თამარ სამნიაშვილი*

მონაცემთა სუბიექტის თანხმობა, როგორც სამართლებრივი საფუძველი: თეორიული და პრაქტიკული ასპექტები

სტატიაში განხილულია მონაცემთა სუბიექტის თანხმობის ინსტიტუტი, როგორც პერსონალურ მონაცემთა დამუშავების სამართლებრივი საფუძველი. გაანალიზებულია თანხმობის კანონიერების კრიტერიუმები და მისი ფორმულირების თავისებურებები სამართლებრივ დოკუმენტებში, ხელშეკრულებებსა და ონლაინ სივრცეებში, გამჭვირვალობისა და ინფორმირებულობის პრინციპების დაცვის აუცილებლობის გათვალისწინებით.

სტატია ეფუძნება საქართველოს ეროვნული კანონმდებლობისა და საერთაშორისო სამართლის, განსაკუთრებით კი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”)[1] შედარებით ანალიზს. გამოკვეთილია თანხმობის ინსტიტუტის პრაქტიკაში რეალიზების ძირითადი გამოწვევები და რისკები. სტატიაში წარმოჩენილია თანხმობის ეფექტური გამოყენებისთვის საჭირო კრიტერიუმები, რომელთა პრაქტიკაში დანერგვა და რეალიზებაც ხელს უწყობს მონაცემთა დაცვის კულტურის განვითარებასა და საზოგადოების ნდობის გამყარებას როგორც კერძო, ისე საჯარო სექტორში.

საკვანძო სიტყვები: *პერსონალური მონაცემები, განსაკუთრებული კატეგორიის მონაცემები, არასრულწლოვნის პერსონალური მონაცემები, თანხმობა, არასრულწლოვნის თანხმობა, თანხმობის გამოხმობის უფლება, თანხმობა ხელშეკრულებაში, თანხმობა ონლაინ სივრცეში, მზა ჩანაწერები („cookie ფაილები“), „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”).*

---

* ილიას სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი, სსიპ - საქართველოს ეროვნული არქივის პერსონალურ მონაცემთა დაცვის ოფიცერი.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016 (შემდგომში — GDPR).

1. შესავალი

მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავების თაობაზე „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით გათვალისწინებულ ერთ-ერთ სამართლებრივ საფუძველს წარმოადგენს.[2] საკითხი, რომ მონაცემთა დამუშავებისათვის პასუხისმგებელ პირს მონაცემთა დამუშავებისათვის ესაჭიროება სამართლებრივი საფუძველი, სიახლეს არ წარმოადგენს. საზოგადოების სამართლებრივი ცნობიერების ზრდასთან ერთად, ერთი მხრივ, იზრდება მონაცემთა სუბიექტის მოლოდინები/მოთხოვნები და, მეორე მხრივ, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთა ვალდებულება, დაამუშაონ მონაცემები კანონშესაბამისად.

თანხმობა, როგორც პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი, პრაქტიკაში ერთ-ერთ ხშირად გამოყენებულ და აქტუალურ საკითხს წარმოადგენს. შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო თანხმობის საკითხზე მსჯელობისას აღნიშნავს, რომ ის, როგორც წესი, არც ყველაზე მარტივ და არც ყველაზე შესაბამის ალტერნატივას არ წარმოადგენს, მაგალითად, იმიტომ, რომ პირი, რომელიც თანხმობას გასცემს, უფლებამოსილია ნებისმიერ დროს გამოითხოვოს იგი.[3]

აღნიშნულ საფუძველს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები, უმეტეს შემთხვევაში, არსებული/დაგეგმილი პროცესების კანონთან შესაბამისობაში მოსაყვანად იყენებენ. კერძოდ, შემთხვევებში, როდესაც სახეზე არ არის მონაცემთა დამუშავების სხვა სამართლებრივი საფუძველი და, შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი პროცესისთვის საფუძვლის შექმნას თანხმობის მოპოვებით ახორციელებს. აღნიშნულ შემთხვევაში კი წარმოიქმნება რისკი, რომ თანხმობა იქცეს „უნივერსალურ ინსტრუმენტად", რომელიც პასუხისმგებელ პირებს საშუალებას მისცემს, პროცესები მხოლოდ ფორმალურად მოაქციოს სამართლებრივ ჩარჩოში. შესაბამისად, ყურადღების მიღმა არ უნდა დარჩეს ის რისკები, რომლებიც აღნიშნული საფუძვლის მოპოვებას და შემდგომში მის რეალიზებას შესაძლოა ახლდეს თან.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანო ("ICO") თანხმობის საკითხზე მსჯელობისას სარეკომენდაციო მითითებას იძლევა, რომლის თანახმადაც, კონკრეტულ პროცესში შერჩეულ უნდა იქნეს სამართლებრივი საფუძველი, რომელიც ყველაზე ზუსტად ასახავს დამუშავების მიზანსა და რეალურ ურთიერთობას სუბიექტთან. თუ თანხმობის

[2] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", №3144-XIმს-Xმპ, 14/06/2023, მუხლი 5 (1) (ა).

[3] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 15, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

მიღება რთულია, ხშირად ამის მიზეზი არის ის, რომ სხვა სამართლებრივი საფუძველი უფრო შესაფერისია და ამიტომ უნდა იქნეს განხილული ალტერნატივები.[4]

თანხმობის მნიშვნელობა კიდევ უფრო თვალსაჩინო ხდება თანამედროვე ციფრულ რეალობაში. ინტერნეტსერვისების, სოციალური ქსელების, მობილური აპლიკაციების და ციფრული მარკეტინგის ეპოქაში მონაცემთა დამუშავების უდიდესი ნაწილი სწორედ თანხმობის საფუძველს ეფუძნება. მომხმარებლები ყოველდღიურად აჭერენ ღილაკს „ვეთანხმები“, თუმცა რეალურად იშვიათად აქვთ დრო ან შესაძლებლობა, სრულად გაეცნონ, რას გულისხმობს ეს თანხმობა და რამდენად რეალურია მათი თავისუფალი არჩევანი. სწორედ ამიტომ ბოლო წლების განმავლობაში განსაკუთრებით გააქტიურდა დისკუსია „ფორმალური თანხმობის“ პრობლემასა და მის ეფექტიანობაზე.

