ნორბერტ ბერნსდორფი*

საქართველოში პერსონალურ მონაცემთა დაცვის არსებული მდგომარეობა — 2024 წლის კომუნიკაცია ევროკავშირის გაფართოების პოლიტიკის შესახებ**

სტატიაში განხილულია ევროკომისიის მიერ ცოტა ხნის წინ გამოქვეყნებული სამუშაო დოკუმენტის „ანგარიში საქართველოს შესახებ 2024“ ძირითადი მიგნებები, რომლებიც აფასებს ქვეყნის მიერ 2023 წლის დეკემბრის შემდეგ მიღწეულ პროგრესს, მას შემდეგ, რაც ევროპულმა საბჭომ საქართველოს კანდიდატის სტატუსი მიანიჭა. ნაშრომი მიზნად ისახავს, გააანალიზოს ანგარიშში მოცემული ძირითადი მიგნებები და შეფასებები პერსონალურ მონაცემთა დაცვის სამართლებრივი ჩარჩოს ევროკავშირის სამართალთან დაახლოების კუთხით საქართველოს მიერ მიღწეული პროგრესის შესახებ. ამასთანავე, ნაშრომი გვთავაზობს ევროკომისიის დასკვნების სამართლებრივ ანალიზს საქართველოს მიერ პერსონალურ მონაცემთა დაცვის სფეროში ევროპის საბჭოს სამართლებრივ ინსტრუმენტებთან შესაბამისობასთან დაკავშირებით. დაბოლოს, ცალკე თავი ეთმობა საქართველოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ეფექტიანობისა და მისი საზედამხედველო როლის განხილვას პერსონალური მონაცემების დაცვის უზრუნველყოფის ნაწილში.

საკვანძო სიტყვები: *საქართველოს პერსონალურ მონაცემთა დაცვის კანონმდებლობა, პროგრესის ანგარიში, ევროკავშირის სამართალი (acquis), საქართველოს პერსონალურ მონაცემთა დაცვის სამსახური, სამართლებრივი შესაბამისობა.*

---

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, წინამდებარე ჟურნალის სარედაქციო კოლეგიის წევრი.

** პუბლიკაცია წარმოადგენს საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურთან თანამშრომლობის ფარგლებში წარდგენილ მოხსენებას. ის ეძღვნება საქართველოს ევროკავშირში ინტეგრაციის საკითხებს.

1. ამოსავალი წერტილი: „საქართველოს 2024 წლის ანგარიში“

2024 წლის ოქტომბერში ევროკომისიამ („ევროკავშირის კომისია“) წარმოადგინა თავისი სამუშაო დოკუმენტი - „საქართველოს 2024 წლის ანგარიში“[1]. „საქართველოს 2024 წლის ანგარიში“ თან ახლავს ევროკომისიის „2024 წლის კომუნიკაციას ევროკავშირის გაფართოების პოლიტიკის შესახებ“, რომელიც წარედგინება ევროპის პარლამენტს, ევროკავშირის საბჭოს, ევროპის ეკონომიკურ და სოციალურ კომიტეტსა და რეგიონების კომიტეტს. ანგარიში მოიცავს 2023 წლის 15 ივნისიდან 2024 წლის 1 სექტემბრამდე პერიოდს. მე-7 გვერდზე, ნაწილში „ძირითადი მიგნებები“, ევროკომისია მიიჩნევს, რომ მისი 2023 წლის რეკომენდაციები არ შესრულებულა და კვლავ რჩება ძალაში. 2025 წლისთვის ის საქართველოს აძლევს რეკომენდაციას, რომ „მოახდინოს პერსონალურ მონაცემთა დაცვის სამართლებრივი ჩარჩოს დაახლოება ევროკავშირის სამართალთან (acquis): რეგულაციასა (EU) 2016/679 და დირექტივასთან (EU) 2016/680.“ ანგარიშის 41-ე გვერდზე, სათაურით „თავი 23: მართლმსაჯულება და ფუნდამენტური უფლებები“, ევროკომისია აცხადებს, რომ, „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მიღების მიუხედავად, საქართველოში პერსონალურ მონაცემთა დაცვა სრულად არ არის შესაბამისობაში ევროკავშირის შესაბამის მეორად კანონმდებლობასთან[2] და რომ საქართველოს ჯერ კიდევ არ აქვს ხელი მოწერილი ევროპის საბჭოს 1981 წლის 28 იანვრის კონვენციაზე - პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, მის მოდერნიზებულ ვერსიაზე[3]. ევროკომისია ადასტურებს, რომ პერსონალურ მონაცემთა დაცვის სამსახური (“PDPS”) „ზოგადად დამაკმაყოფილებლად ახორციელებს მონაცემთა დამუშავებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ცენტრალურ ბაზაში განხორციელებული საქმიანობის კანონიერების მონიტორინგს“; თუმცა “PDPS”-მა უფრო აქტიური როლი უნდა შეასრულოს, განსაკუთრებით ფარული საგამოძიებო მოქმედებების მონიტორინგის ნაწილში. ევროკომისია ეყრდნობა 2022 და 2023 წლების სტატისტიკურ მონაცემებს, რომლებიც თავად “PDPS”-ის მიერ იქნა მოწოდებული.

