ბექა მელაძე*

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება - გამოწვევები და შესაძლებლობები

ჩვენ ვცხოვრობთ რეალობაში, სადაც თითოეული გადაწყვეტილება ეფუძნება გარშემო არსებული ინფორმაციის ნაკადს. მონაცემთა სწორი და სწრაფი ანალიზი აძლიერებს ინდუსტრიებს, გარდაქმნის საზოგადოებას და აჩქარებს პროგრესს. ამ ტრანსფორმაციაში განსაკუთრებული როლი უკავია ღრუბლოვან სისტემებს ("Cloud Systems"). აღნიშნული ტექნოლოგია უამრავ შესაძლებლობას ქმნის და სახელმწიფოს, ბიზნეს სექტორსა თუ ფიზიკურ პირს ყოველდღიურ საქმიანობას უმარტივებს. მიუხედავად ამისა, არსებობს მრავალი გამოწვევაც, რომელიც დაკავშირებულია პერსონალური მონაცემების კანონიერ და ეთიკურ დამუშავებასთან.

საკვანძო სიტყვები: *პერსონალური მონაცემები, ღრუბლოვანი სისტემები, დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირი, მონაცემთა საერთაშორისო გადაცემა, მონაცემთა უსაფრთხოება.*

1. შესავალი

ღრუბლოვანი სისტემები ბოლო ათწლეულის ერთ-ერთი ყველაზე მზარდი ტექნოლოგიაა, რომელიც ტრადიციულ, ფიზიკურ ინფრასტრუქტურასთან დაკავშირებული შეზღუდვების საპირწონედ, ხელს უწყობს მონაცემთა სწრაფ და ეფექტიან დამუშავებას. აღნიშნული მოდელი გვთავაზობს მოქნილ მიდგომას, რაც დღევანდელ ციფრულ სამყაროში არსებული მზარდი მოცულობის მონაცემთა სამართავად აუცილებელია. მხოლოდ 2024 წელს ექვსას მილიარდზე მეტი[1] დაიხარჯა ღრუბლოვანი

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი, პერსონალურ მონაცემთა დაცვის სამსახურის კერძო სექტორზე ზედამხედველობის დეპარტამენტის იურისტი.

[1] Public cloud services end-user spending worldwide from 2017 to 2024,

სისტემების მომსახურებაზე და პროგნოზების თანახმად, ის 2027 წლისთვის დაახლოებით 1 ტრილიონ დოლარს მიაღწევს. ზრდა გამოწვეულია სხვადასხვა ინდუსტრიაში ღრუბლოვანი სერვისების დანერგვით, რადგან კომპანიები უპირატესობას ანიჭებენ ღრუბლოვანი სისტემების ხარჯთ-ეფექტიანობას[2].

მოქნილობისა და სისწრაფის პარალელურად, წარმოიშობა არაერთი გამოწვევა, რომელიც დაკავშირებულია მესამე პირის სერვერების მეშვეობით პერსონალური მონაცემების დამუშავებასთან, მათ შორის, სუბიექტების სტატუსის და უსაფრთხოების ნაწილში მათი ფუნქციების განსაზღვრა. ამასთან, განსაკუთრებულ სირთულეს წარმოადგენს მონაცემთა დამუშავების ადგილმდებარეობის დადგენა, რაც შესაძლოა დაკავშირებული იყო სხვადასხვა ვალდებულებასთან.

წინამდებარე ნაშრომი შეისწავლის პერსონალური მონაცემების დამუშავების პროცესში ღრუბლოვანი სისტემების გამოყენებას, განიხილავს მათ შესაძლებლობებსა და გამოწვევებს, რომლებიც დაკავშირებულია კონფიდენციალობასა და უსაფრთხოებასთან.