პრაქტიკაში თანხმობის გამოყენება განსაკუთრებით აქტუალურია კერძო სექტორში, რომელშიც ის ხშირად დაკავშირებულია პირდაპირ მარკეტინგთან, დასაქმების პროცესებთან, სადაზღვევო და საბანკო მომსახურებასთან, განათლებისა და ჯანდაცვის სექტორში მონაცემთა დამუშავებასთან. საჯარო სექტორში თანხმობის გამოყენება შედარებით შეზღუდულია, ვინაიდან აღნიშნულ სექტორში მონაცემთა დამუშავება უმეტესად კანონით დადგენილ ვალდებულებებს ან საჯარო ინტერესს ეფუძნება. აღნიშნულ შემთხვევებში ნებაყოფლობითობის საკითხი განსაკუთრებით სენსიტიურია, რადგან მოქალაქე საჯარო უწყებასთან ურთიერთობისას ხშირად ვერ აღიქვამს თანხმობის თავისუფალ არჩევანს. სწორედ ამიტომ, უმრავლეს შემთხვევაში, „საჯარო დაწესებულებები ვერ დაეყრდნობიან მონაცემთა სუბიექტის თანხმობას, მონაცემთა სუბიექტსა და დამუშავებისთვის პასუხისმგებელ პირთა შორის ძალთა ბალანსის გათვალისწინებით.“[5]

სტატიის მიზანი არა მხოლოდ თანხმობის, როგორც მონაცემთა დამუშავების სამართლებრივი საფუძვლის, თეორიული ანალიზია, არამედ მისი პრაქტიკული მნიშვნელობის, მასთან დაკავშირებული რისკების და განვითარების პერსპექტივების გამოკვეთაა.

[4] *Information Commissioner's Office (ICO)* Guideline on *When is consent appropriate?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].

[5] პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა სუბიექტისგან თანხმობის მიღების“ შესახებ, 10.

2. პერსონალური მონაცემების დამუშავება თანხმობის საფუძველზე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ითვალისწინებს თანხმობის დეფინიციას და განსაზღვრავს მისი კანონიერად მიჩნევისთვის სავალდებულო კრიტერიუმებს:[6]

- **ინფორმაციის მიღების შემდეგ** - გაცემულ თანხმობას არ უნდა ჰქონდეს წინმსწრები ხასიათი, უნდა გაიცეს მას შემდეგ, რაც სუბიექტს მიეწოდა ინფორმაცია, თუ რის თაობაზე არის მოთხოვნილი თანხმობა. აღნიშნული, თავის მხრივ, უზრუნველყოფს რეალური არჩევანის შესაძლებლობას;
- **ინფორმირებულობა** - მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები უნდა დარწმუნდნენ, რომ იყენებენ გასაგებ და მარტივ ენას ინფორმირებისათვის. ტექსტი უნდა იყოს მარტივად გასაგები ნებისმიერი პირისათვის და არა მხოლოდ იურისტებისათვის, არ უნდა შეიცავდეს გრძელ, რთულად გასაგებ კონფიდენციალობის პოლიტიკებსა და წესებს, რომლებიც წარმოდგენილი იქნება მხოლოდ იურიდიული ტერმინებით;
- **კონკრეტული მიზანი** - აღნიშნული კრიტერიუმიც პირდაპირ უკავშირდება ინფორმირების მოთხოვნასთან. სუბიექტისათვის ცნობილი უნდა იყოს, კონკრეტულად რა მიზნით მუშავდება მისი მონაცემები და რაზე გასცემს შესაბამის თანხმობას;
- **აქტიური მოქმედება** - თანხმობა უნდა იყოს მონაცემთა სუბიექტის აქტიური ქმედებით დაფიქსირებული, რაც კონკრეტულ შემთხვევაში შესაძლოა გამოიხატოს თანხმობის თაობაზე წერილობითი ფორმის არსებობისას მონიშვნის გაკეთებით, ბმულზე გადასვლით, ზეპირი სახით თანხმობის განცხადებით ან სხვა შესაბამისი ფორმით;
- **თავისუფლება** - თანხმობის თავისუფალი ხასიათი გულისხმობს შესაძლებლობას, მონაცემთა სუბიექტმა დამოუკიდებლად, ზეწოლის გარეშე მიიღოს გადაწყვეტილება საკუთარი მონაცემების დამუშავების თაობაზე;
- **მკაფიოობა** - მონაცემთა სუბიექტის ნება კონკრეტული მონაცემების ასევე კონკრეტული დამუშავების თაობაზე უნდა იყოს მკაფიო და არ უნდა იწვევდეს ეჭვს მისი არსებობის საკითხი;
- **ფორმა** - წერილობით (მათ შორის ელექტრონულად) ან ზეპირად - ფორმის საკითხი ძირითადად დამოკიდებულია მონაცემთა კატეგორიაზე, რომლის დამუშავების შესახებაც გაიცემა შესაბამისი თანხმობა. კერძოდ, განსაკუთრებული კატეგორიის მონაცემთა შემთხვევაში მხოლოდ წერილობითი ფორმით არის შესაძლებელი

[6] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 3 (მ).

თანხმობის გაცხადება.[7] ასევე მსგავს, კონკრეტულ რეგულირებას ითვალისწინებს კანონი პირდაპირი მარკეტინგის განხორციელებისას სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მონაცემების გარდა სხვა მონაცემების დამუშავებისას.[8]

აღსანიშნავია, რომ თანხმობის მოთხოვნები ხშირად ქმნის მონაცემთა სუბიექტისთვის არჩევანის ილუზიას, მაშინ როდესაც სინამდვილეში ასეთი არჩევანის შესაძლებლობა არ არსებობს.[9] შესაბამისად, თანხმობის კანონიერების შეფასების ეტაპზე მნიშვნელოვანია, რომ ყველა ზემოთ ჩამოთვლილი კრიტერიუმი სრულად დაკმაყოფილდეს.

3. თანხმობა პრაქტიკაში

თანხმობა მონაცემთა დამუშავების საფუძვლად ძირითადად კერძო სექტორის შემთხვევაში გვხვდება. აღნიშნულის განმაპირობებელი ძირითადად ის ფაქტია, რომ, საჯარო სექტორის შემთხვევაში, მისი წარმომადგენლების მხრიდან მონაცემთა დამუშავებისას იშვიათ შემთხვევებში თუ არის შესაძლებელი წარმოვიდგინოთ კონკრეტული სიტუაცია, როდესაც თანხმობა მონაცემთა სუბიექტის მიერ არ აღიქმება იძულებითი ხასიათის მატარებლად როგორც პირდაპირი, ასევე ირიბი ხასიათის ზემოქმედებისა და მოსალოდნელი გავლენის გათვალისწინებით.

მსგავსი საფრთხე შესაძლოა არსებობდეს მონაცემთა სუბიექტის თანხმობის კანონიერებასთან დაკავშირებით, როდესაც სუბიექტი დასაქმებული პირია, ხოლო მონაცემთა დამუშავება დამსაქმებლის მიერ ხორციელდება. აღნიშნულ შემთხვევაშიც აშკარაა დაქვემდებარებული მდგომარეობა და, შესაბამისად, რეალური საფრთხე, რომ მონაცემთა სუბიექტის მიერ კონკრეტული პროცესი დაკავშირებული იქნება გარკვეულ ზეწოლასა და მის მიერ გაცხადებულ ნებაზე უარყოფით გავლენასა და დამოკიდებულებაზე.