[1] Brussels, 30 October 2024, SWD(2024) 697 final.

[2] ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების და 95/46/EC დირექტივის გაუქმების შესახებ („პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია“), OJ L 119, 2016 წლის 4 მაისი, გვ. 1 და შემდგომი; ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 კომპეტენტური ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის, ანდა სისხლისსამართლებრივი სასჯელის აღსრულების მიზნებისთვის პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების და საბჭოს 2008/977/JHA ჩარჩო გადაწყვეტილების გაუქმების შესახებ, OJ L 119, 2016 წლის 4 მაისი, გვ. 89 და შემდგომი.

[3] Basic document: European Treaty Series – No. 108.

სათაურით „თავი 10: ციფრული ტრანსფორმაცია და მედია“, ევროკომისია თავისი ანგარიშის 73-ე გვერდზე უკმაყოფილებას გამოთქვამს იმასთან დაკავშირებით, რომ ციფრული სერვისების სფეროში საქართველოს ეროვნული კანონმდებლობა მხოლოდ ნაწილობრივ არის დაახლოებული ევროპარლამენტისა და საბჭოს 2019 წლის 20 ივნისის დირექტივასთან (EU) 2019/1024 ღია მონაცემებისა და საჯარო სექტორის ინფორმაციის[4] ხელახლა გამოყენების შესახებ. ის ასევე ანალოგიურ უკმაყოფილებას გამოთქვამს ევროკავშირის სხვა, უფრო ახალ, მეორად კანონმდებლობასთან მიმართებით[5]. „ანგარიში საქართველოს შესახებ 2024-ის“ მომზადებისას ევროკომისია იყენებს „ახალ მეთოდს“, რომელიც 2020 წლის თებერვალში გაწევრიანების შესახებ მოლაპარაკებების წარმართვისთვის შემუშავდა. ეს მეთოდი მოლაპარაკებების ცალკეული თავების თემატურ კლასტერებად დაჯგუფებას გულისხმობს. ამ კონტექსტში მოლაპარაკებების 23-ე თავის — „მართლმსაჯულება და ფუნდამენტური უფლებები“ მოთხოვნებთან შესაბამისობა განსაკუთრებით მკაცრად კონტროლდება.

2. ზოგადი და დაუსაბუთებელი სამართლებრივი კრიტიკის დილემა

„საქართველოს 2024 წლის ანგარიში“-ს დოკუმენტში ევროკომისია რეგულარულად ვერ წარმოადგენს კონკრეტულ მტკიცებულებებს თავისი დასკვნების გასამყარებლად, მათ შორის, საქართველოში პერსონალურ მონაცემთა დაცვის „არსებული მდგომარეობის“ შეფასებისას. ამის ნაცვლად, ის მე-4 გვერდზე, მე-2 სქოლიოში, იძლევა შემდეგ ზოგად მითითებას:

„ის (ეს ანგარიში) ეფუძნება სხვადასხვა წყაროდან მიღებულ ინფორმაციას, მათ შორის, საქართველოს, ევროკავშირის წევრი სახელმწიფოების, ევროპარლამენტის ანგარიშებიდან და სხვადასხვა საერთაშორისო და არასამთავრობო ორგანიზაციიდან მიღებულ მონაცემებს. ის ასევე მოიცავს სხვა დაინტერესებული მხარეების მიერ შემუშავებული შედარებითი შეფასებებისა და ინდექსების შედეგებს, განსაკუთრებით კანონის უზენაესობის სფეროში.“

რა თქმა უნდა, არსებობს ტექნიკური შეზღუდვები იმ ანგარიშისთვის კონკრეტული მტკიცებულებების წარმოდგენისას, რომლებიც 30-ზე მეტ მოლაპარაკების თავსა და ექვს კლასტერში რეფორმების მიმდინარე მდგომარეობას ეხება. მიუხედავად ამისა, ზოგადი და დაუსაბუთებელი სამართლებრივი კრიტიკა, კონკრეტული მაგალითებისა და მტკიცებულებების

[4] OJ L 172, 26 June 2019, pp. 56 et seq.

