ტექნოლოგიური განვითარების პირობებში, პერსონალური მონაცემების დაცვა სამართალდამცავი ორგანოების საქმიანობაში

კობა გრიალაშვილი
დოქტორანტი, აღმოსავლეთ ევროპის უნივერსიტეტი
kobagrialashvili@gmail.com

აბსტრაქტი
გლობალიზაციამ ახალი გამოწვევები გააჩინა პერსონალური მონაცემების დამუშავების მიმართულებით. მნიშვნელოვნად გაიზარდა მათი დამუშავების მასშტაბები. ამ მხრივ, აღსანიშნავია სამართლდამცავი ორგანოების მხრიდან მონაცემთა დამუშავების მოცულობა, რამდენადაც კანონმდებლობით დაკისრებული უფლებამოსილების განხორციელების მიზნით, მათ აქვთ როგორც ღია, ასევე ფარული წყაროებიდან მონაცემთა მოპოვებისა და სხვაგვარი დამუშავების შესაძლებლობა, ხოლო ტექნოლოგია საშუალებას აძლევს სამართალდამცავ ორგანოებს, პერსონალური მონაცემები უპრეცედენტო მასშტაბით დაამუშაონ. უნდა აღინიშნოს, რომ პერსონალურ მონაცემთა დაცვის უფლება, ადამიანის უფლებათა ევროპული კონვენციის, ისევე როგორც საქართველოს კონსტიტუციის მიხედვით ცალკე უფლებად არ არის აღიარებული და ის პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცულ სივრცეში არის მოქცეული. თუმცა ევროკავშირმა ამ კუთხით განსხვავებული მიდგომა აირჩია. კერძოდ, 2009 წელს ლისაბონის ხელშეკრულების საფუძველზე ამოქმედდა „ფუნდამენტურ უფლებათა ქარტია“, სადაც ცალკე უფლებად არის მიჩნეული პერსონალურ მონაცემთა დაცვის უფლება. აღნიშნული განაპირობა ტექნოლოგიური განვითარების შედეგად გამოწვეულმა რისკებმა. შესაბამისად პერსონალური მონაცემების დამუშავება სამართალდამცავი საქმიანობის მიზნებისთვის წარმოადგენს ჩარევას პირადი ცხოვრების დაცვის და პერსონალური მონაცემების დაცვის უფლებებში. თუმცა ეს უფლებები არ არის აბსოლუტური ხასიათის. იმისათვის რომ აღნიშნულ უფლებებში ჩარევა იყოს გამართლებული, აუცილებელია ბალანსის დაცვა, ერთი მხრივ, შესაბამისი პირის/სუბიექტის უფლებასა და, მეორე მხრივ, სამართალდამცავი ორგანოების ეფექტიანად ფუნქციონირებას შორის.
მოხსენებაში ყურადღება იქნება გამახვილებული თუ რა გამოწვევები გააჩნია გლობალიზაციამ და ტექნოლოგიურმა პროგრესმა პერსონალური მონაცემების დაცვის მიმართულებით. განსაკუთრებით მაშინ, თუ მონაცემებს სამართალდამცავი ორგანოები ამუშავებენ. განხილული იქნება ამ მიმართულებით ევროპის საბჭოს და ევროკავშირის მიდგომები. ამასთან მოხდება საქართველოს კანონმდებლობის შესაბამისობის შეფასება ევროპულ რეგულაციებთან, სამართალდამცავი ორგანოების საქმიანობის განხორციელების დროს, თუ რა სტანდარტით არის დაცული პერსონალური მონაცემები. გაიცემა შესაბამის რეკომენდაციები.

საკვანძო სიტყვები: პერსონალური მონაცემი, სამართალდამცავი ორგანოების საქმიანობა, ტექნოლოგიური განვითარება.

JEL: K42; D83; L86

DOI: 10.52244/c2025.43

შესავალი

სწრაფმა ტექნოლოგიურმა განვითარებამ ახალი გამოწვევები გააჩინა მონაცემების დამუშავების მიმართულებით. მნიშვნელოვნად გაიზარდა მონაცემების დამუშავების მასშტაბები. მონაცემების კანონიერად დამუშავებასა და მათ დაცვას დიდი მნიშვნელობა ენიჭება, განსაკუთრებით საჯარო სექტორში. აქ მონაცემები დიდი მოცულობით მუშავდება, რაც დაკავშირებულია სახელმწიფო უწყებების ეფექტიან ფუნქციონირებასთან, ფიზიკური პირების უფლებების დაცვასთან და სახელმწიფო სერვისების მიწოდებასთან. ამ მხრივ, აღსანიშნავია სამართლდამცავი ორგანოების მხრიდან მონაცემთა დამუშავების მოცულობა, რამდენადაც კანონმდებლობით დაკისრებული უფლებამოსილების განხორციელების მიზნით, მათ აქვთ როგორც ღია, ასევე ფარული წყაროებიდან მონაცემთა მოპოვებისა და სხვაგვარი დამუშავების შესაძლებლობა. მონაცემების დამუშავება სამართალდამცავი მიზნებისთვის წარმოადგენს ჩარევას პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებაში.

მოცემული ნაშრომის ძირითადი მიზანია, ევროკავშირის და ევროპის საბჭოს რეგულაციებისა და ადამიანის უფლებათა ევროპული სასამართლოს მიერ დადგენილ სტანდარტების მიმოხილვა, პერონალური მონაცემების დაცვის მიმართულებით, როდესაც მონაცემებს სამართალდამცავი ორგანოები ამუშავებენ. ასევე ეროვნული კანონმდებლობის მიმოხილვა შესაბამის ჭრილში. საკითხის აქტუალობის პარალელურად, ნაშრომი წარმოადგენს პირველ ქართულ მეცნიერულ კვლევას, სადაც შემოთავაზებულია მონაცემთა დაცვის სტანდარტი, სამართალდამცავი ორგანოების საქმიანობის განხორციელებისას. ამ სფეროში განსაკუთრებულად მნიშვნელოვანია მონაცემთა დამუშავების დეტალური წესების არსებობა, მონაცემთა დაცვის ძლიერი და თანმიმდევრული ჩარჩო, რომელსაც ექნება აღსრულების ეფექტიანი მექანიზმები. შესაბამისად, კვლევის საგანია თეორიული სამართლებრივი საფუძვლების შემუშავება, რომელიც სართაშორისო საუკეთესო სტანდარტების შესაბამისად უზრუნველყოფს ფიზიკური პირის მონაცემების დაცვას, როდესაც სამართალდამცავი ორგანოები ამ მონაცემებს ამუშავებენ.

პერსონალურ მონაცემთა დაცვის ზოგადი კონცეფცია

პერსონალურ მონაცემთა დაცვის თვალსაზრისით ევროკავშირი სამაგალითოდ მიიჩნევა მსოფლიოს მასშტაბით. ევროკავშირის მონაცემთა დაცვის სტანდარტები ემყარება

გამოცდილებასა და კულტურას, რომელიც ათწლეულების განმავლობაში ყალიბდებოდა ევროპის ქვეყნებში. ევროპაში მონაცემთა დაცვის სტანდარტები დაფუძნებულია ევროპის საბჭოს 1981 წლის 28 იანვარს მიღებულ კონვენციაზე „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“[1] (შემდეგში 108-ე კონვენცია), და ევროკავშირის ინსტრუმენტებზე, მათ შორის, როგორიცაა ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ“[2] (მონაცემთა დაცვის საერთო რეგულაცია - GDPR), და ევროპის პარლამენტისა და ევროპის საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU)2016/68 „კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი მიმოცვლის შესახებ“[3] (შემდეგში - LED დირექტივა). ასევე, ადამიანის უფლებათა ევროპული სასამართლოსა და ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტულ სამართალზე.[4] რამდენიმე წლის წინ ევროპის საბჭოს კანონმდებლობა გადაიხედა და პერსონალური მონაცემების საკითხები ახლებურად მოწესრიგდა. რეფორმის პაკეტი მოიცავს ევროპის საბჭოს 108-ე კონვენციის მოდერნიზებას[5] (შემდეგში 108+ კონვენცია), 108-ე კონვენციის შესწორების ოქმით CETS No.223,[6] რითიც გაუმჯობესდა სამართლებრივი საფუძვლები, მათ შორის, საპოლიციო დანაყოფების მიერ თავიანთი საქმიანობის განხორციელებისას, ტექნოლოგიური საშუალებების გამოყენებით, პერსონალურ მონაცემთა დაცვის ძირითადი უფლების მაღალი სტანდარტით დაცვის მიზნით. ხოლო ევროკავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვა დამოუკიდებელ ფუნდამენტურ უფლებად არის აღიარებული. 2009 წელს ლისაბონის ხელშეკრულების საფუძველზე ძირითად უფლებათა ქარტიას[7] სამართლებრივად სავალდებულო ძალა მიენიჭა და იგი ევროკავშირის პირველადი კანონმდებლობის ნაწილი გახდა.