თუმცა არ ნიშნავს, რომ დამსაქმებლები ვერასდროს დაეყრდნობიან თანხმობას, როგორც მონაცემთა დამუშავების სამართლებრივ საფუძველს. შესაძლოა არსებობდეს სიტუაციები, როდესაც დამსაქმებელი შეძლებს დაამტკიცოს, რომ თანხმობა მართლაც თავისუფლად არის გაცემული. დამსაქმებელსა და თანამშრომლებს შორის არსებული ძალაუფლების უთანასწორობის გამო, თანამშრომლები თავისუფალი ნების გამოვლენას მხოლოდ გამონაკლის შემთხვევებში შეძლებენ, მაშინ, როდესაც მათი

[7] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 6 (1)(ა).
[8] იქვე, მუხლი 12 (2).
[9] *Cate, F. H.* The Failure of Fair Information Practice Principles In *Consumer Protection in the Age of the Information Economy* 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].

თანხმობის გაცემა ან მასზე უარი ნამდვილად არ გამოიწვევს რაიმე უარყოფით შედეგს.[10]

დამუშავების საფუძვლად თანხმობის განსაზღვრისას მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს საკმაოდ მნიშვნელოვანი ბერკეტები აქვთ ხელთ, რომელთა კანონშეუსაბამო, ან „შეფარვითი" ფორმულირებისასაც, შესაძლოა მოპოვებულ თანხმობას სამართლებრივი ძალა არ ჰქონდეს და შეფასებისას დადგინდეს, რომ დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა დამუშავების კონკრეტულ პროცესს რეალურად სამართლებრივი საფუძვლის გარეშე ახორციელებდა.

ასევე საყურადღებოა შემთხვევა, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი თანხმობას უთითებს დამუშავების საფუძვლად იმ კატეგორიის მონაცემებისათვის, რომლებიც ფაქტობრივად აუცილებელია გარიგების შესრულებისთვის. აღნიშნულ შემთხვევაში მიიჩნევა, რომ თანხმობა სწორი სამართლებრივი საფუძველი არ არის.[11]

რა თქმა უნდა, გამოირიცხება შემთხვევა, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტის თანხმობას მხოლოდ მოიაზრებს მის ისეთ ქმედებებში, როგორებიცაა: დუმილი, უმოქმედობა, წინასწარ განხორციელებული მონიშვნები, საწყისი პარამეტრებისა და წესებისა და პირობების ერთიანი მიღების შემთხვევები.

ხშირია მოსაზრება, რომ მონაცემთა დამუშავების სამართლებრივ საფუძვლად სუბიექტის თანხმობის მითითება საფრთხის შემცველი და რისკის მატარებელი შესაძლოა აღმოჩნდეს, აღნიშნული საფრთხეები კი შესაძლოა წარმოჩნდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ სრულყოფილი ინფორმირების მიუხედავად. ამერიკელი მონაცემთა დაცვის და კონფიდენციალობის ექსპერტი ფრედ ქეითი თავის ნაშრომში, „სამართლიანი ინფორმირების პრაქტიკული პრინციპების წარუმატებლობა", ინფორმირების პრაქტიკაში რეალიზების სირთულეებს შორის გამოყოფს საზოგადოების მხრიდან იგნორს მიწოდებული კონფიდენციალობის პოლიტიკებისა და ინფორმაციის მიმართ.

ამასთან, მონაცემთა დაცვის რეგულაციების და მარეგულირებელი კანონმდებლობის კომპლექსურობის მატებასთან ერთად, რთულდება ასევე იმ შეტყობინებების შინაარსი, რომელთაც აღნიშნული რეგულირებები მოითხოვს.[12]

ასევე, მსგავს რისკებს განიხილავს მონაცემთა დაცვის ევროპული საბჭო ("EDPB") სახელმძღვანელო რეკომენდაციაში თანხმობის შესახებ, რომელშიც

---

[10] *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018,7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].

[11] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 10, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[12] *Cate, F. H.* The Failure of Fair Information Practice Principles In *Consumer Protection in the Age of the Information Economy,* 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].

აღნიშნულია საფრთხის თაობაზე, როდესაც, მონაცემთა სუბიექტები მათი მხრიდან თანხმობის ხშირად გაცემის შედეგად, თანხმობის მოპოვების ფორმების გაცნობის გარეშე გამოხატავენ ნებას, როდესაც წარმოიქმნება რეალური რისკი მათთვის, რადგან, როგორც წესი, თანხმობა მოთხოვნილია ისეთი ქმედებებისთვის, რომლებიც შესაბამისი ნების გამოხატვის გარეშე კანონიერი არ იქნებოდა.[13]

აღნიშნული გარემოებები კი, თავის მხრივ, ზრდის თანხმობის კანონიერებასთან დაკავშირებულ რისკებს.

3.1. არასრულწლოვნის თანხმობა

არასრულწლოვნის მონაცემების კანონიერად დამუშავების საკითხის მნიშვნელობას მისი სპეციალური წესით რეგულირებაც მოწმობს. საქართველოს ეროვნული კანონმდებლობით, ისევე, როგორც საერთაშორისო სტანდარტებით, განსაკუთრებული ყურადღება ექცევა არასრულწლოვნის უფლებების დაცვას და მათი რეალიზების რეალური მექანიზმების დანერგვას. აღნიშნული კი, პირველ რიგში, თავად არასრულწლოვნის ბუნებრივი მახასიათებლებით არის განპირობებული. მათი მხრიდან საკითხის მნიშვნელობისა და რისკების შესაძლო არასრულყოფილი აღქმა, საუკეთესო ინტერესების სრულად შეუფასებლობა წარმოადგენს იმ გარემოებათა არასრულ ჩამონათვალს, რომლებიც განაპირობებს მათი უფლებების დაცვის მაღალ სტანდარტს.

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო ყურადღებას ამახვილებს ონლაინ სივრცეში არასრულწლოვანთა უფლებების დაცვის საკითხზე. ბავშვები და ახალგაზრდა პირები სწრაფად და პროფესიონალურად გადაადგილდებიან სხვადასხვა პლატფორმაზე, მაგრამ ეს ყოველთვის არ ნიშნავს, რომ ისინი აცნობიერებენ რისკებს ან სრულად ხვდებიან შედეგებს, რომლებიც შესაძლოა მომავალში გამოვლინდეს.[14]

არასრულწლოვნისგან თანხმობის მოპოვებისას მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს თანხმობის ტექსტის მარტივი, აღქმადი, ბავშვისთვის გასაგები ენით მიწოდება, საჭიროების შემთხვევაში დამატებითი ვიზუალური საშუალებების გამოყენებით.[15] აღნიშნული საშუალებების რამდენიმე მაგალითს განიხილავს ასევე მონაცემთა დაცვის კომისია (“Data Protection Commission”): ანიმაციები,

---

[13] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[14] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide,3, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

[15] *The Autoriteit Persoonsgegevens (AP)*, Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].