2. ღრუბლოვანი სისტემების არსი

ღრუბლოვანი სისტემები ნებისმიერ პირს აძლევს საშუალებას ინტერნეტის გამოყენებით ისარგებლოს შესაბამისი მომსახურების მიმწოდებელი კომპანიის ინფრასტრუქტურით, კერძოდ, შეინახოს ან სხვაგვარად დაამუშაოს საკუთარი მონაცემები მსოფლიოს ნებისმიერი წერტილიდან.

მარტივად რომ ითქვას, ღრუბლოვანი სისტემები მომხმარებელს აძლევს საშუალებას მონაცემები, ფაილები, ფოტო/ვიდეო მასალა თუ სხვადასხვა აპლიკაციები ინტერნეტის გამოყენებით, განათავსონ რომელიმე კომპანიის სერვერებზე, ნებისმიერ დროს მასზე წვდომისა და რედაქტირების შესაძლებლობით, სასურველი მოწყობილობის გამოყენებით. დღესდღეობით მსოფლიოს მასშტაბით არაერთ კომპანიას აქვს შექმნილი ღრუბლოვანი სისტემები, რომლებიც სხვადასხვა მიზნით გამოიყენება. აღნიშნულ სფეროში წამყვანი პოზიციები აქვთ ღრუბლოვანი სისტემების პროვაიდერებს: “Amazon Web Services”, “Microsoft Azure” და “Google Cloud Platform (GCP)”.

აშშ-ს სტანდარტებისა და ტექნოლოგების ნაციონალური ინსტიტუტის (“NIST”) განმარტებით ღრუბლოვან სისტემებს გააჩნია 5 თვისება[3]:

<https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].

[2] NexQloud ღრუბლოვანი ტექნოლოგიების ბაზარზე რევოლუციას დეცენტრალიზებული პლატფორმით მოახდენს, 2024, <https://forbes.ge/nexqloud-set-to-disrupt-cloud-computing-with-decentralized-platform/> [21.02.2025].

[3] National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012, 800-146.

1. მყისიერი წვდომა - მომხმარებელს შეუძლია სასურველ დროს ისარგებლოს მომსახურებით (მაგალითად, გახსნას და მიიღოს წვდომა საკუთარ ბაზაზე) ინფრასტრუქტურის მესაკუთრე კომპანიის თანხმობის ან/და დახმარების გარეშე;
2. ფართო ქსელზე წვდომა ("Broad Network Access") - მომხმარებელს შეუძლია საკუთარ მონაცემებზე წვდომა (რედაქტირება, წაშლა, დამატება და სხვა) პარალელურად, რამდენიმე მოწყობილობის მეშვეობით;
3. სისტემის პროვაიდერი საკუთარ ინფრასტრუქტურულ რესურსებს მრავალ მომხმარებელს შორის ანაწილებს მათივე მოთხოვნის შესაბამისად;
4. მოქნილობა - მომხმარებელს აქვს შესაძლებლობა საჭიროების შესაბამისად გაზარდოს ან შეამციროს რესურსები, მაგალითად, "Google Drive"-ზე შეიძინოს სტანდარტული მოცულობისგან განსხვავებული რესურსის რაოდენობა;
5. პერსონალიზებული საფასური - მომსახურების საფასური განისაზღვრება გამოყენებული რესურსის შესაბამისად.

აქვე, უნდა აღინიშნოს, რომ ღრუბლოვანი სისტემები საკმაოდ მრავალფეროვანია და მოიცავს რამდენიმე განსხვავებულ სერვისს, კერძოდ:

- პროგრამული უზრუნველყოფა, როგორც მომსახურება ("Software as a Service") - ონლაინ რეჟიმში მომუშავე ელექტრონული ფოსტის და დოკუმენტების შენახვის სისტემა ("Google Drive", "Dropbox", "Gmail", "Outlook 365" და სხვა);
- პლატფორმა, როგორც მომსახურება ("Platform as a Service") - გამოიყენება დეველოპერების მიერ ღრუბლოვან სისტემაში აპლიკაციების შესაქმნელად, ("Google App Engine");
- ინფრასტრუქტურა, როგორც მომსახურება ("Infrastructure as a Service") - ძირითად შემთხვევაში გამოიყენება იურიდიული პირების მიერ, რომლებიც საკუთარი სერვერის შექმნის ნაცვლად იყენებენ ღრუბლოვანი სისტემების პროვაიდერი კომპანიის ინფრასტრუქტურას.