[5] General Data Protection Regulation, OJ L 119, 4 May 2016, 1 et seq.; Regulation (EU) of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ("Digital Services Act"), OJ L 277, 27 October 2022, pp. 1 et seq.; Regulation (EU) of the European Parliament and of the Council of September 14, 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 ("Digital Markets Act"), OJ L 265, 12 October 2022, pp. 1 et seq.

გარეშე, რთულად გასაგებია და გაკრიტიკებულ ინსტიტუტებს გაუმჯობესების შესაძლებლობას არ უტოვებს.

ობიექტური სამართლებრივი კრიტიკის ერთ-ერთი ძირითადი მოთხოვნაა, ნათლად ჩამოაყალიბოს ის წინაპირობები, რომლებსაც კრიტიკა ემყარება. ის უნდა იყოს შემოწმებადი, დასაბუთებული და მოიცავდეს როგორც დადებით, ისე უარყოფით ასპექტებს. სამართლებრივი კრიტიკის ძირითადი ფუნქციაა ხარვეზების, შეცდომებისა და წინააღმდეგობების მეთოდური იდენტიფიცირება პრაქტიკული პროცედურებისა და პირობების გაუმჯობესების მიზნით. კანონის ზოგადი და დაუსაბუთებელი კრიტიკა რამდენიმე პრობლემას ქმნის. უპირველეს ყოვლისა, მან შეიძლება გამოიწვიოს თანამშრომლობის შემცირება, რადგან ის არ არის კონსტრუქციული და არ გვთავაზობს გაუმჯობესების გზებს. მას ასევე შეუძლია შეარყიოს ნდობა გამკრიტიკებელი ინსტიტუტის — ამ შემთხვევაში ევროკომისიის - მიმართ და შექმნას ნეგატიური ატმოსფერო. ზოგადმა კრიტიკამ, მათი გადაჭრის ნაცვლად, შეიძლება „დაფაროს“ რეალური პრობლემები. კანონის კონსტრუქციული კრიტიკა შეიძლება ამოვიცნოთ შემდეგი მახასიათებლებით: მას მოჰყავს კონკრეტული მტკიცებულებები გაკრიტიკებული ქმედებისათვის და გვთავაზობს ცვლილებების კონსტრუქციულ გზებს. ის მიზნად ისახავს ვითარების გაუმჯობესებას. ფორმალური თვალსაზრისით, ის პატივისცემითა და დაფასებით უნდა იყოს გამოხატული.

სამწუხაროდ, „საქართველოს 2024 წლის ანგარიში“ 41-ე და 73-ე გვერდებზე ვერ აკმაყოფილებს საქართველოს პერსონალურ მონაცემთა დაცვის კანონმდებლობისა და მისი აღმსრულებელი ინსტიტუტის “PDPS”-ის მიმართ ასეთი პოზიტიური მიდგომის კრიტერიუმებს - მათ შორის ატმოსფეროს თვალსაზრისითაც – შემდეგი მიზეზების გამო:

3. ევროპის საბჭოს მოდერნიზებული 108-ე კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“

108-ე კონვენციის თავდაპირველი ვერსია ხელმოსაწერად 1981 წლის 28 იანვარს გაიხსნა და ის იყო პირველი იურიდიულად სავალდებულო საერთაშორისო ხელშეკრულება, რომელმაც მონაცემთა დაცვის პრინციპები დაადგინა. 2001 წელს მას დამატებითი ოქმი დაემატა. უკვე გარკვეული ხანია, 108-ე კონვენციის მოდერნიზებული ვერსია რატიფიკაციისთვის ხელმისაწვდომია. ეს „108+ კონვენცია“ ძალაში შევა, როდესაც ევროპის საბჭოს 38 წევრი სახელმწიფო მოახდენს მის რატიფიცირებას.