ვიდეოები, სურათები, გამოსახულებები, თამაშთან დაკავშირებული ნიშნები - მორგებული მომხმარებელთა ასაკობრივ ჯგუფზე, განხილულია არასრულწლოვანთათვის ინფორმირების ეფექტიან საშუალებად.[16]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ასევე განსაზღვრავს საკითხის რეგულირების სპეციალურ წესს, როდესაც საქმე ეხება არასრულწლოვნის განსაკუთრებული კატეგორიის მონაცემებს.[17] აღნიშნულ შემთხვევაში, გარდა არასრულწლოვანთან დაკავშირებული მაღალი რისკისა, დამატებით თავს იჩენს თავად მონაცემთა მახასიათებელი, რაც განაპირობებს დაცვის მაღალ სტანდარტს. კერძოდ, არასრულწლოვნის განსაკუთრებული კატეგორიის მონაცემთა დამუშავება კანონის შესაბამისად, შესაძლებელია მხოლოდ მისი მშობლის ან კანონიერი წარმომადგენლის წერილობითი თანხმობით, თუ კანონით სხვა რამ არ არის გათვალისწინებული.[18]

3.1.1. არასრულწლოვნის თანხმობა – საერთაშორისო და ეროვნული პრაქტიკა

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”), ისევე როგორც საქართველოს ეროვნული კანონმდებლობა, სპეციალურ რეგულირებას ითვალისწინებს არასრულწლოვნის მონაცემების დამუშავებისათვის. კერძოდ, განხილულ შემთხვევებში ზღვრულ ასაკად მიჩნეულია 16 წელი, როდესაც მონაცემთა სუბიექტს ენიჭება უფლება განკარგოს საკუთარი პერსონალური მონაცემები და დაეთანხმოს დამუშავების კონკრეტულ პროცესს.[19] საკითხის სრულყოფილი განხილვისთვის უნდა აღინიშნოს ხსენებული წესიდან გამონაკლისები, როდესაც კანონი პირდაპირ განსაზღვრავს რეგულირების განსხვავებულ წესს.[20]

დამატებით უნდა აღინიშნოს, რომ საქართველოს კანონმდებლობა არასრულწლოვანთა მონაცემების დამუშავებისას მონაცემთა სუბიექტის დაცვის მაღალი სტანდარტის უზრუნველსაყოფად მკაცრ მოთხოვნებს აწესებს და მინიმალურ ასაკს მონაცემთა დამუშავებაზე თანხმობის გაცემისათვის 16 წელს ითვალისწინებს,[21] მაშინ, როდესაც “GDPR”-ის მე-8 მუხლი იძლევა საშუალებას, წევრი სახელმწიფოების მიერ მინიმალური ასაკად არანაკლებ 13

---

[16] *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021, 29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].

[17] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 7 (3).

[18] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 7 (1).

[19] GDPR, Article 8 (1).

[20] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, №3144-XIმს-Xმპ, 14/06/2023, მუხლი 7 (1).

[21] იქვე.

წელი განისაზღვროს.[22] აღნიშნული განსხვავება ასახავს საქართველოს კანონმდებლობის მიდრეკილებას არასრულწლოვანთა მონაცემთა დაცვის მიმართულებით უფრო მკაცრი სტანდარტის შენარჩუნებისკენ.

აღნიშნული მიდგომის საპირისპიროდ, ბრიტანეთის მონაცემთა დაცვის ზოგადი რეგულაცია (UK GDPR) იყენებს უფრო მოქნილ რეგულირებას და განსაზღვრავს, რომ არასრულწლოვნის მონაცემთა დამუშავებისას თანხმობის გაცემისთვის მინიმალური ასაკი 13 წელია.[23]

შვედეთის მონაცემთა დაცვის საზედამხედველო ორგანო გზამკვლევში „ციფრულ პლატფორმებზე ბავშვებისა და ახალგაზრდა პირების უფლებების შესახებ“ 13-დან 16 წლამდე პირების მიერ თანხმობის გაცემის საკითხზე მსჯელობისას აღნიშნავს, რომ თითოეულ კონკრეტულ შემთხვევაში უნდა შეფასდეს, შეუძლია თუ არა აღნიშნულ პირს, გააცნობიეროს თანხმობის შედეგები. ამ შეფასებაზე მოქმედებს რამდენიმე ფაქტორი, მათ შორის: რამდენად სენსიტიურია მოწოდებული პერსონალური მონაცემები, რამდენ ხანს ინახება ისინი, ასევე ბავშვის ასაკი და განვითარების დონე.[24]

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანო (“CNIL — Commission nationale de l'informatique et des libertés”) არასრულწლოვანთა მონაცემების დაცვის საკითხზე მსჯელობისას ასევე ყურადღებას ამახვილებს მშობელთა მხრიდან კონტროლის მექანიზმების მნიშვნელობაზე. „არასრულწლოვნები ყოველთვის ვერ ახერხებენ სრულად გააცნობიერონ ის რისკები, რომლებიც ონლაინ სივრცეში ემუქრებათ, და მიიღონ ინფორმირებული გადაწყვეტილებები. მშობლებს სჭირდებათ ეფექტიანი საშუალებები, რათა მხარი დაუჭირონ ბავშვებს მათ ონლაინ ცხოვრებაში.“[25]თუმცა აქვე არის აღნიშვნა საჭირო სიფრთხილესთან დაკავშირებით, რომ კონტროლის მექანიზმი არ იყოს განსაკუთრებით ჩამრევი ხასიათის, რათა მათი გამოყენება არ იწვევდეს არასრულწლოვანში მუდმივი მეთვაყურეობის ქვეშ ყოფნის განცდას.[26]

საფრანგეთის მონაცემთა დაცვის საზედამხედბელო ორგანოს (“CNIL”) რეკომენდაციაში ასევე განსაზღვრულია მშობელთა კონტროლის მექანიზმების მონაცემთა დაცვის რეგულაციებთან შესაბამისობის საჭიროებაც. კერძოდ, აღნიშნული მექანიზმების შეფასებისას სახეზე უნდა იყოს შემდეგი წინაპირობები:

- **პროპორციულობის პრინციპი**, რომელიც ითვალისწინებს ბავშვის საუკეთესო ინტერესებს, ასაკს, განვითარების დონესა და ისეთი

[22] GDPR, Article 8 (1).
[23] UK General Data Protection Regulation (UK GDPR), Article 8 (1).
[24] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide,20,< https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[25] *CNIL (Commission nationale de l'informatique et des libertés), Recommendation 5: Promote parental controls that respect the child's privacy and best interests,* 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
[26] იქვე.