აქვე, უნდა აღინიშნოს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ"[4] საქართველოს კანონის მე-2 მუხლის პირველი პუნქტის თანახმად, კანონის მოქმედება ვრცელდება საქართველოს ტერიტორიაზე მონაცემთა ავტომატური საშუალებებით დამუშავებასა და ნახევრად ავტომატური საშუალებებით დამუშავებაზე. შესაბამისად, თუკი პირი პერსონალურ მონაცემებს ამუშავებს საქართველოს ტერიტორიაზე, მათ შორის, აქვს მხოლოდ წვდომა ღრუბლოვან სისტემაზე, აღნიშნულზე ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მოქმედება, მიუხედავად იმისა, თუ სად არის განთავსებული ან რომელ იურისდიქციაში ექცევა ღრუბლოვანი სისტემა ან/და მისი პროვაიდერი

[4] „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023.

კომპანია[5] (ღრუბლოვანი სისტემის ადგილმდებარეობის და შესაბამისი იურისდიქციის საკითხთან დაკავშირებული იხილეთ წინამდებარე სტატიის 4.2. თავი).

მიუხედავად ღრუბლოვანი სისტემების გამოყენების მრავალფეროვნებისა, პერსონალური მონაცემების დამუშავების მხრივ, განსაკუთრებით საინტერესოა პროგრამული უზრუნველყოფა, როგორც სერვისი, რადგან იგი ყველაზე ხშირად გამოიყენება დამუშავებისთვის პასუხისმგებელი პირების მიერ პერსონალური მონაცემების შენახვის, გაზიარების და სხვაგვარი დამუშავებისთვის.

3. სუბიექტების სამართლებრივი სტატუსი

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება მეტად კომპლექსური თემაა, სადაც რამდენიმე მხარეა ჩართული. ხშირ შემთხვევაში, რესურსების დისბალანსისა და დომინანტური მდგომარეობიდან გამომდინარე, რთულია განისაზღვროს, რომელი მხარე წარმოადგენს დამუშავებისთვის პასუხისმგებელ პირს და რომელი დამუშავებაზე უფლებამოსილ პირს. ამ კუთხით, მნიშვნელოვანია შეფასდეს, ერთი მხრივ, ღრუბლოვანი სისტემის პროვაიდერი კომპანიის, ხოლო მეორე მხრივ, მისი პროდუქტის მომხმარებლის როლი და ფუნქცია.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „ო“ ქვეპუნქტის თანახმად, „დამუშავებისთვის პასუხისმგებელი პირი არის ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას“, ამავე მუხლის „ჟ“ ქვეპუნქტის თანახმად კი „დამუშავებაზე უფლებამოსილი პირი არის ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით“.

ღრუბლოვანი სისტემებით სარგებლობისას მომხმარებელი თავად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, შესაბამისად, სწორედ იგი არის დამუშავებისთვის პასუხისმგებელი პირი, ხოლო, მეორე მხრივ, ღრუბლოვანი სისტემის პროვაიდერ კომპანიას მომხმარებლის მონაცემთა დამუშავების ნაწილში პირადი მიზანი არ გააჩნია და მოქმედებს მხოლოდ დამუშავებისთვის პასუხისმგებელი პირი მიზნებისთვის, შესაბამისად იგი გვევლინება, როგორც დამუშავებაზე უფლებამოსილი პირი[6].

[5] შეად.: EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.

[6] შეად.: The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.