გასაგებია, რომ ევროკომისია თავის ანგარიშში მოუწოდებს საქართველოს, ხელი მოაწეროს (და შემდგომში მოახდინოს რატიფიცირება) ევროპის საბჭოს 1981 წლის 28 იანვრის კონვენციას „პერსონალური

მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“, მის მოდერნიზებულ ვერსიას. საქართველოს მიერ 108+ კონვენციის რატიფიცირებით, მისი ძალაში შესვლა საბოლოოდ ერთი ნაბიჯით კიდევ უფრო დაახლოებაა.

თუმცა ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) – თავისი გადაწყვეტილებებით – დიდი ხანია, რაც იკისრა ცენტრალური გადაწყვეტილების მიმღები ორგანოს როლი ევროპის საბჭოს წევრი სახელმწიფოებისთვის მონაცემთა დაცვის საკითხებზე. ის დამხმარე საშუალებად იყენებს 108-ე კონვენციას თავისი განმარტებებით. მიუხედავად ამისა, 1987 წლიდან პერსონალურ მონაცემთა დაცვის უფლება დამოუკიდებლად და გადამწყვეტად მომდინარეობს ადამიანის უფლებებიდან, რომლებიც გათვალისწინებულია ადამიანის უფლებათა ევროპული კონვენციით (“ECHR”), კერძოდ, კონვენციის მე-8 მუხლიდან („პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და კორესპონდენციის დაცვის უფლება“), რადგან “ECtHR” გადაწყვეტილებას იღებს არა უშუალოდ 108-ე კონვენციის, არამედ “ECHR”-ით გათვალისწინებული ადამიანის უფლებების საფუძველზე. 108-ე კონვენციის სამართლებრივი მნიშვნელობა „უკანა მხარეს გადადის“. ამასთანავე, ეს საერთაშორისო ხელშეკრულება კვლავაც მხოლოდ ზოგად პრინციპებს ადგენს პერსონალურ მონაცემთა დაცვისთვის, როგორებიცაა დამუშავების სამართლებრივი საფუძვლის ქონის საჭიროება, დამუშავების გამჭვირვალობა, ინფორმაციისა და შესწორების უფლება და კონტროლის მექანიზმების შექმნა.

1987 წლის საქმეზე „ლეანდერი შვედეთის წინააღმდეგ“[6] მიღებული გადაწყვეტილების შემდეგ, რომელშიც “ECtHR”-მა პირველად გააანალიზა საჯარო ორგანოს მიერ ფიზიკური პირის პერსონალური მონაცემების შენახვის საკითხი, ამ სფეროში სასამართლო პრაქტიკა მნიშვნელოვნად განვითარდა. წლების განმავლობაში სასამართლომ განიხილა მრავალი სიტუაცია, რომლებშიც ამ საკითხთის მიმართ კითხვები დაისვა. ფართო სპექტრი პერსონალურ მონაცემებთან დაკავშირებული ოპერაციებისა, როგორებიცაა ასეთი მონაცემების შეგროვება, შენახვა, გამოყენება და გავრცელება, ახლა უკვე “ECtHR”-ის პრეცედენტული სამართლის კორპუსით რეგულირდება. ეს სასამართლო პრაქტიკა საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სწრაფი ევოლუციის პარალელურად განვითარდა.

პერსონალურ მონაცემთა დაცვის უფლება არ არის ავტონომიური უფლება “ECHR”-ით გათვალისწინებულ სხვადასხვა უფლებასა და თავისუფლებას შორის. მიუხედავად ამისა, სასამართლომ აღიარა, რომ პერსონალურ მონაცემთა დაცვას ფუნდამენტური მნიშვნელობა აქვს პირის მიერ “ECHR”-ის მე-8 მუხლით გარანტირებული პირადი და ოჯახური ცხოვრების, საცხოვრისისა და მიმოწერის პატივისცემის უფლებით სარგებლობისთვის[7]. ეს მუხლი არის

[6] ECtHR, Case of *Leander v. Sweden*, Application no. 9248/81, hudoc.

[7] ECtHR, Case of *Z v. Finland*, Application no. 22009/93, hudoc; Case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, hudoc; Case of *L.B. v. Hungary*, Application no. 36345/16, hudoc.