ზედმეტად ჩამრევი ფუნქციების გამოყენების გამორიცხვას, მაგალითად, როგორიცაა მუდმივი თვალყურის დევნება;

- **გამჭვირვალობის პრინციპი** ბავშვის მიმართ, რომელიც მოიაზრებს კონტროლის მექანიზმების შესახებ ზუსტი ინფორმაციის მიწოდებას;
- **ბავშვის მონაცემთა უსაფრთხოების პრინციპი**, რათა მშობელმა უზრუნველყოს, რომ მესამე პირებს არ ჰქონდეთ წვდომა მოპოვებულ მონაცემებზე (მაგ: ბავშვის გეოლოკაციის მონაცემები).[27]

მშობელთა/კანონიერ წარმომადგენელთა მიერ არასრულწლოვანთა კონტროლის საკითხზე მსჯელობისას შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო აღნიშნავს, რომ ბავშვები არ უნდა დაექვემდებარონ მათი პირადი და ოჯახური ცხოვრებისთვის უკანონო და თვითნებურ შეზღუდვებს. კონტროლის განმახორციელებლებს ეკისრებათ პასუხისმგებლობა ბავშვის აღზრდასა და განვითარებაზე მათი საუკეთესო ინტერესების გათვალისწინებით, აღნიშნულ კონტექსტში კი განსაკუთრებით მნიშვნელოვანი ამოცანაა არსებული ინტერესების დაბალანსება და მისი მნიშვნელობის გაცნობიერება. ამასთან, რაც ასაკით უფროსია ბავშვი, მით მეტი ყურადღება უნდა ექცეოდეს მის თავისუფალ ნებასა და თანხმობის გამოხატვის უფლებას.[28]

3.2. თანხმობა დოკუმენტში, რომლითაც რამდენიმე საკითხი არის დარეგულირებული

მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს განსაკუთრებული სიფრთხილე მართებს, როდესაც თანხმობის ფორმულირება შემადგენელი ნაწილია დოკუმენტის, რომელიც თანხმობის საკითხთან ერთად არეგულირებს სხვა საკითხებსაც.

აღნიშნულ შემთხვევაში განსაკუთრებით მნიშვნელოვანია შესაბამის დოკუმენტში თანხმობის ტექსტი იყოს ჩამოყალიბებული მკაფიოდ, მარტივი და გასაგები ენით და ასევე გამოყოფილად დოკუმენტის სხვა ნაწილებისგან.[29]

მსგავს რეგულირებას ითვალისწინებს ასევე "GDPR"-ის დოკუმენტიც. მე-7 მუხლის მე-2 ნაწილის თანახმად, თუ მონაცემთა სუბიექტი თანხმობას გამოხატავს წერილობით დოკუმენტში, რომელიც სხვა საკითხებსაც არეგულირებს, თანხმობასთან დაკავშირებული ტექსტი/განცხადება უნდა

[27] იქვე.
[28] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 40, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[29] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", №3144-XIმს-Xმპ, 14/06/2023, მუხლი 32 (1).

იყოს მოცემული იმგვარად, რომ ნათლად გამოირჩეოდეს სხვა საკითხებისაგან, იყოს გასაგები და იოლად აღქმადი, დაწერილი ნათელი და მარტივი ენით.[30]

განხილული მოთხოვნა ემყარება მონაცემთა დამუშავების პროცესში გამჭვირვალობის პრინციპის დაცვასა და რეალიზებას. მონაცემთა სუბიექტისთვის ნათელი უნდა იყოს, კონკრეტულად რომელ დამუშავების პროცესზე აცხადებს თანხმობას, რომელი მონაცემები დამუშავდება, რა მიზნითა და საფუძვლით. სავალდებულო წესით უნდა გამოირიცხოს თანხმობის ფორმათა ფორმულირება იმ წესით, როდესაც ის არ არის თვალსაჩინო, დოკუმენტის სრული ტექსტისგან გამოყოფილი და გონივრული შეფასებით არ აღიქმება, როგორც მონაცემთა სუბიექტისთვის მიცემული არჩევანი საკუთარი მონაცემების განკარგვასთან დაკავშირებით.

3.3. თანხმობა ხელშეკრულებაში

გამჭვირვალობის პრინციპის დაცვა განსაკუთრებით მნიშვნელოვანია როდესაც დოკუმენტი, რომლითაც მონაცემთა სუბიექტისგან თანხმობა არის მოპოვებული, წარმოადგენს ხელშეკრულებას.

აღნიშნულ შემთხვევაში თანხმობის ნებაყოფლობითობის საკითხი განსაკუთრებით სენსიტიურია, ვინაიდან ხელშეკრულების დოკუმენტში ფორმულირებული თანხმობა უნდა იძლეოდეს იმის საშუალებას, რომ მონაცემთა სუბიექტმა აღიქვას საკუთარი ნების ნებაყოფლობითად გამოხატვის თავისუფლება, რომ შეუძლია, თავისუფლად გააკეთოს არჩევანი და მის მიერ მიღებული გადაწყვეტილება არ იმოქმედებს ხელშეკრულების პირობებზე, მათ შორის ხელშეკრულების დადება/არდადების საკითხზეც.

„როდესაც მონაცემთა სუბიექტის თანხმობა გაცემულია ხელშეკრულების ან მომსახურების ფარგლებში, თანხმობის ნებაყოფლობითობის განსაზღვრისას, სხვა გარემოებებთან ერთად, უნდა შეფასდეს, თუ რამდენად არის თანხმობა ხელშეკრულების ან მომსახურების აუცილებელი წინაპირობა და თუ შეიძლება ამ თანხმობის გარეშე შესაბამისი მომსახურების მიღება/ხელშეკრულების დადება.”[31]

აღნიშნული რეგულირება შესაბამისია “GDPR”-ის მიდგომასთან, რომელიც ხაზს უსვამს მონაცემთა დამუშავებაზე თანხმობის გაცემისას სუბიექტის ნების ნათლად გამოვლენას, დამუშავდეს ის მონაცემებიც, რომლებიც არ არის აუცილებელი ხელშეკრულების შესრულებისთვის.[32]

3.4. თანხმობა ონლაინ სივრცეში

[30] GDPR, Article 7 (2).
[31] პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა სუბიექტისგან თანხმობის მიღების“ შესახებ, 21.
[32] GDPR, Article 7 (4).

დღევანდელი რეალობის გაციფრულებისა და ონლაინ სერვისების გამოყენების მზარდი ტენდენციების პარალელურად იზრდება ონლაინ პლატფორმებზე მონაცემთა სუბიექტისგან მონაცემთა დამუშავებაზე მოპოვებულ თანხმობასთან დაკავშირებული რისკების რაოდენობაც. ვებგვერდებზე, მობილურ აპლიკაციებსა და ონლაინ სერვისებით მოპოვებული თანხმობის კანონიერების საკითხი ერთ-ერთ აქტუალურ და პრობლემურ საკითხს წარმოადგენს.

