რომ რეგულაცია არ ვრცელდება პირადობის დამადასტურებელ მოწმობებზე და ევროკავშირის კანონმდებლობამ მკაფიოდ გადაწყვიტა ამ დოკუმენტების რეგულაციის ფარგლებს მიღმა დატოვება. რაც შეეხება მეორე კითხვას, რეგულაციით მონაცემთა შეგროვებისა და შენახვის საკითხები არ წესრიგდება. რეგულაცია არ ქმნის წევრი ქვეყნებისთვის მონაცემთა შესანახად მონაცემთა ბაზების შექმნის სამართლებრივ საფუძველს და ეს საკითხი ექსკლუზიურად წევრი სახელმწიფოების კომპეტენციას მიეკუთვნება.

რეგულაცია არ მოითხოვს წევრი სახელმწიფოებისგან კანონმდებლობით იმის უზრუნველყოფას, რომ ამ რეგულაციის შესაბამისად შეგროვებული და შენახული ბიომეტრიული მონაცემები არ იქნას დამუშავებული ან გამოყენებული სხვა მიზნებით, გარდა პასპორტისა და სხვა სამგზავრო დოკუმენტის გაცემისა. ეს საკითხი რეგულაციის მოწესრიგების სფეროში არ ექცევა. ამდენად, სასამართლომ მეორე შეკითხვას უარყოფითი პასუხი გასცა.

6. შეჯამება

გენეტიკური და ბიომეტრიული მონაცემები, რომლითაც პირის უნიკალური იდენტიფიცირება ხდება, ევროპული სტანდარტებით განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს მიეკუთვნება. ამგვარი მონაცემების დამუშავებამ ერთდროულად შეიძლება მოიტანოს მნიშვნელოვანი სარგებელიც და საფრთხე შეუქმნას ადამიანის ძირითად უფლებებსა და თავისუფლებებს. მათი გამოყენების აუცილებელი წინაპირობა იმ მიზნის მკაფიოდ და ნათლად განსაზღვრაა, რისთვისაც ისინი გროვდება და მუშავდება. ამასთან, მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რაც საჭიროა ლეგიტიმური მიზნის მისაღწევად. გარდა ამისა, მონაცემთა შენახვის ვადა არ უნდა აღემატებოდეს იმ ვადას, რაც აუცილებელია იმ მიზნის მისაღწევად, რისთვისაც ისინი შეგროვდა და მუშავდება.

განსაკუთრებით მნიშვნელოვანია სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება, რათა მონაცემები დაცული იყოს შემთხვევითი, არაავტორიზებული ან უკანონო წვდომის, გამოყენების, შეცვლის, გამჟღავნების, განადგურების ან დაზიანებისაგან. მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელია მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (“privacy by design”) და მონაცემთა დაცვა პირველად პარამეტრად (“privacy by default”).

ბიომეტრიული მონაცემების გამოყენება, განსაკუთრებით კი სახის ამოცნობა მონაცემთა სუბიექტის უფლებებისთვის მომეტებულ რისკს შეიცავს. არსებითად მნიშვნელოვანია, რომ ასეთი ტექნოლოგიების გამოყენება მოხდეს ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით გათვალისწინებული პრინციპების დაცვით. მიუხედავად იმისა, რომ ამ ტექნოლოგიების გამოყენება ეფექტურად მიიჩნევა, დამმუშავებლებმა, პირველ რიგში, უნდა შეაფასონ მონაცემთა დამუშავების გავლენა მონაცემთა სუბიექტების ძირითად უფლებებსა და თავისუფლებებზე და ლეგიტიმური მიზნის მისაღწევად განიხილონ ნაკლებად მზღუდავი საშუალებები. [221]

რაც შეეხება გენეტიკურ მონაცემებს, ის ერთ ინდივიდს სხვებისგან გამოარჩევს, ამჟღავნებს სხვადასხვა დაავადებისადმი ადამიანის გენეტიკურ მიდრეკილებას და ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციას, ადგენს პირის ეთნიკურ წარმომავლობასა და ფიზიკურ მახასიათებლებს. გასათვალისწინებელია ისიც, რომ გენეტიკური მონაცემების დაუმუშავებელი მასალიდან მიღება და მოპოვება ადვილია. ამავე დროს, ამგვარ მონაცემებს დაავადების პროგნოზირების უნარი აქვს. მათ განსაკუთრებულად სენსიტიურს ხდის ის ფაქტი, რომ ინფორმაციის რაოდენობა, რაც შესაძლებელია მიღებულ იქნას ამ მონაცემებიდან, ტექნოლოგიებისა და კვლევების წინსვლასთან ერთად იზრდება.

დისკრიმინაციის საფრთხეების თავიდან ასაცილებლად, მნიშვნელოვანია, გენეტიკური მონაცემების დამუშავების მიზნის შეფასება. სწორედ ამგვარად არის შესაძლებელი იმის განსაზღვრა, ამ მონაცემების დამუშავება ატარებს თუ არა დისკრიმინაციულ ხასიათს. ევროპული კანონმდებლობა განსაკუთრებულ ყურადღებას ამახვილებს დასაქმების ან დაზღვევის პროცესში გენეტიკური მონაცემების დამუშავებაზე, ვინაიდან სწორედ ამ კონტექსტში არსებობს დისკრიმინაციის ყველაზე დიდი საფრთხე.

გენეტიკური მონაცემების დამუშავებისას დაცული უნდა იყოს პერსონალურ მონაცემთა დაცვის პრინციპები და საფუძვლები. გენეტიკურ მონაცემთა დამუშავება ხშირად მონაცემთა სუბიექტის

[221] Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, პარ. 73, ხელმისაწვდომია: https://bit.ly/3kFg7nN წვდომის თარიღი: 21.07.2021.

თანხმობას ეფუძნება. მნიშვნელოვანია, რომ თანხმობის გაცემისას მონაცემთა სუბიექტი დამუშავების მიზნებისა და შესაძლო რისკების შესახებ სათანადოდ ინფორმირებული იყოს.

ინფორმაციის მიღების უფლებას მჭიდროდ უკავშირდება მონაცემთა სუბიექტის უფლება, სურვილის შემთხვევაში, უარი განაცხადოს მის შესახებ გენეტიკური ინფორმაციის მიღებაზე. ეს უფლება შესაძლოა ოჯახის წევრებზეც გავრცელდეს, როდესაც, მაგალითად, დამუშავებული მონაცემები სერიოზული დაავადების ან მოულოდნელი კავშირების შესახებ ინფორმაციას ამჟღავნებს.

ტ. შევჩენკოს ქ. 20, 0108
თბილისი, საქართველო

+ 995 32 292 15 14

INFO@IDFI.GE

WWW.IDFI.GE