მთავარი ვექტორი, რომლის მეშვეობითაც ხდება პერსონალური მონაცემების დაცვა "ECHR"-ის სისტემაში, თუმცა ამ დაცვასთან დაკავშირებული მოსაზრებები შეიძლება ECHR-ისა და მისი ოქმების სხვა დებულებების ფარგლებშიც იქნას გათვალისწინებული.

შედეგად, საქართველოს უკვე არ შეუძლია თავი აარიდოს ევროპის საბჭოს მიერ მონაცემთა დაცვის სფეროში დადგენილ სამართლებრივ სტანდარტებს. მიუხედავად იმისა, მოაწერს თუ არა ხელს (და შემდგომში მოახდენს თუ არა რატიფიცირებას) 108+ კონვენციას, საქართველო უკვე ვალდებულია, იხელმძღვანელოს "ECtHR"-ის მიერ მონაცემთა დაცვის სფეროში დადგენილი პრეცედენტული სამართლით, რაც ნიშნავს, რომ 108+ კონვენციის „მიღებას" მაქსიმუმ დამატებითი ხასიათი ექნება.

4. პერსონალურ მონაცემთა დაცვის ძირითად რეგულაციასთან, ციფრული სერვისების აქტთან და ციფრული ბაზრების აქტთან დაახლოება

„საქართველოს 2024 წლის ანგარიში"-ის 73-ე გვერდზე ევროკომისია არ განმარტავს, თუ რატომ მიიჩნევს, რომ ხსენებული სამი სამართლებრივი აქტი - რომლებიც ევროკავშირის რეგულაციებს წარმოადგენს („რეგულაცია", „აქტები") - გაწევრიანებამდე საქართველოსგან მოითხოვდა პერსონალურ მონაცემთა დაცვის კანონმდებლობის დაახლოებას. სამართლებრივი თვალსაზრისით, ევროკავშირის დირექტივები წევრი სახელმწიფოებისთვის მხოლოდ მისაღწევი შედეგის დადგენით შემოიფარგლება. ამ შედეგის მიღწევის გზებს თავად წევრი სახელმწიფოები განსაზღვრავენ; მათ დირექტივების იმპლემენტაცია გარკვეულ ვადებში, საკუთარი ეროვნული კანონმდებლობის მეშვეობით უნდა უზრუნველყონ. ამის საპირისპიროდ, ევროკავშირის რეგულაციები პირდაპირ და დაუყოვნებლივ სავალდებულოა ყველა წევრი სახელმწიფოსთვის და არა მხოლოდ მისაღწევ შედეგთან მიმართებით, როგორც ეს დირექტივის შემთხვევაშია. როგორც წესი, ევროკავშირის რეგულაციები არ საჭიროებს ეროვნულ კანონმდებლობაში გადმოტანას (ტრანსპოზიციას).

ევროკავშირში გაწევრიანებისას ევროკავშირის კანონმდებლობის მიღება - ცნობილი როგორც „მიღება" ან „გადასვლა" - ავტომატური პროცესია[8]. ამის ტექნიკური ინსტრუმენტი კანდიდატი ქვეყნის „გაწევრიანებაა". ეს ხორციელდება ევროკავშირის ყველა სხვა წევრ სახელმწიფოსთან (საერთაშორისო) გაწევრიანების შეთანხმების მეშვეობით. გაწევრიანების დღიდან კანდიდატი ქვეყანა ხდება ევროკავშირის ყველა ხელშეკრულების მხარე, მათი მოქმედი რედაქციით. ამ ხელშეკრულებების საფუძველზე გაწევრიანების თარიღამდე მიღებული ევროკავშირის მთელი კანონმდებლობა ავტომატურად ხდება სავალდებულო გაწევრიანებული სახელმწიფოსთვის.

[8]იხ.: *Bernsdorff N.,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, 13 et seq.

მას უპირატესი იურიდიული ძალა აქვს ნებისმიერ ეროვნულ კანონთან შედარებით. ევროკავშირის მონაცემთა დაცვის კანონმდებლობისთვის ეს ნიშნავს, რომ გაწევრიანებისთანავე ისიც ავტომატურად ხდება ეროვნული სამართლებრივი სისტემის ნაწილი, როგორც პირველადი სამართალი. ის „ინერგება“ ეროვნულ სამართლებრივ წესრიგში.