მონაცემთა დაცვის ევროპული საბჭო (“EDPB”) თანხმობის შესახებ არსებულ რეკომენდაციაში განიხილავს ციფრულ გარემოსთან დაკავშირებულ სპეციფიკას და მასთან არსებულ რისკებს. კერძოდ, ონლაინ სივრცეებში მონაცემთა სუბიექტები ყოველდღიურად იღებენ თანხმობის მრავალ მოთხოვნას, რომლებიც გამოიხატება ღილაკების მონიშვნასა და ბმულის გადართვაში. აღნიშნული ქმედებების სიხშირე კი შესაძლოა განაპირობებდეს სუბიექტის დამოკიდებულებას, თანხმობის მექანიზმთან გადაჭარბებული ურთიერთობის შედეგად შემცირდეს მისი სიფრთხილე და ყურადღება.[33]

მიუხედავად იმისა, რომ ონლაინ სივრცეში მოპოვებული თანხმობის შემთხვევაშიც სავალდებულოა კანონით გათვალისწინებული კრიტერიუმებისა და მოთხოვნების დაცვა, პრაქტიკაში ხშირია შემთხვევები, როდესაც თანხმობის მოპოვების ფორმა მხოლოდ ფორმალობას წარმოადგენს. აღნიშნულ მავნე პრაქტიკას განსაკუთრებით ხშირად ვხვდებით ვებსაიტზე მზა-ჩანაწერების ე.წ. „cookie ფაილების“ საკითხის რეგულირებასთან დაკავშირებით. ვებსაიტზე შესვლისას ხშირად არის წარმოდგენილი არსებულ „cookie ფაილებზე“ ერთობლივი თანხმობის ფორმები, მაშინ, როდესაც მონაცემთა სუბიექტის უფლებაა გააკეთოს არჩევანი და დაეთანხმოს მისი მონაცემების დამუშავებას მხოლოდ იმ მზა ჩანაწერების ფარგლებში, რომლებიც მას სურს, ან რომლებიც წარმოადგენს ვებგვერდის ფუნქციონირებისა და უსაფრთხოებისთვის აუცილებელ ჩანაწერს და, შესაბამისად, მისი ფუნქციონირებაც სავალდებულო ხასიათის მატარებელია.

ამასთან, მნიშვნელოვანია, რომ: „თანხმობა მოპოვებულ იქნეს ვებსაიტზე შესვლისთანავე, სანამ ისინი მომხმარებლის მოწყობილობაზე განთავსდება, მაგალითად, “cookie” ბანერების მეშვეობით. მონაცემთა დამუშავების თითოეულ მიზანთან მიმართებით (რეკლამირების, ანალიტიკის და ა.შ.) თანხმობა განცალკევებული უნდა იყოს და სუბიექტმა ინდივიდუალურად უნდა განაცხადოს იგი.“[34]

საყურადღებოა, რომ თანხმობის კანონით განსაზღვრული კრიტერიუმები ონლაინ სივრცეშიც დიდ მნიშვნელობას იძენს, განსაკუთრებით კი გამჭვირვალობის და ინფორმირებულობის პრინციპი, რომლის შესაბამისადაც,

[33] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[34] პერსონალურ მონაცემთა დაცვის სამსახურის გზამკვლევი „ვებსაიტის შექმნის მსურველთათვის“ 27.

მონაცემთა სუბიექტისათვის მიწოდებული ინფორმაცია უნდა იყოს გასაგები, აღქმადი და კონკრეტული.

ონლაინ სივრცეებში წინასწარ გაკეთებულ მონიშვნებთან დაკავშირებით საინტერესო მსჯელობას ვხვდებით ევროკავშირის მართლმსაჯულების სასამართლოს ("CJEU") ერთ-ერთ გადაწყვეტილებაში (საქმეზე Planet49 GmbH (C-673/17, 2019 წლის 1 ოქტომბერი), რომელშიც აღნიშნულია, რომ მსგავს შემთხვევებში: „შეუძლებელია ობიექტურად დადგინდეს, ნამდვილად გასცა თუ არა მომხმარებელმა ვებსაიტზე თანხმობა საკუთარი პერსონალური მონაცემების დამუშავებაზე იმით, რომ არ მოხსნა მონიშვნა წინასწარ გაკეთებული მონიშვნიდან, ან საერთოდ - იყო თუ არა ეს თანხმობა ინფორმირებული. არ არის გამორიცხული, რომ მომხმარებელს არც წაეკითხა წინასწარ მონიშვნასთან დაკავშირებული ინფორმაცია, ან საერთოდ ვერ შეემჩნია ის და ისე გაეგრძელებინა ვებსაიტზე თავისი საქმიანობა."[35]

ონლაინ სივრცეში მიღებული თანხმობაც თავისთავად ექვემდებარება მოთხოვნას, მოპოვებულ იქნეს აქტიური ქმედებით (ღილაკზე დაჭერა, მონიშვნა და სხვ.), რაც, თავის მხრივ, გამორიცხავს ავტომატურად მონიშნული ფორმებით მოპოვებული თანხმობის სამართლებრივ ძალას.

3.5. თანხმობის გამოხმობის უფლება

თანხმობის ნებაყოფლობითი ხასიათის ერთ-ერთ გარანტიას ასევე წარმოადგენს მისი თავისუფალი გამოხმობის შესაძლებლობა და მის შესახებ მონაცემთა სუბიექტების ინფორმირება. აღნიშნულ შემთხვევაშიც მსგავსად მონაცემთა დამუშავების თაობაზე ინფორმაციის მიწოდების წინსწრებითი ხასიათისა, თანხმობის გამოხმობაზე ინფორმირებაც წინასწარ უნდა განხორციელდეს, მანამ, სანამ სუბიექტი განაცხადებს თანხმობას.

თანხმობის გამოხმობის საკითხის რეგულირებას „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი რამდენიმე ნორმაში ითვალისწინებს.

პირდაპირი მარკეტინგი - „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-12 მუხლი,[36] რომლითაც განსაზღვრულია თანხმობის გამოხმობის შესახებ ინფორმაციის მიწოდების ვალდებულებისა და აღნიშნული უფლების რეალიზების გარანტიების თაობაზე, კერძოდ, მისი უსასყიდლო და შეუზღუდავი გამოყენების ჭრილში.

მონაცემთა სუბიექტის უფლებების თავში - „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-20 მუხლი,[37] რომელშიც

[35] მართლმსაჯულების ევროპული სასამართლო (European Court of Justice), CJEU, Case C-673/17, Planet49 GmbH [2019], §55, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].

[36] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", №3144-XIმს-Xმპ, 14/06/2023, მუხლი 12 (3).

[37] იქვე, მუხლი 20.