---

[1] „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენცია. 28.01.1981. https://rm.coe.int/convention-108-for-the-protection-of-individuals.

[2] „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ“ ევროპარლამენტისა და საბჭოს რეგულაცია (EU) 2016/679. 27.04.2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[3] „კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი მიმოცვლის შესახებ. ევროპის პარლამენტისა და ევროპის საბჭოს დირექტივა (EU) 2016/68 27.04. 2016

[4] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო. ევროპის საბჭო. 2018 წლის გამოცემა. გვ. 3.

[5] 2018 წლის 10 ოქტომბერს გაიხსნა ხელმოსაწერად.

[6] Council of Europe. 2018. Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), CETS: 223.

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

პერსონალურ მონაცემთა დაცვის უფლება

პერსონალურ მონაცემთა დაცვის უფლება, ევროკავშირის კანონმდებლობისგან განსხვავებით, ადამიანის უფლებათა ევროპული კონვენციის, ისევე როგორც საქართველოს კონსტიტუციის მიხედვით ცალკე უფლებად არ არის აღიარებული და ის პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცულ სივრცეში არის მოქცეული. საქართველოს კონსტიტუციის მე-15 მუხლი[8] განამტკიცებს პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებებს. ეს უფლებები ემსახურება ინდივიდის პირადი სფეროს ამა თუ იმ ასპექტის დაცვას. იქედან გამომდინარე, რომ სამართლებრივი და დემოკრატიული სახელმწიფოს მთავარი ფასეულობა ადამიანია, შესაბამისად მაღალია მისი პირადი სფეროს პატივისცემის ხარისხი. საქართველოს საკონსტიტუციო სასამართლომ საქმეზე, ლონდა თოლორაია და სახალხო დამცველის საქართველოს პარლამენტის წინააღმდეგ აღნიშნა, რომ ადამიანის პირადი ცხოვრების დაცულობას უზრუნველყოფს კონსტიტუციით გათვალისწინებული სახელმწიფოს შესაბამისი ვალდებულებები: „ერთი მხრივ, არსებობს სახელმწიფოს პოზიტიური ვალდებულება, უზრუნველყოს პირადი ცხოვრების პატივისცემა და ამ უფლებით ეფექტიანი სარგებლობა, რაც, პირველ რიგში, გულისხმობს პიროვნების თავისუფალი განვითარების ხელშემშლელი გარემოებების, შეზღუდვების უგულებელყოფას, აღკვეთას. ხოლო, მეორე მხრივ, სახელმწიფოს აქვს ნეგატიური ვალდებულება, არ ჩაერიოს კონსტიტუციის მე-15 მუხლით დაცული უფლებებით სარგებლობაში და, შესაბამისად, უზრუნველყოს პიროვნების დაცვა მის პირად ცხოვრებაში სახელმწიფო ხელისუფლების ორგანოების ან თანამდებობის პირების მხრიდან თვითნებური ჩარევისაგან“.[9] რაც შეეხება ევროპის საბჭოს კანონმდებლობას, პერსონალურ მონაცემთა დაცვა მიეკუთვნება ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით დაცულ უფლებებს. მართალია, კონვენციაში ნახსენები არ არის პერსონალურ მონაცემთა დაცვა, თუმცა ევროპულმა სასამართლომ თავის პრაქტიკაში განმარტა, რომ პერსონალური მონაცემები დაცულია კონვენციის მე-8 მუხლით („პირადი და ოჯახური ცხოვრების დაცულობის უფლება“).[10] შესაბამისად, ანალოგიური ძირითადი უფლების სტატუსის მატარებელია პერსონალურ მონაცემთა დაცვის ფუნდამენტური უფლებაც.[11] სწორედ ევროპული კონვენციის მე-8 მუხლზე მითითებით ევროპის საბჭოს მინისტრთა კომიტეტმა მიიღო არაერთი მნიშვნელოვანი საერთაშორისო სამართლებრივი დოკუმენტი პერსონალურ მონაცემთა დაცვის შესახებ. როგორც აღინიშნა, 2009 წელს ლისაბონის ხელშეკრულების საფუძველზე ამოქმედდა „ფუნდამენტურ უფლებათა ქარტია“ და იგი ევროკავშირის პირველადი კანონმდებლობის ნაწილი გახდა. ხელშეკრულების მიღებამ მონაცემთა დაცვის სამართლებრივი

---

[8] საქართველოს კონსტიტუცია, მუხლი 15.

[9] საქართველოს საკონსტიტუციო სასამართლოს 2022 წლის 17 ნოემბრის N1/9/1673,1681 გადაწყვეტილება საქმეზე ლონდა თოლორაია და სახალხო დამცველი საქართველოს პარლამენტის წინააღმდეგ, II, 17.

[10] კორკელია. კ, ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებების კრებული. 2019-2023. პერსონალურ მონაცემთა დაცვა. გვ.8.

[11] გოშაძე, კ. (2020). პერსონალურ მონაცემთა დაცვის ძირითადი უფლება. „იურისტების სამყარო“, თბილისი, გვ.42

განვითარება ახალ საფეხურზე აიყვანა და ევროკავშირის დონეზე კანონმდებლობით განამტკიცა პერსონალურ მონაცემთა დაცვის უფლება. მისი მოქმედება ვრცელდება ყველა სფეროზე, მათ შოროს საპოლიციო საქმიანობაზე. აქვე აღსანიშნავია, რომ ევროკავშირის შესახებ ხელშეკრულება[12] ითვალისწინებს ზედამხედველობის ინსტრუმენტების აუცილებლობას არსებობას, რათა ეფექტურად იქნეს დაცული მონაცემთა დაცვის წესები. სწორედ ეს გახდა GDPR-ის და LED დირექტივის მიღების საფუძველი. ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლით განმტკიცდა პერსონალურ მონაცემთა დაცვის უფლება. ხსენებულ მუხლი მოიცავს მანამდე არსებული აქტების სულისკვეთებას და მასში გათვალისწინებულია უფლების დაცვის ქმედითი ინსტრუმენტებიც. ამასთან, 2018 წლიდან ამოქმედდა GDPR და LED დირექტივა, რომელმაც დაადგინა პერსონალურ მონაცემთა დაცვის ახალი სტანდარტები, შემოიღო მნიშვნელოვანი ცნებები და განმარტებები, ტექნოლოგიურის განვითარების გათვალისწინებით.

პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ კონვენცია და შესწორების ოქმი

ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლზე საფუძველზე ევროპის საბჭომ მიიღო არაერთი მნიშვნელოვანი რეზოლუცია თუ სხვა სახის სამართლებრივი აქტი. საბოლოოდ 1981 წელს ხელმოსაწერად გაიხსნა 108-ე კონვენცია. ხსენებული კონვენცია დღესაც მოქმედი სავალდებულო ძალის მქონე აქტია და ის ვრცელდება ყველა სახის მონაცემთა დამუშავებაზე, როგორც კერძო, ისე საჯარო სექტორში, მათ შორის, მართლმსაჯულებისა და სამართალდამცველი ორგანოების საქმიანობაზე. საქართველოს პარლამენტის მიერ აღნიშნული დოკუმენტის რატიფიცირება მოხდა 2005 წელს, ხოლო ძალაში 2006 წელს შევიდა, რის შედეგადაც 108-ე კონვენცია საქართველოს კანონმდებლობის ნაწილი გახდა.[13] მოგვიანებით, ციფრული ეპოქის გამოწვევებზე საპასუხოდ და უფრო ეფექტიანი აღსრულების მექანიზმის დანერგვის მიზნით, საჭირო გახდა ამ კონვენციის მოდერნიზება. შედეგად შემუშავდა კონვენციის შესწორების ოქმი, 108+ კონვენცია. ეს დოკუმენტი 2018 წელს გაიხსნა ხელმოსაწერად,[14] თუმცა საქართველოს მისი ხელმოწერა და რატიფიცირება არ განუხორციელებია.[15] რაც შეეხება ხსენებული დოკუმენტის შინაარსს, კონვენციის მოდერნიზებული ტექსტი გვთავაზობს სიახლეებს მონაცემთა დამუშავების რეგულირებისას, მათ შორის შემოთავაზებულია მონაცემთა დამუშავების პროპორციულობის, მინიმიზაციისა და კანონიერების პრინციპების უზრუნველყოფის მეტი გარანტიები. ასევე უზრუნველყოფილია დამუშავებისას მეტი

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT.