აქვე, უნდა აღინიშნოს, რომ, მონაცემთა დამუშავების პროცესში, როგორც წესი, დამუშავებისთვის პასუხისმგებელი პირი განსაზღვრავს „თამაშის წესებს“ და დამუშავებაზე უფლებამოსილი პირი „ემორჩილება“ მას. მიუხედავად ამისა, ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავებისას უმეტეს შემთხვევაში, სერვისის პროვაიდერის დომინანტური როლიდან და მისი რესურსებიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელი პირი თანხმდება დამუშავებაზე უფლებამოსილი პირის წესებსა და პირობებს. მაგალითად, თუკი მომხმარებელს სურს ისარგებლოს “Google Cloud Platform”-ით, მომხმარებელი ვერ განუსაზღვრავს ასეთ მასშტაბურ კომპანიას „თამაშის წესებს“, თუმცა მონაცემთა დამუშავების მიზნებს და საშუალებებს კვლავ მომხმარებელი განსაზღვრავს, რაც უმთავრეს კრიტერიუმს წარმოადგენს სამართლებრივი სტატუსის დადგენისას[7].

4. პერსონალური მონაცემების დამუშავება ღრუბლოვან სისტემებში

მონაცემთა დამუშავების ეფექტიანობიდან გამომდინარე, ღრუბლოვან სისტემებს აქტიურად იყენებენ როგორც კომპანიები, ისე სახელმწიფო ორგანოები. ამასთან, ღრუბლოვანი სისტემები მომხმარებლებს აძლევს შესაძლებლობას დაზოგონ ხარჯები და გააუმჯობესონ სერვისები.

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა დამუშავება რამდენიმე მნიშვნელოვან ეტაპად შეიძლება დაიყოს. პირველ რიგში, უნდა აღინიშნოს, რომ დამუშავებისთვის პასუხისმგებელი ნებისმიერი პირი თავად წყვეტს როგორ, რა ფორმით და რა მოცულობით ატვირთავს ღრუბლოვან სისტემაში მონაცემებს.

ღრუბლოვან სისტემებში მონაცემთა დამუშავების ყველაზე გავრცელებული სახე მათი შენახვაა (“Data at Rest”), რა დროსაც მნიშვნელოვანია გათვალისწინებული იყოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლით გათვალისწინებული უსაფრთხოების ზომები, როგორც პროვაიდერის მხრიდან, ისე დამუშავებისთვის პასუხისმგებელი პირის მხრიდან.

შენახვის გარდა, ღრუბლოვანი სისტემები გამოიყენება მონაცემთა სხვაგვარი დამუშავებისთვისაც (“Data in Use”), მაგალითად, მათი გადმოწერისთვის, გაზიარებისთვის, ანალიტიკისთვის, ხელოვნური ინტელექტის სწავლებისთვის და სხვა. ასეთ დროს, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, რომ ღრუბლოვანი სისტემის გამოყენება მას არ ათავისუფლებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული ვალდებულებებისგან, მათ შორის, დაიცვას უსაფრთხოების ტექნიკური თუ ორგანიზაციული ზომები და

[7] შეად. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].

რაც მთავარია მონაცემები დაამუშაოს შესაბამისი სამართლებრივი საფუძვლისა და პრინციპების შესაბამისად.

5. გამოწვევები და რისკები

არაერთხელ აღინიშნა, რომ ღრუბლოვანი სისტემები კომპანიებს და სახელმწიფოებს ეხმარება მონაცემთა ეფექტურ და მოქნილ დამუშავებაში, თუმცა, მეორე მხრივ, იგი ქმნის არაერთ პრობლემურ საკითხს, რომელიც დაკავშირებულია პერსონალურ მონაცემთა დამუშავების კანონიერებასთან. გამოწვევათაგან უმნიშვნელოვანესია უსაფრთხოებასთან და სისტემების ადგილმდებარეობასთან დაკავშირებული საკითხები.