ამ ფონზე ევროკომისიამ ვერ განმარტა, თუ რატომ მოეთხოვება კანდიდატ ქვეყანას, საქართველოს, ევროკავშირის არსებული წევრი სახელმწიფოებისგან განსხვავებით, გაწევრიანებამდე „ჩაანაცვლოს“ ზემოხსენებული ევროკავშირის რეგულაციების შინაარსი თავის ეროვნულ მონაცემთა დაცვის კანონმდებლობაში, ანუ, „წინასწარ გაითვალისწინოს“ ევროკავშირის რეგულაციები გაწევრიანებამდეც კი. თუ ევროკავშირის რეგულაციები ასევე მოითხოვს ეროვნულ კანონმდებლობაში მინიმალური დონის „ხელსაყრელი გარემოს“ შექმნას, სასურველი იქნებოდა ამ „ხელსაყრელი გარემოს“ შესახებ შესაბამისი განმარტებებისა და მისი მონახაზის წარმოდგენა.

თუმცა, რომც არსებობდეს ციფრული სერვისების აქტის საქართველოს ეროვნულ მონაცემთა დაცვის კანონმდებლობაში „ჩანაცვლების“, ან სულ მცირე, უფრო მეტად ასახვის საჭიროება, 2024 წლის ივნისში “TAIEX”-ის სამუშაო შეხვედრის შედეგების ცოდნის გარეშე გაუგებარი იქნებოდა, თუ სად და რა კუთხით უნდა განხორციელებულიყო შემდგომი დაახლოება 2024 წლის სექტემბრამდე:

ევროკავშირის ციფრული სერვისების აქტი ქმნის ონლაინ სერვისებისთვის წესების ერთიან ჩარჩოს უსაფრთხო ციფრული გარემოს ხელშეწყობისა და მომხმარებელთა დაცვის მიზნით[9]. ძირითადი ასპექტები მოიცავს უფრო მკაცრ ვალდებულებებს ონლაინ პლატფორმებისთვის, როგორებიცაა სოციალური ქსელები და სავაჭრო პლატფორმები, კონტენტის მოდერაციისა და მომხმარებელთა საჩივრების განხილვის კუთხით. ციფრული სერვისების აქტი ითხოვს მეტ გამჭვირვალობას მოდერაციის პროცესებსა და რეკლამასთან დაკავშირებით, შეიცავს ზომებს სიძულვილის ენისა და დეზინფორმაციის წინააღმდეგ და აძლიერებს არასრულწლოვანთა დაცვას. ძალიან დიდ პლატფორმებზე უფრო მკაცრი წესები ვრცელდება.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ვრცელი დებულებების გათვალისწინებითა და მისი მოქმედების სფეროსთან (მე-2 მუხლი) დაკავშირებით, გაუგებარია, რატომ არ ავალდებულებს კანონი ონლაინ შუამავლებს, როგორებიცაა ონლაინ პლატფორმები, სოციალური ქსელები, სავაჭრო პლატფორმები და აპლიკაციების მაღაზიები, აიღონ პასუხისმგებლობა უკანონო კონტენტზე. ასევე, საჭიროებს განმარტებას, თუ რატომ არ არის კანონის III თავში („მონაცემთა სუბიექტის უფლებები“) მოცემული საჩივრის მექანიზმები საკმარისი პლატფორმის ოპერატორების მიერ მიღებული გადაწყვეტილებების წინააღმდეგ სამართლებრივი ზომების

[9] *დამატებით იხ.: Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, 7 et seq.

მისაღებად. დაბოლოს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი შეიცავს მრავალ დებულებას მონაცემთა დამუშავებაზე პასუხისმგებელ პირებისა და დამუშავებაზე უფლებამოსილი პირების ვალდებულებების შესახებ (23-ე მუხლი და შემდგომი). “PDPS”-ის მეშვეობით ეროვნული საზედამხედველო ორგანო ახორციელებს მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის მონიტორინგს, მათ შორის, ციფრული სერვისის პროვაიდერების მიერ (49-ე მუხლი და შემდგომი).