[13] კონვენცია არ ექვემდებარება ECtHR-ის სასამართლო კონტროლს, თუმცა ამ სასამართლოს პრეცედენტული სამართალი ითვალისწინებს მას ევროპული კონვენციის მე-8 მუხლის კონტექსტში. წლების მანძილზე ECtHR საკუთარ გადაწყვეტილებებში მიუთითებს, რომ პერსონალურ მონაცემთა დაცვა პირადი და ოჯახური ცხოვრების პატივისცემის უფლების მნიშვნელოვანი ნაწილია.

[14] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[15] ამ ეტაპისთვის, დოკუმენტს 32 ხელმომწერი ჰყავს, ხოლო 11-მა სახელმწიფომ მოახდინა მისი რატიფიცირება. საქართველო ევროპის საბჭოს იმ 8 წევრ ქვეყანას შორის არის, ვისაც ჯერ არ განუხორციელებია ოქმის ხელმოწერა და რატიფიცირება.

გამჭვირვალობა. რაც გულისხმობს მონაცემთა სუბიექტისათვის მონაცემთა დამმუშავებლის ვინაობის და მისამართის, დამუშავების საფუძველის და მიზნის, მონაცემთა მიმღებების და დამუშავებული მონაცემების კატეგორიების, მონაცემთა სუბიექტის უფლებების რეალიზების საშუალებების შესახებ ინფორმაციის მიწოდებას. კონვენციით გაზრდილია მონაცემთა სუბიექტის უფლებების დაცვის გარანტიები, რაც გულისხმობს სუბიექტის უფლებას მის შესახებ, რომ მნიშვნელოვანი გადაწყვეტილება არ იქნას მიღებული მხოლოდ ავტომატიზებული საშუალებების გამოყენებით, მისი მოსაზრების გათვალისწინების გარეშე. მოთხოვნის საფუძველზე, გასაგები ფორმით მიიღოს ინფორმაცია მისი პერსონალური მონაცემების დამუშავების შესახებ. მოითხოვოს მისი პერსონალური მონაცემების დამუშავების შეწყვეტა. მნიშვნელოვანი საკითხია ასევე, ის რომ მოდერნიზებული კონვენცია დაუშვებლად მიიჩნევს ეროვნული უსაფრთხოებისა და თავდაცვის მიზნებისთვის მონაცემთა დამუშავებაზე სრულ გამონაკლისს. გამონაკლისი დაიშვება მხოლოდ ცალკეულ დებულებებთან დაკავშირებით, კანონით გათვალისწინებულ შემთხვევებში, თუ ეს პატივს სცემს ფუნდამენტური უფლებებისა და თავისუფლებების არსს და აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში. გამონაკლისის დაშვების მიუხედავად, კონვენცია ცალსახად ითვალისწინებს სახელმწიფო უსაფრთხოებისა და თავდაცვის მიზნებისათვის პერსონალურ მონაცემთა დამუშავებაზე ეფექტური და დამოუკიდებელი ზედამხედველობის უზრუნველყოფის ვალდებულებას. ასევე ახლებურად ჩამოყალიბდა სენსიტიურ (განსაკუთრებული კატეგორიის) მონაცემთა ჩამონათვალი, გენეტიკური, ბიომეტრიული, ეთნიკური კუთვნილების შესახებ მონაცემების დამატების სახით. კონვენციით განსაზღვრულია მონაცემთა დაცვის წესების დარღვევისას მისი დეკლარირების/შეტყობინების ვალდებულება საზედამხედველო (მაკონტროლებელი) ორგანოსთვის, მათ შორის მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შემთხევაში, თუკი ამ ფაქტმა შეიძლება მნიშვნელოვნად შელახოს მონაცემთა სუბიექტის უფლებები. Privacy by Design პრინციპის (მონაცემთა დაცვის წესების განსაზღვრა შიდაორგანიზაციული არქიტექტურის მიხედვით) დაცვა სავალდებულოდ მოითხოვება. ამასთან, კონვენციით გარანტირებულია შესაბამისი უფლებები ხელოვნურ ინტელექტთან მიმართებით და შემოთავაზებულია მონაცემთა საერთაშორისო გადაცემისთვის მეტად ცხადი სამართლებრივი რეგულირების რეჟიმი.

მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის

როგორც აღინიშნა, ევროკავშირში ცალკე სამართლებრივი აქტით არის დარეგულირებული მონაცემთა დამუშავების პროცესი სამართალდამცავი ორგანოების მიერ. განსხვავებით მონაცემთა დაცვის საერთო რეგულაციისა (GDPR), რომელსაც ფორმალურად პირდაპირ მოქმედი ძალა გააჩნია ევროკავშირის ყველა წევრ სახელმწიფოში, LED დირექტივა ამგვარი ბუნებით არ გამოირჩევა, ვინაიდან მისი იმპლემენტირება მოითხოვს ევროკავშირის თითოეულ წევრ სახელმწიფოში შესაბამისი, შიდა ეროვნული კანონმდებლობის მიღებას. LED დირექტივით გათვალისწინებულია სამართალდამცავი ორგანოების

თავისებურებები, რაც გულისხმობს მეტად ფართო ინსტრუმენტების არსებობას, რათა შესაბამისმა ორგანოებმა ეფექტურად განახორციელონ მათზე კანონმდებლობით დაკისრებული ფუნქცია-მოვალეობები. ზოგადად შეიძლება ითქვას, რომ სამართალდამცავი ორგანოების საქმიანობის სპეციფიკურობის გათვალისწინებით, დირექტივა ევროკავშირის ფარგლებში ადგენს ყოვლისმომცველ ჩარჩოს მონაცემთა დაცვის მაღალი სტანდარტის უზრუნველსაყოფად; მისი მოქმედება ვრცელდება პერსონალურ მონაცემთა მთლიანად ან ნაწილობრივ ავტომატური საშუალებებით დამუშავებაზე. ამასთან, ხაზგასასმელია ის გარემოება, რომ დირექტივის მოქმედება ვრცელდება ასევე იმ პერსონალური მონაცემების არაავტომატური საშუალებებით დამუშავებაზე, რომლებიც წარმოადგენენ ფაილური სისტემის ნაწილს ან ფაილურ სისტემაში შესატანად მუშავდება. პირის მონაცემების დაცვა არ უნდა იყოს დამოკიდებული ტექნოლოგიების გამოყენების საკითხზე, რათა დავიდან არ იქნეს აცილებული დირექტივის მოქმედება. შესაბამისად დირექტივის მოქმედება ვრცელდება როგორც ავტომატური საშუალებით დამუშავებულ, ისე ხელით დამუშავებულ მონაცემებზე, რომელიც მიზანიც არის შემდგომში ფაილურ სისტემაში შენახვა. რაც შეეხება დირექტივის მოქმედების ფარგლებს, იგი ადგენს ევროკავშირის წევრი ქვეყნებისთვის მინიმალურ სტანდარტს, რაც არ გამორიცხავს იმას, რომ წევრმა სახელმწიფოებმა უფრო მაღალი სტანდარტები დაადგინონ. შესაბამისად LED დირექტივის მოქმედება ვრცელდება მონაცემთა დამუშავერბისას ევროკავშირის სახელმწიფოების შესაბამისი ორგანოების საქმიანობაზე, როდესაც ისინი მუშავდება დანაშაულის პრევენციის, გამოძიების, დევნის ან სასჯელის აღსრულების მიზნებისთვის, მათ შორის, საზოგადოებრივი უსაფრთხოებისთვის, საფრთხეებისგან დაცვისა და მათი პრევენციის მიზნით. იმ შემთხვევაში თუ იგივე ორგანოები მონაცემებს ამუშავებენ ჩამოთვლისგან განსხვავებული მიზნებისთვის, მათზე გავრცელდება მონაცემთა დაცვის საერთო რეგულაცია. რაც შეეხება ხსენებული დირექტივის მიზანს, განზოგადებულად შეგვიძლია ვთქვათ, რომ LED დირექტივის ძირითადი მიზანია საპოლიციო და სისხლის სამართლის სფეროში ფიზიკური პირების ფუნდამენტური უფლებების დაცვის დონის ამაღლება, ასევე, ევროკავშირის წევრ სახელმწიფოებს შორის პერსონალური მონაცემების გაცვლის გაუმჯობესება, რათა ერთიანი წესებით შეძლონ მონაცემების დაცვა. აქ იგულისხმება სახელმწიფოს პოზიტიური ვალდებულება, დაიცვას ფიზიკური პირების ფუნდამენტური უფლებები და თავისუფლებები. ეს ეხება პერსონალური მონაცემების დაცვის უფლებასა და ნეგატიურ ვალდებულებას, რომ არ შეფერხდეს პერსონალური მონაცემების გაცვლა ევროკავშირის ფარგლებში სამართალდამცავი ორგანოების მიერ, როდესაც ასეთი მონაცემების გაცვლა სავალდებულოა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით და პერსონალური მონაცემების დამუშავება არ არის აკრძალული ფიზიკური პირების დაცვასთან დაკავშირებული სახვა მიზეზების გამო. იმისათვის, რათა დირექტივა იყოს გამოყენებული, უნდა დაკმაყოფილდეს როგორც პირადი, ასევე მატერიალური მოქმედების სფერო. სხვა სიტყვებით, მონაცემთა დამუშავება უნდა განხორციელდეს შესაბამისი სამართალდამცავი ორგანოს მიერ (პირადი მოქმედების სფერო) დანაშაულის პრევენციის, გამოძიების, დევნის ან სასჯელის აღსრულების მიზნებისთვის, მათ შორის საზოგადოებრივი უსაფრთხოებისთვის საფრთხეებისგან