5.1. ღრუბლოვანი სისტემის ადგილმდებარეობა და საერთაშორისო გადაცემის ასპექტი

ღრუბლოვანი სისტემების მთავარ განმასხვავებელ ნიშანს წარმოადგენს ის, რომ მომხმარებელს შეუძლია ინტერნეტის გამოყენებით ისარგებლოს სერვის პროვაიდერი კომპანიის ინფრასტრუქტურითა და დაამუშაოს მონაცემები მსოფლიოს ნებისმიერი წერტილიდან. შესაბამისად, როდესაც დამუშავებისთვის პასუხისმგებელი პირი იყენებს ღრუბლოვან სისტემებს, შესაძლოა, მონაცემები ინახებოდეს (ან სხვაგვარად მუშავდებოდეს) საქართველოს ფარგლებს გარეთ, გამომდინარე იქიდან, რომ ღრუბლოვანი სისტემების პროვაიდერი კომპანიების უმეტესობას, მათ შორის, “Google”-ს, “Amazon”-სა და “Microsoft”-ს საკუთარი ბაზები/ინფრასტრუქტურა განლაგებული აქვთ სხვადასხვა ქვეყნებში[8]. ასეთ დროს მნიშვნელოვანია გათვალისწინებულ იქნეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე მუხლი, რომლის თანახმადაც მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ არსებობს მონაცემთა დამუშავების ამ კანონით გათვალისწინებული მოთხოვნები და შესაბამის სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.[9]

აქვე უნდა აღინიშნოს, „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23

[8] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012, 16.

[9] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 37-ე მუხლი.

ბრძანება.[10] აღნიშნულ ბრძანებაში მოცემულია ქვეყნების ჩამონათვალი, სადაც მონაცემთა გადაცემა დასაშვებია დამატებითი საფუძვლის გარეშე.

ზემოაღნიშნული საკანონმდებლო ნორმიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელმა პირმა, პირველ რიგში, დეტალურად უნდა მოიკვლიოს თუ კონკრეტულად რომელ ქვეყანაში/ქვეყნებში ინახება მონაცემები[11].

შესაბამისი ინფორმაციის მიღების შემდეგ, თუკი დადგინდა, რომ მონაცემთა გადაცემა ხდება საქართველოს საზღვრებს გარეთ ისეთ ქვეყანაში, რომელიც არ არის სათანადო გარანტიების მქონე ქვეყნების ნუსხაში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს და მოითხოვოს ნებართვა მონაცემთა საერთაშორისო გადაცემაზე[12] ან მოიპოვოს მონაცემთა სუბიექტების წერილობითი თანხმობა[13].

ღრუბლოვანი სისტემების მეშვეობით მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებით საინტერესოა ევროკავშირის მონაცემთა დაცვის ზედამხედველის (“EDPS”) 2024 წლის 8 მარტის გადაწყვეტილება[14], რომლის ფარგლებშიც დადგინდა, რომ ევროკომისია (“European Commission”) იყენებდა “Microsoft 365”-ის პროგრამას, მონაცემებს ამუშავებდა ღრუბლოვანი სისტემის მეშვეობით, ხოლო სერვერები განლაგებული იყო აშშ-ში, აქედან გამომდინარე, ადგილი ჰქონდა მონაცემთა საერთაშორისო გადაცემას შესაბამისი სამართლებრივი საფუძვლის გარეშე.

5.2. უსაფრთხოება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის თანახმად, უსაფრთხოება მონაცემთა დამუშავების ერთ-ერთ პრინციპს წარმოადგენს, ამასთან, 27-ე მუხლის მე-2 პუნქტის თანახმად, „დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან მიიღონ მონაცემთა დამუშავების შესაძლო და თანამდევი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომები (მათ შორის, მონაცემთა ფსევდონიმიზაცია, მონაცემებზე წვდომის აღრიცხვა,

[10] „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანება.

[11] Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].