ციფრული ბაზრების აქტი არის ევროკავშირის რეგულაცია, რომელიც მიზნად ისახავს ციფრულ ბაზრებზე კონკურენციის ხელშეწყობას დომინანტური საბაზრო პოზიციის მქონე დიდი ონლაინ პლატფორმების, ე.წ. „გეითკიპერების“ (“gatekeepers”), რეგულირებით. მისი მიზანია სამართლიანი პირობების შექმნა და ბაზარზე არსებული ძალაუფლების ბოროტად გამოყენების თავიდან აცილება. ციფრული ბაზრების აქტი კრძალავს ე.წ. „გეითკიპერების“ გარკვეულ ქმედებებს, როგორებიცაა საკუთარი სერვისებისთვის უპირატესობის მინიჭება ან მონაცემთა გადაცემის შეფერხება, და ამის ნაცვლად მოითხოვს მეტ თავსებადობასა და სამართლიან პირობებს.

არც აშკარაა და არც ევროკომისია განმარტავს, სამართლიანი კონკურენციის ინტერესებიდან გამომდინარე, თუ რატომ არ შეიძლება ციფრული ბაზრების აქტით ე.წ. „გეითკიპერებისთვის“ დაწესებული „ნებადართული“ და „აკრძალული“ ქმედებები აღსრულდეს საქართველოს მონაცემთა დაცვის კანონმდებლობის ჩვეულებრივი ინსტრუმენტებით (მე-13 მუხლი და შემდგომი, მე-18 მუხლი, 64-ე მუხლი, X თავი). მომხმარებლებისთვის მესამე მხარის ციფრული სერვისებით სარგებლობის შეზღუდვა ასევე შეიძლება აიკრძალოს საქართველოს მონაცემთა დაცვის კანონმდებლობით და ე.წ. „გეითკიპერებს“ კონფლიქტის შემთხვევაში შეიძლება მოეთხოვოთ გარკვეული კომპიუტერული აპლიკაციების ან პროგრამული უზრუნველყოფის დეინსტალაცია.

რაც შეეხება „ევროკავშირის პერსონალურ მონაცემთა დაცვის ძირითად რეგულაციას“, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დებულებები უკვე ძალიან ახლოსაა მის მოთხოვნებთან[10]. კანონი ითვალისწინებს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაციის ბევრ პრინციპს, მათ შორის: მონაცემთა სუბიექტის უფლებებს, გამჭვირვალობას, უსაფრთხოების ვალდებულებებსა და მონაცემთა დარღვევის შესახებ შეტყობინებებს.

[10] იხ.: *Bernsdorff N.,* the New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, 101 et seq.

5. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ეფექტიანი ზედამხედველობის განხორციელება

მონაცემთა დაცვის საზედამხედველო ორგანოებს, როგორც წესი, უწევთ პასუხის გაცემა მონაცემთა დაცვის ყველა სფეროდან, ყველა ინდუსტრიის მასშტაბით დასმულ შეკითხვებზე, აგრეთვე, ე.წ. „ჯვარედინი შემოწმებების“ ფარგლებში. იქ, სადაც მათ შეუძლიათ ნდობა გამოუცხადონ პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს, ნაკლები ზედამხედველობაა საჭირო, ხოლო სხვა სფეროებში რეგულარულად უნდა განხორციელდეს მიზნობრივი შემოწმებები. ამ სფეროში ყოველთვის არსებობს კონსულტაციისა და ცნობიერების ამაღლების დიდი საჭიროება. მონაცემთა დაცვასთან შესაბამისობის შემოწმებისას ყველა საკითხი ყოველთვის თანაბრად რელევანტური არ არის. არ არსებობს მონაცემთა დაცვის „მზა“ გადაწყვეტილებები; მონაცემთა დაცვის საზედამხედველო ორგანოების მიერ გამოყენებული ზომები უნდა შეესაბამებოდეს იდენტიფიცირებულ კონკრეტულ რისკს მონაცემთა დაცვის სფეროში. ასეთი ზომების მიღებამდე ასევე უნდა განხორციელდეს გავლენის შეფასება. ამ ფონზე თითქმის შეუძლებელია შეფასდეს მონაცემთა დაცვის საზედამხედველო ორგანოები – და, შესაბამისად, საქართველოს “PDPS” – აქტიურად მართავენ თუ არა მონაცემებს და ახორციელებენ თუ არა მონაცემთა დაცვის ეფექტიან კონცეფციას.