დაცვისა და მათი პრევენციის მიზნით (მატერიალური მოქმედების სფერო).[16] ევროკავშირის წევრი ქვეყნების კანონმდებლობა შესაძლებელია განსხვავდებოდეს ქმედების სისხლის სამართლის დანაშაულად დასჯადობას მიხედვით. ერთი და იგივე ქმედება, რაც შეიძლება ერთ ქვეყანაში დანაშაულს წარმოადგენდეს, სხვა ქვეყანაში შეიძლება ადმინისტრაციულ სამართალდარღვევად ან სულაც საფრთხის ხარისხის მცირე მნიშვნელობის გამო, არ ითვლებოდეს კანონდარღვევად. სისხლის სამართალი ძალიან ღრმად არის ფესვგადგმული ამა თუ იმ ქვეყნის შიდა პოლიტიკურ, სოციალურ და კონსტიტუციურ სისტემაში, ეს არის სფერო, რომელიც ხშირად ასოცირდება სახელმწიფოს სუვერენული ძალაუფლების მონოპოლიასთან. მაგალითად, დირექტივაზე შემუშავებისას, კომისიის ექსპერტთა ჯგუფის ჩატარებული შეხვედრების ოქმებიდან ჩანს, რომ წევრ სახელმწიფოებს შორის კონსენსუსი არ არსებობდა იმასთან დაკავშირებით, თუ როგორ უნდა მომხდარიყო განსხვავება სისხლის სამართლის დანაშაულის, ადმინისტრაციული სამართალდარღვევის ან წვრილმანი ქმედებისგან იმ წევრ სახელმწიფოებში, რომელთა სამართლებრივი სისტემები ასეთ განსხვავებას არ ახდენს. საბოლოოდ, ევროკომისიის გადაწყვეტილებით იმპლემენტაციის პროცესში წევრ სახელმწიფოებს შეუძლიათ დაეყრდნონ სისხლის სამართლის დანაშაულის ცნებას, როგორც ეს განსაზღვრულია მათ ეროვნულ სამართლებრივ სისტემებში.[17] ზემოთ აღნიშნული საკითხი საყურადღებოა იმდენად, რამდენადაც არსებობს დანაშაულთან ბრძოლის მოტივით LED დირექტივის ფართოდ განმარტების რისკები, მაშინ როდესაც ტექნოლოგიური განვითარება ხელს უწყობს კომპეტენტურ ორგანოებს პერსონალური მონაცემები გამარტივებულად შეაგროვონ თანამედროვე მეთვალყურეობის საშუალებებით და მონაცემთა ბაზების გამოყენებით, ასევე კერძო პირების მიერ შეგროვებულ მონაცემებზე წვდომის შესაძლებლობით. ნებისმიერი ბუნდოვანება მნიშვნელოვან კითხვებს გააჩენს იმ პირთა უფლებების მდგომარეობის შესახებ, რომელთა მონაცემებიც შეიძლება დამუშავდეს ხსენებული მოტივით. აქვე, მხედველობაშია მისაღები დანაშაულის ჩადენის ან ზიანის რისკის გარდუვალობა, რამაც შესაძლოა გაამართლოს LED დირექტივის სტანდარტის გამოყენება. მონაცემთა დამუშავების მიზანს, ასევე, წარმოადგენს სასჯელის აღსრულება. აქაც ყურადღება უნდა გამახვილდეს სასჯელის მნიშვნელობაზე, რადგან შესაძლებელია შინაარსობრივად მხოლოდ სისხლის სამართლის მნიშვნელობით სასჯელი არ იგულისხმებოდეს ამ ტერმინის ქვეშ, და ასევე მოიცავდეს ადმინისტრაციულ ან/და დისციპლინურ სახდელებს. ეს საკითხი ეროვნული კანონმდებლობით შეიძლება დაკონკრეტდეს, რადგან ზოგიერთი ადმინისტრაციული ან დისციპლინური სახდელი შეიძლება შინაარსობრივად ძალიან ჰგავდეს სისხლის სამართლებრივი მიზნებისთვის სასჯელის აღსრულებას. მაგალითად, როდესაც მსჯავრდებული სასჯელის მოხდის პერიოდში ჩაიდენს დისციპლინურ გადაცდომას, რთულია ამ დროს დისციპლინური სახდელის შეფარდების დროს, არ გავრცელდეს LED დირექტივით დადგენილი რეგულაცია.

---

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

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

დანაშაულისგან განცალკევებულად უნდა განვიხილოთ საზოგადოებრივი უსაფრთხოების საკითხი, როდესაც არსებობს საფრთხისგან მისი დაცვის აუცილებლობა. ამ ფრაზამ რეალურად გააფართოვა დირექტივის მოქმედების ფარგლები და არსებობს რისკი, რომ იგი გასცდეს დანაშაულის შემადგენლობას და გავრცელდეს მონაცემთა დამუშავების ფართო სპექტრზე, ვინაიდან წევრი ქვეყნების ეროვნული კანონმდებლობის შესაბამისად, საზოგადოებრივი უსაფრთხოების მნიშვნელობაში შესაძლებელია მოიაზრებოდეს სხვა სიკეთეების დაცვა, როგორიცაა საზოგადოებრივი ჯანმრთელობის საკითხი და სხვა. LED დირექტივაში ამ ფრაზის დამატებამ გამოწვია აზრთა სხვადასხვაობა, ამასთანავე სამეცნიერო ლიტერატურაშიც გაკრიტიკებულია ეს საკითხი. „დირექტივის გამოყენების სფეროს გაფართოება გარდაუვლად წარმოშობს კითხვებს ინდივიდების უფლებების ღირებულებასთან, ასევე, ასეთი საკანონმდებლო გადაწყვეტის აუცილებლობასა და პროპორციულობასთან დაკავშირებით. ამის გათვალისწინებით, ზოგიერთი ავტორი გვთავაზობს დირექტივის პირველი მუხლიდან ფრაზის „მათ შორის საზოგადოებრივი უსაფრთხოებისთვის საფრთხეებისგან დაცვისა და მათი პრევენციის“ ამოღებას“.[18]