დეტალურად არის განმარტებული აღნიშნულის რეალიზებისათვის საჭირო წინაპირობები:

- **დროში შეუზღუდავად, ნებისმიერ დროს** - აღნიშნული გამოირიცხავს დამუშავებისთვის პასუხისმგებელი პირის შესაძლებლობას, თუნდაც საკუთარი კონკრეტული მიზნის მითითებითა და ამ გზით დასაბუთებით, დააწესოს რაიმე ვადა თანხმობის გამოხმობისათვის;
- **განმარტებისა და დასაბუთების გარეშე** - კანონის მიზნებისა და მონაცემთა სუბიექტის ძირითადი უფლებების რეალიზების ქმედითი ღონისძიებების დასანერგად მნიშვნელოვანია, რომ გარანტირებული იყოს საკუთარი მონაცემების თავისუფლად განკარგვის შესაძლებლობა, მათ შორის – გაცემული თანხმობის განმარტებისა და დასაბუთების გარეშე მისი გამოთხოვის უფლება;
- **იმავე ფორმით გამოხმობის შესაძლებლობა, რომლითაც თანხმობა განაცხადა** - ნებაყოფლობითობისა და თავისუფლად ნების გამოვლენის კრიტერიუმი, რა თქმა უნდა, მოიაზრებს, რომ გამოირიცხოს დამუშავებისთვის პასუხისმგებელი პირის მხრიდან ზემოქმედების, ზეწოლის, ხელშეშლის, უფლების რეალიზებისთვის ხელოვნურად შექმნილი წინააღმდეგობების გათვალისწინება. რაც, თავის მხრივ, მოიაზრებს პასუხისმგებელი პირის ვალდებულებას, არ გაითვალისწინოს მხოლოდ კონკრეტულ შემთხვევებში, პირობებსა და ფორმით თანხმობის გამოხმობის შესაძლებლობა.

ამასთან, თანხმობის გამოხმობის კანონიერების შემოწმებისას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მტკიცების ტვირთია, დაადასტუროს, რომ მონაცემთა სუბიექტებისათვის აღნიშნული უფლების რეალიზება არ არის დაკავშირებული გარკვეულ ხარჯებთან და, შესაბამისად, არ არის აშკარა უარყოფითი შედეგების საფრთხე.[38]

აღნიშნული უფლების თავისუფლად და ნებისმიერ დროს რეალიზების შესაძლებლობის შეფასებისას ასევე ყურადღება უნდა მიექცეს კონკრეტული პროცესის თავისებურებებსაც. კერძოდ, თუ მონაცემთა სუბიექტს შესაძლოა შეეზღუდოს თანხმობის გამოხმობის უფლება იმ საფუძვლით, რომ მისი რეალიზებით დამუშავების შესაბამისი პროცესი დაზიანდება, მაგალითად, კვლევის შედეგებს შეექმნება საფრთხე, რეკომენდებულია, მსგავსი პროცესი არ იყოს დაფუძნებული თანხმობის სამართლებრივ საფუძველზე. ვინაიდან თანხმობის გამოხმობა ნებისმიერ დროს შეუზღუდავად უნდა იყოს შესაძლებელი.[39]

[38] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 13, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[39] *Information Commissioner's Office (ICO),* "What is Valid Consent?", <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].

3.6. თანხმობის გამოხმობა ონლაინ სივრცეში

ონლაინ სივრცეში, გარდა თანხმობის მოპოვებასთან დაკავშირებული საკითხებისა, მნიშვნელოვანია, გათვალისწინებული და პრაქტიკაში რეალიზებული იყოს მისი გამოხმობის შესაძლებლობა და უფლება.

მონაცემთა სუბიექტის აღნიშნული უფლების სრულყოფილი რეალიზებისათვის კი აუცილებელია ციფრული გარემო და მისი სპეციფიკა პრაქტიკაში შესაბამისი იყოს კანონის მოთხოვნებთან. ვებგვერდზე თანხმობის გამოხმობისათვის რთული და მრავალსაფეხურიანი გზების დასახვა პირდაპირ მიანიშნებს მონაცემთა დამუშავებაზე პასუხისმგებელი პირის არაკეთილსინდისიერ დამოკიდებულებასა და მონაცემთა სუბიექტის უფლებებისადმი არაჯეროვანი პატივისცემის საკითხებზე.

თანხმობა მხოლოდ ტექნიკური ფორმულარით ან ღილაკზე დაჭერით არ უნდა შემოიფარგლოს — ის უნდა იყოს რეალური ნების გამოხატულება, გამჭვირვალობისა და ინფორმირებულობის პრინციპსა და თავისუფალ არჩევანზე დაფუძნებული.

4. საერთაშორისო პრაქტიკა და გამოწვევები

მონაცემთა დამუშავების საფუძვლად თანხმობის განხილვის საკითხი, ისევე როგორც მისი კანონშესაბამისობა და მასთან დაკავშირებული უფლებების ქმედითობა, საერთაშორისო სამართლის ერთ-ერთ აქტუალურ საკითხს წარმოადგენს. პრაქტიკის ანალიზით ნათელია, რომ ნებაყოფლობითობის, ინფორმირებულობისა და გამჭვირვალობის პრინციპებს განსაკუთრებით დიდი მნიშვნელობა ენიჭება.

ამასთან, საერთაშორისო პრაქტიკის ანალიზი უზრუნველყოფს შესაძლებლობას, შეფასდეს ეროვნული კანონმდებლობის შესაბამისობა საერთაშორისო სტანდარტებთან, იდენტიფიცირდეს არსებული გამოწვევები და რისკები შედარებითი განხილვის საფუძველზე.

4.1. „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”)

საერთაშორისო პრაქტიკის დამკვიდრებაში მნიშვნელოვანი ადგილი უკავია ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციას“ (“General Data Protection Regulation – GDPR”),[40] რომელიც განსაზღვრავს მონაცემთა დამუშავების პრინციპებს, უფლებებსა და ვალდებულებებს, რომლებიც მიმართულია ფიზიკური პირების მონაცემების დაცვისკენ.

"GDPR” განსაკუთრებულ მნიშვნელობას ანიჭებს და ნათლად გამოყოფს თანხმობის შემდეგ სავალდებულო მახასიათებლებს:

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016

- ნათლად გამოხატული მოქმედება;
- ნებაყოფლობითობა;
- კონკრეტულობა;
- ინფორმირებულობა;
- მკაფიოობა.[41]

გარდა აღნიშნულისა, "GDPR" განსაზღვრავს მითითებას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მტკიცების ტვირთზე, შეძლოს მონაცემთა სუბიექტის მიერ დამუშავების პროცესზე გაცემული თანხმობის დემონსტრირება.[42] ასევე, ნათლად არის წარმოჩენილი საფრთხეები, როდესაც დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის აშკარა უთანასწორო ვითარებაა, განსაკუთრებით კი იმ შემთხვევაში, როდესაც დამუშავებისთვის პასუხისმგებელი პირი სახელმწიფო უწყებას წარმოადგენს.[43]

"GDPR"-ით გათვალისწინებული თანხმობის რეგულირების საკითხის ანალიზისას ცხადი ხდება მისი და საქართველოს კანონმდებლობის ერთმანეთთან შესაბამისობა და საკითხის მსგავსად რეგულირების პრაქტიკა. კერძოდ, განხილულ შემთხვევებში ვხვდებით რეგულირების ერთიან მიდგომას თანხმობის წერილობით დოკუმენტში გამოხატვის მიმართ, როდესაც დოკუმენტით ასევე სხვა საკითხებიც რეგულირდება. საკითხზე მსჯელობისას მკაფიოდ არის განსაზღვრული როგორც ეროვნული, ასევე საერთაშორისო კანონმდებლობის შესაბამისად, რომ თანხმობის ტექსტი/განცხადება გამორჩეულად/გამოყოფილად იყოს გათვალისწინებული სხვა საკითხებისგან, ნათლად და იოლად გასაგები ენით გადმოცემული.