ნამდვილად არ არის დამაჯერებელი, რომ აქტივობის გასაზომად (და მომავალი პროგნოზების საფუძვლად) რამდენიმე წლის (2022, 2023) განმავლობაში „საქმეთა რაოდენობის“ არათანაბარი მაჩვენებლების გამოყენება, როგორც ეს ევროკომისიამ გააკეთა „საქართველოს შესახებ 2024 წლის ანგარიშის“ 41-ე გვერდზე დართულ გრაფიკზე. ეს გრაფიკი ყველა მიმართულებით ხაზოვან ზრდას აჩვენებს. “PDPS”-ის 2025 წლის პირველი ექვსი თვის[11] საქმიანობის შესახებ „სპეციალური ანგარიშის“ გათვალისწინებით, ევროკომისიის მოსაზრება, რომ “PDPS”-მა ამ მიმართულებით „უფრო აქტიური როლი“ უნდა შეასრულოს, არ ჩანს დასაბუთებული. 2025 წლის პირველ ნახევარში ინსპექტირებების/შემოწმებების რაოდენობა 155 იყო. მისივე სტატისტიკის მიხედვით, “PDPS”-მა 496 განცხადება/შეტყობინება მიიღო. სამსახურმა 278 ადმინისტრაციული სამართალდარღვევა გამოავლინა და 277 შემთხვევაში ადმინისტრაციული სახდელი გამოიყენა. გაიცა 369 დავალება და რეკომენდაცია. ასევე აღსანიშნავია “PDPS”-ის საერთაშორისო საქმიანობა,

[11] საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის 2025 წლის 6 თვის სტატისტიკა /იანვარი-ივნისი.

რომლის შესახებაც მან სხვა „სპეციალურ ანგარიშში“[12] ისაუბრა. “PDPS”-ის 2025 წლის პირველი ექვსი თვის საქმიანობის შესახებ „სპეციალურ ანგარიშში“ აღწერილი ფარული საგამოძიებო მოქმედებების[13] მონიტორინგის სფეროში განხორციელებული მრავალრიცხოვანი შემოწმებების გათვალისწინებით, რომელთა განხორციელებაც “PDPS”-ს ევალება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის VII თავის შესაბამისად, გაუგებარია, თუ რატომ არსებობს, ევროკომისიის აზრით, ამ სფეროში კვლავ გაძლიერებული მოქმედების საჭიროება.

ბიბლიოგრაფია:

1. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 სისხლისსამართლებრივი დანაშაულის პრევენციის, გამოძიების, გამოვლენის ან სისხლისსამართლებრივი დევნის, ან სისხლისსამართლებრივი სასჯელის აღსრულების მიზნებისთვის კომპეტენტური ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, ასეთი მონაცემების თავისუფალი გადაადგილებისა და საბჭოს 2008/977/JHA ჩარჩო-გადაწყვეტილების გაუქმების თაობაზე.
2. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი გადაადგილების შესახებ და 95/46/EC დირექტივის გაუქმების თაობაზე („პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია“).
3. ევროპის საბჭო, კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ (108-ე კონვენცია), ევროპულ ხელშეკრულებათა სერია №108 (1981).
4. სამსახურის მიერ 2022-2024 წლებში განხორციელებული საერთაშორისო აქტივობები პერსონალურ მონაცემთა დაცვის კანონმდებლობის საუკეთესო ევროპული პრაქტიკისა და სტანდარტების იმპლემენტაციის მიზნით.
5. საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის 2025 წლის 6 თვის (იანვარი-ივნისი) საქმიანობის სტატისტიკა, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახური.
6. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and

[12] სამსახურის მიერ 2022-2024 წლებში განხორციელებული საერთაშორისო აქტივობები პერსონალურ მონაცემთა დაცვის კანონმდებლობის საუკეთესო ევროპული პრაქტიკისა და სტანდარტების იმპლემენტაციის მიზნით.
[13] იქვე, 8-11.

amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
8. *Bernsdorff N.,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, 13 et seq.
9. *Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, 7 et seq.
10. *Bernsdorff N.,* the New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, 101 et seq.
11. Case of *L.B. v. Hungary*, Application no. 36345/16, hudoc.
12. Case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, hudoc.
13. ECtHR, Case of *Leander v. Sweden*, Application no. 9248/81, hudoc.
14. ECtHR, Case of *Z v. Finland*, Application no. 22009/93, hudoc.
15. European Commission**,** Staff Working Document SWD (2024) *697 final* (Brussels, 30 October 2024).
16. OJ L 119, 4 May 2016, 1 et seq.
17. OJ L 172, 26 June 2019, 56 et seq.