LED დირექტივა მნიშვნელოვან ყურადღებას უთმობს ასევე მონაცემთა დამუშავების პრინციპებს. სამართალდამცავი ორგანოების სპეციფიკური საქმიანობის მიუხედავად, რაც გულისხმობს მონაცემთა დამუშავებისას სხვა საჯარო ორგანოებისგან განსხვავებულ მიდგომას, ისინი მაინც შეზღუდულნი არიან სახელმძღვანელო პრინციპებით. სამართალდამცავი ორგანოების მიერ შეგროვებული მონაცემები უნდა აკმაყოფილებდეს კანონიერებისა და სამართლიანობის, განსაზღვრულობის და პროპორციულობის, სიზუსტისა და უსაფრთხოების დაცვის კრიტერიუმებს.[19] პერსონალური მონაცემები უნდა შეგროვდეს დირექტივის ფარგლებში განსაზღვრული, მკაფიო და ლეგიტიმური მიზნებისთვის და არ უნდა დამუშავდეს ისეთი მიზნებისთვის, რომლებიც შეუთავსებელია სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის ან სისხლის სამართლის სასჯელების აღსრულების მიზნებთან, მათ შორის, საზოგადოებრივი უსაფრთხოებისთვის საფრთხეებისგან დაცვისა და მათი პრევენციის მიზანთან. ეს მიზნები თავისთავად ძალიან ფართოა შესაბამისი პრინციპის დასაკმაყოფილებლად. აუცილებელია რომ მიზანი იყოს კონკრეტულად განსაზღვრული, რათა გამოჩნდეს თუ რატომ მუშავდება კონკრეტული მონაცემები. მხოლოდ სამართალდამცავი ორგანოების საქმიანობისთვის ზოგადი საჭიროება ვერ ჩაითვლება ლეგიტიმურ მიზნად. ევროკაშირის მართლმსაჯულების სასამართლოს განმარტების თანახმად, საქმეში Inspektor v. Inspektorata kam Visshia sadeben savet, როდესაც მონაცემები შეგროვდა დანაშაულის გამოძიების მიზნებისთვის და შემდგომ ეს მონაცემები დამუშავდა სისხლის სამართლის დევნის მიზნით, ეს ორი მოქმედება განსხვავებულ მიზნებს ემსახურება, მაშინ როდესაც შესაბამისი სისხლის სამართლის გამოძიება უშედეგოდ დასრულდა.[20] დირექტივით გათვალისწინებული პრინციპები, მნიშვნელოვნად განსხვავდება მონაცემთა დაცვის საერთო რეგულაციის ექვივალენტური

[18] იქვე.
[19] LED დირექტივა, მუხლი 4.
[20] CJEU, C-180/21, Inspektor v. Inspektorata kam Visshia sadeben savet, (2022), 44.

დებულებებისგან. ისინი შექმნილია სპეციალურად სამართალდამცავი ორგანოების საჭიროებებისა და მათი დამუშავების საქმიანობის კონკრეტული ხასიათისთვის.

ევროკავშირში მონაცემთა სუბიექტის უფლებები მონაცემთა დაცვის კანონმდებლობის ძირითადი კომპონენტია. LED დირექტივის ზოგადი მიზანია მონაცემთა სუბიექტების უფლებების გაძლიერება. აღნიშული მიზნის უზრუნველსაყოფად ის ითვალისწინებს ევროკავშირის წევრი სახელმწიფოების ვალდებულებას, შეიმუშავოს ისეთი მექანიზმები, რომლებიც უზრუნველყოფს მონაცემთა დამმუშავებლის ვალდებულებას, ხელი შეუწყონ მონაცემთა სუბიექტის უფლებების რეალიზებას. ამისთვის დირექტივა ითვალისწინებს მონაცემთა სუბიექტის უფლებას ინფორმაციის ხელმისაწვდომობაზე, რაც გულისხმობს მისთვის გასაგები ფორმით ინფორმაციის მიღებას დამუშავებისთვის პასუხისმგებელი პირის შესახებ, მონაცემთა დამუშავების მიზნების შესახებ, რომლებისთვისაც მუშავდება მონაცემები. ასევე, უფლებას საზედამხედველო ორგანოსთვის მიმართვის შესახებ და ინფორმაცია მონაცემთა სუბიექტთან დაკავშირებულ მონაცემებთან წვდომის, მათი გასწორების, წაშლის ან დამუშავების შეზღუდვის მოთხოვნის დამუშავებისთვის პასუხისმგებელი პირისთვის წარდგენის უფლების არსებობის შესახებ. გარდა ამისა, კონკრეტულ შემთხვევებში და საკუთარი უფლებების განხორციელების მიზნით, მონაცემთა სუბიექტს უნდა ეცნობოს დამუშავების სამართლებრივი საფუძვლისა და მონაცემების შენახვის ხანგრძლივობის შესახებ, იმდენად, რამდენადაც ასეთი დამატებითი ინფორმაცია აუცილებელია იმ კონკრეტული გარემოებების გათვალისწინებით, რომლებშიც მონაცემები მუშავდება, რათა უზრუნველყოფილი იყოს მონაცემთა სუბიექტის მონაცემების მიმართ სამართლიანი დამუშავება. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია უპასუხოს სუბიექტის მოთხოვნებს, გარდა იმ შემთხვევისა, თუ მოთხოვნები აშკარად უსაფუძვლო ან გადაჭარბებულია.

სუბიექტების უფლებების დასაცავად, LED დირექტივა ასევე ითვალისწინებს მონაცემებზე წვდომის შესაძლებლობას, რაც გულისხმობს სუბიექტის უფლებას, ჰქონდეს წვდომა მის შესახებ დამუშავებულ და შენახულ მონაცემებზე, აგრეთვე იცოდეს ამ მონაცემების კატეგორიები, დამუშავების მიზნები და სამართლებრივი საფუძველი, რაც ადასტურებს მის შესახებ ინფორმაციის დამუშავების კანონიერებას. იქ, სადაც შესაძლებელია, სუბიექტს უნდა მიეწოდოს ინფორმაცია დამუშავების პერიოდულობისა და მონაცემების გადაცემის შესახებ, თუ ვის და სად გადაეცა ინფორმაცია და ვინ არის ამ ინფორმაციის მიმღები. სუბიექტს უფლება აქვს, ასევე იცოდეს დამმუშავებლის მხრიდან მონაცემების გასწორების, წაშლის ან დამუშავების შეზღუდვის შესახებ. აგრეთვე საზედამხედველო ორგანოში საჩივრის შეტანის შესახებ.[21] ამ მუხლის მიზანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ხელი შეუწყოს სუბიექტს, მისთვის გასაგები და ხელმისაწვდომი ფორმით ჰქონდეს წვდომა მის შესახებ არსებულ მონაცემებზე, იმ შემთხვევაში თუ ასეთი მონაცემების დამუშავებას აქვს ადგილი.

მონაცემთა სუბიექტის უფლებების დაცვის მიზნით, დირექტივა, ასევე ითვალისწინებს ისეთი მექანიზმების არსებობას, როგორიც არის მონაცემთა დამუშავების გასწორება, წაშლა და შეზღუდვა. ეს მექანიზმები ხელს უწყობს მონაცემთა სუბიექტს მოახდინოს შესაბამისი რეაგირება როდესაც მისი მონაცემის კანონის დარღვევით მუშავდება. იმ შემთხვევაში თუ

[21] LED დირექტივა, მუხლი 14.

საგამოძიებო ორგანოებში ინახება არაზუსტი მონაცემები, ეს კიდევ უფრო მეტად ზრდის სუბიექტის უფლებების დარღვევის რისკებს. მონაცემების გასწორების საჭიროება ძირითადად მაშინ წარმოიშვება, როცა სუბიექტის შესახებ ინფორმაცია არასწორია ან ფაქტობრივი შეცდომებით არის შეტანილი სამართალდამცავი ორგანოების მონაცემთა ბაზებში. მაგალითად, პირის შესახებ ბიომეტრიულ მონაცემებს შეიძლება არასწორად ინახავდეს პოლიცია, რამაც შეიძლება არსებითი გავლენა მოახდინოს მის პირად ცხოვრებაზე. რაც შეეხება მონაცემების წაშლის საკითხის, ეს სუბიექტის უფლებასა და დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას წარმოადგენს, იმ შემთხვევაში, თუ დარღვეულია მონაცემთა დამუშავების პრინციპები და საფუძვლები, სენსიტიური მონაცემების დამუშავება მოხდა კანონის დარღვევით ან მონაცემების წაშლა გამომდინარეობს დამუშავებისთვის პასუხისმგებელი პირის სამართლებრივი ვალდებულებიდან. ასევე მნიშვნელოვანია, რომ მონაცემთა წაშლა დროულად მოხდეს, რადგან ადამიანის უფლებათა ევროპული სასამართლომ, მონაცემების წაშლის უფლებასთან დაკავშირებით დაადგინა პირადი ცხოვრების უფლების დარღვევა, მაშინ როდესაც პოლიციის ორგანოების მონაცემთა ბაზებში ბრალდებულების შესახებ ინფორმაცია კანონოთ დადგენილი ვადაზე მეტი ხნით ინახებოდა.[22] მონაცემების წაშლის ნაცვლად დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია შეზღუდოს მონაცემების დამუშავება, იმ შემთხვევაში როდესაც მონაცემების ნამდვილობა სადავოა და სიზუსტის დადგენა შეუძლებელია, ასეთ დროს დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია აცნობოს ამის შესახებ სუბიექტს დამუშავების შეზღუდვის მოხსნამდე, ან მონაცემების დამუშავება აუცილებელია მტკიცებულების მიზნებისთვის.