[12] უნდა აღინიშნოს, რომ ნებართვის მოპოვების შედეგად მონაცემთა საერთაშორისო გადაცემა არის ერთ-ერთი საფუძველი და ალტერნატივად, მონაცემთა დამუშავების სპეციფიკიდან გამომდინარე, შესაძლოა არსებობდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე მუხლის მეორე პუნქტით გათვალისწინებული სხვა საფუძველიც.

[13] სავალდებულოა, რომ წერილობითი თანხმობა აკმაყოფილებდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 32-ე და 37-ე მუხლის მეორე პუნქტი „დ“ ქვეპუნქტის მოთხოვნებს.

[14] EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.

ინფორმაციული უსაფრთხოების მექანიზმები (კონფიდენციალობა, მთლიანობა, ხელმისაწვდომობა) და სხვა), რომლებიც უზრუნველყოფს მონაცემთა დაცვას მონაცემთა დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან“.

ზემოაღნიშნული ჩანაწერიდან გამომდინარე, უსაფრთხოების უზრუნველყოფა ევალება, როგორც დამუშავებაზე უფლებამოსილ პირს - ღრუბლოვანი სისტემების პროვაიდერს, ისე დამუშავებისთვის პასუხისმგებელ პირს - სისტემის მომხმარებელს.

სისტემის სპეციფიკიდან გამომდინარე, ტექნიკური უსაფრთხოების უზრუნველყოფის უმთავრესი ნაწილი სერვისის პროვაიდერი, ანუ დამუშავებაზე უფლებამოსილი პირის ვალდებულებაა, კერძოდ, პირველ რიგში, მან უნდა უზრუნველყოს სისტემის იმგვარი წყობა, რომ სხვადასხვა მომხმარებლებს ერთმანეთის მონაცემებზე წვდომის შესაძლებლობა არ ჰქონდეთ. გარდა ამისა, სისტემა უნდა იყენებდეს დაშიფვრის იმგვარ ტექნოლოგიას (“Public” და “Private key”-ის გამოყენებით), რომ თავად პროვაიდერსაც არ ჰქონდეს, როგორც შენახული (“data at Rest”) ისე „მოძრავ“ (“Data in Use”) მონაცემებზე წვდომის შესაძლებლობა[15].

ჩვენს რეალობაში, საქართველოს კანონმდებლობა, როგორც წესი, ვრცელდება ღრუბლოვანი სერვისის მომხმარებლებზე, ანუ დამუშავებისთვის პასუხისმგებელ პირებზე, რადგან ღრუბლოვანი სისტემების პროვაიდერი ლიდერი კომპანიების საქმიანობა სცილდება საქართველოს იურისდიქციას. აღნიშნულიდან გამომდინარე, მნიშვნელოვანია, განისაზღვროს, უსაფრთხოების დაცვის კუთხით, რა ვალდებულებები გააჩნიათ ღრუბლოვანი სისტემების გამოყენებისას დაშვებისთვის პასუხისმგებელ პირებს.

პირველ რიგში, აუცილებელია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა მოიკვლიოს და შეაფასოს სხვადასხვა ღრუბლოვანი სისტემის უსაფრთხოების მექანიზმები და მხოლოდ ამის შემდგომ აირჩიოს სანდო და უსაფრთხო პროვაიდერი[16].

გარდა ამისა, ღრუბლოვანი სისტემის მომხმარებელმა უნდა უზრუნველყოს უსაფრთხოების ორგანიზაციული ნორმები და შესაბამის მონაცემებზე წვდომა მიანიჭოს მხოლოდ იმ პირებს, რომელსაც ამისი უფლებამოსილება, შესაბამისი საფუძველი და საჭიროება აქვთ[17], ამასთან, განახორციელონ სათანადო ღონისძიებები თანამშრომელთა მიერ მონაცემთა უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, მათ შორის, უზრუნველყონ თანამშრომელთა ინფორმირება მონაცემთა უსაფრთხოების დაცვის საკითხების შესახებ[18].