ასევე პირდაპირი შესაბამისობაა საქართველოს ეროვნულ კანონმდებლობასა და "GDPR" ნორმებს შორის თანხმობის გამოთხოვის საკითხთან დაკავშირებითაც. ორივე განხილულ შემთხვევაში თანხმობის თავისუფლად, შეუზღუდავად გამოხმობის შესაძლებლობა, თავად თანხმობის სწორი ფორმულირების და მისი, როგორც სამართლებრივად გამართული საფუძვლის, რეალიზების წინაპირობად არის განხილული.[44]

საერთაშორისო პრაქტიკა, განსაკუთრებით "GDPR"-ის დებულებები, წარმოადგენს მნიშვნელოვან სტანდარტს, რომლის საფუძველზეც საქართველოს კანონმდებლობა და მასზე დაფუძნებული პრაქტიკა სახელმძღვანელო მითითებებს იღებს. საერთაშორისო რეგულაციები გვიჩვენებს, როგორ უნდა იყოს ფორმულირებული თანხმობის მოთხოვნის ტექსტი, რათა რეალიზებულ იქნეს ნებაყოფლობითობის, ინფორმირებულობისა და გამჭვირვალობის პრინციპები.

შესაბამისად, "GDPR" მონაცემთა დაცვის სფეროში, მათ შორის დამუშავების პროცესების კანონიერების განსაზღვრების ეტაპზე, არა მხოლოდ

[41] იქვე, Recital 32.
[42] იქვე, Article 7(1).
[43] GDPR, Recital 43.
[44] იქვე, Article 7(3).

საგანმანათლებლო და სახელმძღვანელო ინსტრუმენტს წარმოადგენს, არამედ მნიშვნელოვან სტანდარტადაც აღიქმება, რომელიც უზრუნველყოფს ეროვნული კანონმდებლობის განვითარებას ისევე, როგორც არსებული პრაქტიკისა და საზოგადოების სამართლებრივი ცნობიერების ამაღლებას.

5. დასკვნა

მონაცემთა დამუშავების საფუძვლად სუბიექტის თანხმობის გათვალისწინების საკითხის განხილვისას მასთან დაკავშირებული კანონისმიერი მოთხოვნებისა და კრიტერიუმების შეფასებისას ცხადი ხდება, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ დამუშავების პროცესისთვის, ერთი შეხედვით ყველაზე მარტივად მოსაძებნი და მისასადაგებელი საფუძველი, საკმარისად კომპლექსური და მრავლისმომცველია, ხოლო მასთან დაკავშირებული დამცველობითი ბერკეტები კი მნიშვნელოვნად გამორიცხავს თანხმობის მხოლოდ ფორმალურად არსებობის შესაძლებლობას.

თანხმობის ინსტიტუტის ეფექტიანად ფუნქციონირებისთვის გადამწყვეტია რამდენიმე ფაქტორის ერთობლიობა — გამჭვირვალობა, ინფორმირებულობა, ნებაყოფლობითობა და პასუხისმგებელი პირის კეთილსინდისიერება. აღნიშნული კრიტერიუმების ერთიანი სახით წარმოდგენის შემთხვევაში არის შესაძლებელი დავასკვნათ, რომ სუბიექტის თანხმობა რეალურად წარმოადგენს ნების თავისუფალ გამოვლინებას და არა მხოლოდ ფორმალობას.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანო (“ICO”) თანხმობის სამართლებრივ საფუძველთან დაკავშირებით ზოგად პრინციპს აყალიბებს, რომლის თანახმადაც, როდესაც რთულდება თანხმობის სტანდარტის შესრულება, სახეზეა ნიშანი, რომ ის არ წარმოადგენს შესაფერის საფუძველს მონაცემთა დამუშავებისათვის.[45]

თანამედროვე ციფრულ გარემოში, სადაც მონაცემთა დამუშავების მოცულობა და სიხშირე უპრეცედენტოა, განსაკუთრებული მნიშვნელობა ენიჭება თანხმობის გაცემისა და გამოხმობის პრაქტიკულ უზრუნველყოფას — სუბიექტს უნდა ჰქონდეს შესაძლებლობა, გააცნობიეროს, რაზე ეთანხმება და სურვილის არსებობისას გამოითხოვოს იგი უკან.

გრძელვადიან პერსპექტივაში მნიშვნელოვანია, რომ თანხმობის ინსტიტუტი არ იქცეს ფორმალურ მექანიზმად, არამედ იყოს რეალური გარანტი პირის ინფორმირებულობისა და არჩევნის თავისუფლებისათვის. სწორედ აღნიშნული მიდგომის დამკვიდრება უზრუნველყოფს მონაცემთა დაცვის კულტურის განვითარებას, კანონმდებლობის ეფექტიან გამოყენებას

[45] *Information Commissioner’s Office (ICO)* Guideline on *When is consent appropriate?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/

და საზოგადოების ნდობის განმტკიცებას როგორც საჯარო, ასევე კერძო სექტორის მიმართ.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14.06.2023.
2. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა სუბიექტისგან თანხმობის მიღების“ შესახებ, 10, 21.
3. პერსონალურ მონაცემთა დაცვის სამსახურის გზამკვლევი „ვებსაიტის შექმნის მსურველთათვის“, 27.
4. EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).
5. UK General Data Protection Regulation (UK GDPR), <https://www.legislation.gov.uk/ukpga/2018/12/contents> [27.11.2025].
6. *The Autoriteit Persoonsgegevens (AP),* Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].
7. *Cate, F. H.* The Failure of Fair Information Practice Principles In Consumer Protection in the Age of the Information Economy 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].
8. *CNIL (Commission nationale de l'informatique et des libertés),* Recommendation 5: Promote parental controls that respect the child's privacy and best interests, 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
9. *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021, 29. <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].
10. *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018, 7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].
11. *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 10, 13, 19. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

12. *Information Commissioner's Office (ICO)* Guideline on What is valid consent? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].
13. *Information Commissioner's Office (ICO)* Guideline on What is consent appropriate? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].
14. *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 3, 15, 20, 40. <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
15. მართლმსაჯულების ევროპული სასამართლო (European Court of Justice), CJEU, Case C-673/17, Planet49 GmbH [2019], §55 <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].