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

დირექტივით გათვალისწინებული ეს უფლებები არ არის აბსოლუტური და ექვემდებარება შეზღუდვას. ეს დაკავშირებულია სამართალდამცავი ორგანოების საქმიანობის სპეციფიკასთან და სახელმწიფოს უტოვებს უფლებას, რომ გაითვალისწინოს გარკვეული ხასიათის გამონაკლისები. ბუნებრივია აქ საჭიროა ბალანსის დაცვა, სუბიექტის უფლების და სამართალდამცავი ორგანოს საქმიანობისთვის საფრთხის შექმნის თავიდან აცილების

[22] ECtHR, S. And Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), 119, 124.

გათვალისწინებით, რა დროსაც შესაძლებელია აღნიშნული ორგანო მონაცემებს ამუშავებდეს ფარული მეთოდებით. ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეზე Roman Zakharov v. Russia, ხაზი გაუსვა იმ გარემოებას, რომ ფარული საგამოძიებო მოქმედებების შემდეგ პირისთვის შეტყობინების განხორციელება დაკავშირებულია სასამართლოში სამართლებრივი დაცვის ეფექტიანობასთან. სასამართლო აღნიშნავს, რომ რუსეთის კანონმდებლობა არ იძლევა საიდუმლო თვალთვალის ზომებისაგან ეფექტიანი სამართლებრივი დაცვის საშუალებას მაშინ, როდესაც მიყურადების ობიექტის წინააღმდეგ არ არის აღძრული სისხლის სამართლის საქმე. შედეგად, „ეროვნული სამართლებრივი დებულებანი, რომელიც არეგულირებს კომუნიკაციების მიყურადებას არ იძლევა ადექვატური და ეფექტიანი დაცვის გარანტიებს თვითნებობისა და უფლების დარღვევის საფრთხისაგან. ეროვნული კანონმდებლობა არ აკმაყოფილებს „კანონის ხარისხის“ მოთხოვნას და ვერ ინარჩუნებს „ჩარევას“ იმ მასშტაბით, რაც გახლავთ „აუცილებელი დემოკრატიულ საზოგადოებაში“.[23]

LED დირექტივა შესაძლებლობას აძლევს ევროკავშირის წევრ სახელმწიფოებს, სამართლებრივი საფუძვლის არსებობის შემთხვევაში შეზღუდონ მონაცემთა სუბიექტის უფლებები თუ არსებობს ლეგიტიმური ინტერესი, ჩარევა აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში და არსებობს სამართალდამცავი ორგანოებისთვის ხელის შეშლის საშიშროება. ანუ თუ ეს აუცილებელია დანაშაულის პრევენციის, გამოძიების, სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების ხელის შეშლის აღკვეთის მიზნით, ასევე ეს მნიშვნელოვანია საზოგადოებრივი და ეროვნული უსაფრთხოების დასაცავად და სხვათა უფლებებისა და თავისუფლებების დასაცავად.[24] შეჯამებისთვის შეიძლება ითქვას, რომ ამ მხრივ LED დირექტივის მიზანია პირი დაცული იყოს სხვისი მხრიდან მონაცემების ბოროტად გამოყენებისგან. ამასთან, ასეთი უფლება შეიძლება დაექვემდებაროს შეზღუდვას, თუმცა იმ ფარგლებში, რამდენადაც ეს მკაცრად აუცილებელია.[25]

საქართველოს კანონმდებლობის მიმოხილვა და თანმდევი გამოწვევები

- 2019 წლის მაისში საქართველოს პარლამენტში დაინიცირდა პერსონალურ მონაცემთა დაცვის შესახებ ახალი კანონპროექტი. განმარტებითი ბარათის თანახმად „პერსონალურ მონაცემთა დაცვის საკანონმდებლო ბაზის ჰარმონიზაცია და კონსოლიდაცია წარმოადგენდა საქართველოს მიერ ევროპის კავშირთან ასოცირების შეთანხმებითა და ასოცირების დღის წესრიგით ნაკისრ ვალდებულებას. ასოცირების შეთანხმების I დანართის თანახმად, საქართველო ვალდებულია უზრუნველყოს პერსონალურ მონაცემთა დაცვის კანონმდებლობის შესაბამისობა ევროკავშირის No95/46/EC დირექტივასთან, ევროპის საბჭოს 108 კონვენციასთან და მის დამატებით ოქმთან, ასევე, ევროკავშირის 2008 წლის 27 ნოემბრის 2008/977/JHA ჩარჩო გადაწყვეტილებასთან და ევროპის საბჭოს მინისტრთა კომიტეტის 1987 წლის 15 ნოემბრის No R (87)15 რეკომენდაციასთან“.[26]

---

[23] ECtHR, Roman Zakharov v. Russia, (Application no. 47143/06), VII.

[24] LED დირექტივა, მუხლი 13.

[25] Kosta, E., Boehm, F., The EU Law Enforcement Directive (LED): A Commentary. 2024, 256.

[26] https://info.parliament.ge/file/1/BillReviewContent/222087.

კანონპროექტი მოიცავდა პერსონალურ მონაცემთა დაცვის სფეროში ევროკავშირში მოქმედი სამართლებრივი აქტების, კერძოდ, მონაცემთა დაცვის საერთო რეგულაციისა (GDPR) და ე.წ. LED დირექტივის (2016/680) იმპლემენტირებას, რის გამოც იგი კომპლექსური და ხანგრძლივი ანალიზის ობიექტი გახდა. საბოლოოდ, 2023 წლის 14 ივნისს კანონპროექტი მესამე მოსმენით მიიღო საქართველოს პარლამენტმა.[27] აქვე აღსანიშნავია, რომ კანონის ძირითადი დებულებები ამოქმედდება 2024 წლის პირველი მარტიდან,[28] რათა საჯარო და კერძო დაწესებულებებს მიეცეთ შესაბამისი დრო კანონით განსაზღვრული ახალი ვალდებულებების გათვალისწინებისთვის. ახალი კანონის მიღებით საქართველოს კანონმდებლობა მეტწილად დაუახლოვდა ევროპულ სტანდარტებს. მიუხედავად ამისა, არის ცალკეული დებულებები, რომლებიც არ არის შესაბამისობაში, იმ რეგულაციებთან, რაზეც სხვადასხვა თავებში გვქონდა საუბარი. ქვემოთ განხილული იქნება შესაბამისი დებულებები.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-2 მუხლის მეორე პუნქტის „გ“ ქვეპუნქტის მიხედვით, კანონის მოქმედება არ ვრცელდება დანაშაულის თავიდან აცილების, გამოძიების, სისხლისსამართლებრივი დევნის, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისთვის სახელმწიფო საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ნახევრად ავტომატური საშუალებებით დამუშავებასა და არაავტომატური საშუალებებით დამუშავებაზე.[29] მნიშვნელოვანი გაანალიზდეს აღნიშნული ჩანაწერის შესაბამისობა ევროპულ კანონმდებლობასთან. მონაცემთა დაცვის მიმართულებით ევროპის კანონმდებლობის ანალიზის დროს აღინიშნა, ევროპის საბჭოს მოდერნიზებული 108+ კონვენცია და ევროკავშირის LED დირექტივა, ორივე მოქმედებს სამართალდამცავი ორგანოების საქმიანობის განხორციელებისას, გარკვეული გამონაკლისებით, თუმცა მოქმედების სფერო აბსოლუტურად გამორიცხული არ არის, მათ შორის არც ეროვნული უსაფრთხოებას მიკუთვნებულ საქმიანობის განხორციელების დროს. პირიქით საუბარის ზედამხედველობის ძლიერი მექანიზმების არსებობაზე. იმისათვის, რომ პერსონალურ მონაცემთა დაცვის კანონის ზემოთხსენებული ნორმა მონაცემთა დაცვით თვალსაზრისით სრულყოფილად იყოს შესაბამისობაში მოყვანილი ევროპულ რეგულაციებთან, ამ საკითხის გაანალიზება უნდა მოხდეს საპოლიციო დირექტივის ჭრილში, ვინაიდან ეს დირექტივა ეხება სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავებას. დირექტივის მიხედვით მისი მოქმედება ვრცელდება კომპეტენტური ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლის სამართლებრივი დევნის, სასჯელთა აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვის მიზნებით პერსონალურ მონაცემთა დამუშავებაზე. ამავე დირექტივით კომპეტენტური ორგანო განმარტებულია როგორც ნებისმიერი საჯარო უწყება, რომლის კომპეტენციაში შედის დანაშაულების თავიდან აცილება, გამოძიება, დადგენა ან სისხლისსამართლებრივი დევნა, ან სასჯელის აღსრულება, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ

[27] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი. 3144-XIმს-Xმპ. 14/06/2023.