[15] CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012, 10.

[16] შეად. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 13-14, <https://ico.org.uk/> [10.03.2025].

[17] შეად. EU Data Protection Code of Conduct for Cloud Service Providers, 2020, 17-20.

[18] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, 27-ე მუხლის მე-6 პუნქტი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის მე-4 პუნქტის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა. როგორც წესი, ღრუბლოვანი სისტემებს ე.წ. „ლოგირების“ ფუნქცია გააჩნია, მიუხედავად ამისა, დამუშავებისთვის პასუხისმგებელი პირი, ვალდებულია შექმნას რამდენიმე ინდივიდუალური მომხმარებელი, რათა, საჭიროების შემთხვევაში, დადგენადი იყოს კონკრეტულად ვის მიერ მოხდა მონაცემთა რედაქტირება, წაშლა, დამატება და სხვა მოქმედება[19].

6. დასკვნა

დასკვნის სახით შეიძლება ითქვას, რომ ღრუბლოვანი სისტემის პოპულარობის ზრდა, გარდაუვალია, რადგან იგი მონაცემთა სწრაფი და მოქნილი დამუშავების ერთ-ერთი საუკეთესო ტექნოლოგიაა, რომელიც კომპანიებს, სახელმწიფოებს თუ ფიზიკურ პირებს აძლევს შესაძლებლობას დაზოგონ ხარჯები, გაზარდონ ეფექტიანობა და მიიღონ მონაცემებზე წვდომა მსოფლიოს ნებისმიერი წერტილიდან, სხვადასხვა მოწყობილობის მეშვეობით.

ღრუბლოვანი სისტემების შესაძლებლობებს თან ახლავს არაერთი გამოწვევა, რომელიც დაკავშირებულია პერსონალური მონაცემების დამუშავების სამართლებრივ თუ ეთიკურ საკითხებთან.

გამოწვევებისთვის დასაძლევად, სავალდებულოა, რომ დამუშავებისთვის პასუხისმგებელმა/დამუშავებაზე უფლებამოსილმა პირებმა დაიცვან უსაფრთხოების ზომები, კერძოდ, სისტემის პროვაიდერმა იქონიოს მონაცემთა დაშიფვრის ძლიერი ტექნოლოგია, ხოლო მომხმარებელმა, თავის მხრივ, მონაცემებზე წვდომა მიანიჭოს მხოლოდ უფლებამოსილ პირებს და დაიცვას სხვა ორგანიზაციული ნორმები.

გარდა ამისა, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განსაზღვრონ მონაცემთა შენახვის ადგილმდებარეობა და საჭიროების შემთხვევაში შეიქმნან შესაბამისი სამართლებრივი საფუძველი მონაცემთა საერთაშორისო გადაცემისათვის.

აქვე უნდა აღინიშნოს, რომ აუცილებელია ღრუბლოვანი სისტემების და მონაცემთა დაცვის კანონმდებლობას შორის ურთიერთმიმართებაზე ცნობიერების ამაღლება, რათა დამუშავებისთვის პასუხისმგებელ პირებს ჰქონდეს მეტი ინფორმაცია ღრუბლოვანი სისტემების გამოწვევების და მათგან მომდინარე საკანონმდებლო ვალდებულებების თაობაზე, რადგან, პერსონალურ მონაცემთა დაცვა არამხოლოდ ტექნიკური საკანონმდებლო

[19] შეად. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 14-15, <https://ico.org.uk/> [10.03.2025].

მოთხოვნა, არამედ მონაცემთა ნებისმიერი დამუშავებისთვის პასუხისმგებელი პირის ფუნდამენტური პასუხისმგებლობაა.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანება.
3. CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012.
4. EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.
5. EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.
6. EU Data Protection Code of Conduct for Cloud Service Providers, 2020.
7. European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012.
8. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].
9. National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012.
10. Public cloud services end-user spending worldwide from 2017 to 2024 <https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].
11. The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.