[28] ახალი კანონის მიღებამდე მოქმედებდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონი.

[29] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი. 14/06/2023. მუხლი 2.

მიმართული საფრთხეებისგან დაცვა და მათი პრევენცია, ან ნებისმიერი სხვა ორგანო ან უწყება, რომელისთვის წევრ სახელმწიფოს მინდობილი აქვს დანაშაულების თავიდან აცილება, გამოძიება, დადგენა ან სისხლისსამართლებრივი დევნა, ან სასჯელის აღსრულება, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისგან დაცვა და მათი პრევენცია. შესაბამისად, ის რომ პერსონალურ მონაცემთა დაცვის შესახებ კანონის მოქმედება არ ვრცელდება დანაშაულის თავიდან აცილების, გამოძიების, სისხლისსამართლებრივი დევნის, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისთვის სახელმწიფო საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ნახევრად ავტომატური საშუალებებით დამუშავებასა და არაავტომატური საშუალებებით დამუშავებაზე, თავსებადი არ არის ხსენებულ დირექტივასთან. იგივე შეიძლება ითქვას ევროპის საბჭოს კანონმდებლობასთან თავსებადობის თვალსაზრისით. 108+ კონვენციის მოქმედება ვრცელდება მონაცემების როგორც ავტომატიზირებულ, ისე არაავტომატიზირებულ დამუშავებაზე. ამასთანავე, უსაფრთხოების მიზნებისთვის სრული გამონაკლისის გაკეთებას დაუშავებლად მიიჩნევს. გამონაკლისი დაიშვება მხოლოდ ცალკეულ დებულებებთან დაკავშირებით, კანონით გათვალისწინებულ შემთხვევებში, თუ ეს პატივს სცემს ფუნდამენტური უფლებებისა და თავისუფლებების არსს და აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში.

- საქართველოს კანონი „პოლიციის შესახებ“ ითვალისწინებს პირის იდენტიფიკაციას, როგორც ერთ-ერთ პრევენციულ საპოლიციო ღონისძიებას.[30] პირის იდენტიფიკაციის ძირითადი მიზანი საზოგადოებრივი უსაფრთხოების დაცვაა. პირის იდენტიფიკაცია კონკრეტულ ღონისძიებებში გამოიხატება, კერძოდ: თითისა და ხელისგულის ანაბეჭდების აღება, ფოტოსურათის გადაღება, დამახასიათებელი ფიზიკური ნიშნების დაფიქსირება, სიმაღლის გაზომვა, ხმის ჩაწერა, სხვა ბიომეტრიული მონაცემების დაფიქსირება. უპირველეს ყოვლისა, უნდა აღინიშნოს, რომ ეს ღონისძიება არაა პირის კეთილ ნებაზე დამოკიდებული, პოლიციელს უფლება აქვს და ვალდებულია ზემოაღნიშნულ შემთხვევებში განახორციელოს პირის იდენტიფიკაცია. გამომდინარე იქედან, რომ პირის იდენტიფიკაცია წარმოადგენს ადამიანის უფლებებში ინტენსიურ ჩარევას, ამ ღონისძიების განხორციელებისას დგება ოქმი, თუმცა ოქმის შედგენა საჭირო არ არის, თუ პირის იდენტიფიკაცია სპეციალური ელექტრონული პროგრამის გამოყენებით ხორციელდება. როგორც აღინიშნა, საქართველოს კონსტიტუციის მე-15 მუხლი იცავს პირის პირადი ცხოვრების ხელშეუხებლობას.[31] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის თანახმად, ბიომეტრიული მონაცემია ფიზიკური, ფიზიკურ, ფიზიოლოგიურ ან ქცევის მახასიათებელთან (სახის გამოსახულება, ხმის მახასიათებელი ან დაქტილოსკოპიური მონაცემები) დაკავშირებული მონაცემი, რომელიც მისი უნიკალური იდენტიფიცირების ან ვინაობის დადასტურების შესაძლებლობას იძლევა. ბიომეტრიული მონაცემი განსაკუთრებული კატეგორიის მონაცემს წარმოადგენს.[32] ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის თანახმად, ყველას აქვს უფლება, რომ დაცული იყოს მისი პირადი და ოჯახური ცხოვრება, საცხოვრისი და

[30] საქართველოს კანონი „პოლიციის შესახებ,“ 04/10/2013. მუხლი 20.

[31] საქართველოს კონსტიტუცია, მუხლი 15.

[32] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი. 14/06/2023. მუხლი 3.

მიმოწერა. დაუშვებელია ამ უფლების განხორციელებაში საჯარო ხელისუფლების ჩარევა, გარდა ისეთი შემთხვევისა, როდესაც ასეთი ჩარევა ხორციელდება კანონის შესაბამისად და აუცილებელია დემოკრატიულ საზოგადოებაში ეროვნული უშიშროების, საზოგადოებრივი უსაფრთხოების, ქვეყნის ეკონომიკური კეთილდღეობის ინტერესებისათვის, უწესრიგობისა თუ დანაშაულის თავიდან ასაცილებლად, ჯანმრთელობისა ან მორალის, ანდა სხვათა უფლებებისა და თავისუფლებების დასაცავად.[33] ადამიანის უფლებათა ევროპული სასამართლოს მიერ დადგენილი სტანდარტის თანახმად, განსაკუთრებული კატეგორიის მონაცემის (მაგ. ბიომეტრიული) შემოწმება და დამუშავება მკაფიოდ გაწერილი პროცედურებით და სათანადო ლეგიტიმური მიზნის არსებობისას უნდა მოხდეს.[34] საჯარო დაწესებულების ქმედებები უნდა იყოს გამჭვირვალე და დემოკრატიულ პრინციპებთან შესაბამისი.[35] ადამიანის უფლებათა ევროპული სასამართლოს განმარტებით, პერსონალური მონაცემების დამუშავების შესახებ საკანონმდებლო ჩანაწერი უნდა იყოს დეტალური, რომ არ უშვებდეს უფლებამოსილების ბოროტად გამოყენების საფრთხეს.[36] პირის იდენტიფიკაციის მიზნით ხდება პირის შეჩერება. შესაბამისად შეჩერების დროის პროპორციულად იზრდება პოლიციელის მხრიდან პირის დაყოვნების მეტად დასაბუთებულობის მოთხოვნაც. საპოლიციო ღონისძიების განხორციელების ფორმაზე არ უნდა იყოს დამოკიდებული ოქმის შედგენის საკითხი, რადგან აღნიშნული, ფართო უფლებამოსილებას ანიჭებს პოლიციას და საზოგადოებას უკარგავს ბერკეტს, შეამოწმოს რამდენ შემთხვევაში არ დადასტურდა სადავო გარემოებები და ხომ არ იყენებს პოლიცია გადამეტებულად ამ უფლებამოსილებას. ამასთან, ადრესატს ერთმევა უფლება ოქმში დააფიქსიროს შენიშვნა, როდესაც მის მიმართ არ დადასტურდა საეჭვო გარემოებები. მართალია, კანონი სამი დღის შემდეგ მას ინფორმაციის გამოთხოვის უფლებას უტოვებს, მაგრამ აღნიშნული გაუმართლებლად ზღუდავს და ართულებს პირის მდგომარეობას. ამგვარი გართულებული პროცედურა ვერ მიიჩნევა კონვენციის მე-8 მუხლით ნაგულისხმევ ეფექტურ პროცედურულ ჩარჩოდ.

დასკვნა

როგოც ზემოთ აღინიშნა, კვლევის ძირითადი მიზანი იყოს საქართველოს კანონმდებლობის შესაბამისობის შეფასება ევროპულ რეგულაციებთან, სამართალდამცავი ორგანოების საქმიანობისას, თუ რა სტანდარტით არის დაცული პერსონალური მონაცემები. კვლევამ აჩვენა, რომ ადამიანის უფლებებზე დაფუძნებული მიდგომა უნდა იყოს სამართალდამცავი ორგანოების საქმიანობს განხორციელების საფუძველი, მათ შორის პერსონალური მონაცემების დამუშავების დროს. ეროვნული კანონმდებლობა უნდა

---

[33] ევროპის საბჭოს ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია. 04.11.1950. მუხლი 8

[34] Guide on Data protection, Case-law of European Convention on Human Rights CoE, 2021, პარაგრ. 28, 84-119.

[35] Guide on Article 8 of the European Convention on Human Rights, CoE, 2020, პარაგრ. 203-206 .

[36] ბენ ფაიზა საფრთანგეთის წინააღმდეგ (Ben Faiza v. France), Appl. No. 31446/12, 8 February 2018.

უზრუნველყოფდეს პირადი ცხოვრების შეზღუდვისას დაცვის ხარისხი ბევრად მაღალ სტანდარტს. კანონმდებლობაში დეტალურად, მკაფიოდ, საკმარისი დამაჯერებლობითა და სიცხადით უნდა იყოს მოცემული უფლებაში ჩარევის კონკრეტული მიზანი, ამოცანები, საფუძვლები. არაორაზროვანი, ნათელი და განჭვრეტადი უნდა იყოს უფლებაში ჩარევის წესი, სხვა სიტყვებით კანონი უნდა ქმნიდეს ძალიან მკაფიო და თვალნათელ წარმოდგენას, როდის და როგორ შეიძლება აღმოჩნდეს პირთა უფლება შეზღუდვის რისკის ქვეშ.[37] კვლევაში არსებული ინფორმაცია, იძლევა შესაბამისი რეკომენდაციების გაცემის საფუძველს, იმისათვის რომ არსებითადა გაუმჯობესდეს პერსონალური მონაცემების დაცვის ხარისხი საქართველოში.

რეკომენდაციები

- როგორც აღინიშნა, ევროკავშირში ცალკე სამართლებრივი აქტით არის დარეგულირებული მონაცემთა დამუშავების საკითხი პოლიციისა და მართლმსაჯულების ორგანოებისთვის. ძირითადი პრინციპები შესაბამისობაშია მონაცემთა დაცვის ზოგად რეგულაციასთან, თუმცა სამართალდაცვით საქმიანობაში საჭირო გახადა მეტი სიცხადის შემოტანა მონაცემთა დაცვისა და სხვა ლეგიტიმური ინტერესებს შორის ბალანსის დაცვის მიზნით. რის საფუძველზეც ევროკავშირმა მიიღო სპეციალური დირექტივა და ცხადი გახადა სამართალდამცავი ორგანოების მოქმედების არეალი, მონაცემთა დაცვის თვალსაზრისით. მთავარი რეკომენდაცია იქნება, რომ ევროკავშირის წესების მსგავსად, საქართველოს კანონმდებლობაში გაიმიჯნოს პერსონალურ მონაცემთა დაცვის კანონის მოქმედების სფერო და შემუშავდეს სპეციალური სამართლებრივი აქტი ან იმავე კანონში ჩამოყალიბდეს სპეციალური თავი, რომლითაც დარეგულირდება უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების საკითხი.

- ევროპის საბჭოს მარეგულირებელი კანონმდებლობის ანალიზისას აღინიშნა, რომ ციფრული ეპოქის გამოწვევების საპასუხოდ და უფრო ეფექტური აღსრულების მექანიზმის დანერგვის მიზნით, საჭირო გახდა 108 კონვენციის მოდერნიზება. შედეგად მიღებული იქნება კონვენციის შესწორების ოქმი. დოკუმენტი 2018 წელს გაიხსნა ხელმოსაწერად და 32 ხელმომწერი სახელმწიფო ჰყავს, თუმცა საქართველოს ხელმოწერა არ გაუკეთებია. მოდერნიზებული 108+ კონვენციის ხელმოწერით და რატიფიცირებით, საქართველო მნიშვნელოვან ნაბიჯს გადადგამს ევროპის საბჭოს და წევრი ქვეყნების კანონმდებლობის ჰარმონიზაციის თვალსაზრისით.

- საფუძვლიანად იქნება გადასახედი პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, ზემოთ აღნიშნული რეკომენდაციების გათვალიწინების შემთხევაში. კერძოდ, შესაცვლელი იქნება კანონის მოქმედების სფერო. მათ შორის,

---

[37] საქართველოს საკონსტიტუციო სასამართლო, საქმე №1/3/407 (26.12.2007) საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ, II-13.

სამართალდამცავი ორგანოების საქმიანობის გავრცელების კუთხით, როდესაც ისინი არაავტომატიზირებული ფორმით ამუშავებენ სახელმწიფოს საიდუმლოებას მიკუთვნებულ მონაცემებს. გადასახედი იქნება მონაცემთა დაცვის საქმიანობის პრინციპები, მათ შორის გამჭვირვალობის პრინციპის თვალსაზრისით. მონაცემთა სუბიექტის უფლებების უკეთესი დაცვის მექანიზმები იქნება შემოსაღები. უნდა გაიზარდოს მონაცემთა დაცვის საზედამხედველო ორგანოს როლი, უფლებამოსილი ორგანოების საქმიანობაზე, მათ მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის დროს.

- საპოლიციო საქმიანობის მარეგულირებელ კანონმდებლობაში, განსაკუთრებით საპოლიციო ღონისძიების განხორციელების წესებში, პირადი ცხოვრების შეზღუდვისას, დაცვის ხარისხი ბევრად მაღალი უნდა იყოს. შესაბამისად პოლიციის შესახებ საქართველოს კანონში საჭირო იქნება ცვლილებების განხორციელება, სადაც დეტალურად, მკაფიოდ, საკმარისი დამაჯერებლობითა და სიცხადით უნდა იყოს მოცემული უფლებაში ჩარევის კონკრეტული მიზანი, ამოცანები, საფუძვლები. შესაბამისობაში იქნება კანონი მოსაყვანი საპოლიციო დირექტივასთან.

გამოყენებული ლიტერატურა

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

ECtHR, Ben Faiza v. France. (Applications nos. 31446/12) 2018.

ECtHR, Roman Zakharov v. Russia, (Application no. 47143/06). 2015.

ECtHR, S. And Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), 2008.

European Union. (n.d.). *[Document name, if applicable; otherwise use "European Union legal text"]*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT

Guide on Article 8 of the European Convention on Human Rights, CoE, 2020.

Guide on Data protection, Case-law of European Convention on Human Rights CoE, 2021.

Kosta, E., Boehm, F., The EU Law Enforcement Directive (LED): A Commentary. 2024

Parliament of Georgia. (n.d.). *[Title of the bill or document]*. Parliament of Georgia. https://info.parliament.ge/file/1/BillReviewContent/222087

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

„კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი

მიმოცვლის შესახებ. ევროპის პარლამენტისა და ევროპის საბჭოს დირექტივა (EU) 2016/680. 27/04./2016

„პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ“ ევრპარლამენტისა და საბჭოს რეგულაცია (EU) 2016/679. 27/04/2016.

„პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ,“ ევროპის საბჭოს კონვენცია 28/01/1981.

ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია. 04/11/1950.

გოშაძე, კ. პერსონალურ მონაცემთა დაცვის ძირითადი უფლება. იურისტების სამყარო. თბილისი, 2020.

ევროკავშირი ფუნდამენტურ უფლებათა ქარტია. OJ 2012 C 326. 2012.

კორკელია, კ. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებების კრებული. 2019-2023 წლები. პერსონალურ მონაცემთა დაცვა.

მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო. ევროპის საბჭო. 2018 წლის გამოცემა.

საქართველოს კანონი “პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023

საქართველოს კანონი „პოლიციის შესახებ,“ 04/10/2013.

საქართველოს კონსტიტუცია, 24/08/1995.

საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბერის №1/3/407 გადაწყვეტილება, საქმეზე საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ.

საქართველოს საკონსტიტუციო სასამართლოს 2022 წლის 17 ნოემბრის N1/9/1673,1681გადაწყვეტილება საქმეზე ლონდა თოლორაია და სახალხო დამცველი საქართველოს პარლამენტის წინააღმდეგ.