New Vision University - ნიუ ვიჟენ უნივერისტეტი

სალომე ბაზუაშვილი

პერსონალური მონაცემების დაცვა ინტერეტ სივრცეში

შედარებითი კერძო და საერთაშორისო სამართლის სამაგისტრო პროგრამა

სამაგისტრო ნაშრომი შესრულებულია სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი : ლიკა საჯაია

ასოც.პროფესორი, სამართლის დოქტორი

2021 წელი

ანოტაცია

ციფრული ტექნოლოგიების განვითარების კვალდაკვალ, ინტერნეტის გამოყენება დღითიდღე სულ უფრო და უფრო აქტუალური ხდება. 21-ე საუკუნე სწორედ ინტერნეტის და ტექნოლოგიების საუკუნედ მოიაზრება. ინტერნეტი სასიცოცხლო და მამოძრავებელი ძალა გახდა საზოგადოების, სწორედ ამიტომ უნდა გვახსოვდეს, რომ თითოეული ჩვენს მიერ განხორციელებული მოქმედება ინტერნეტ სივრცეში ტოვებს გარკვეულ კვალს და სადღაც ფიქსირდება. ყოველდღიურად უფრო და უფრო მნიშვნელოვანი გამოწვევა ხდება ადამიანების და მათი ქცევის შესახებ მონაცემების შეგროვება და დამუშავება.

მსოფლიო საზოგადოება ყოველღიურად ახორციელებს ინტერნეტში კომუნიკაციას, ისინი იხდიან გადასახადებს, აწარმოებენ აღრიცხვებს, ეს აქტივობები კი თავისთავად პერსონალური მონაცემების გაზიარებას მოითხოვს. სწორედ ინტერნეტის განვითარება და ტექნოლოგიური პროგრესია ერთ-ერთი მთავარი მიზეზი, რამაც წარმოშვა საჭიროება პერსონალური მონაცემების დაცვისა. პერსონალური მონაცემების დაცვამ კი უამრავი პრობლემა წარმოშვა და საჭირო გახდა მისი სამართლებრივ ჩარჩოებში მოქცევა და რეგულირება.

წინამდებარე ნაშრომი მიმოიხილავს პერსონალური მონაცემების დაცვის თანამედროვე გამოწვევებსა და პრობლემებს, ასევე, გაგაცნობთ ამ საკითხთან დაკავშირებულ პრეცედენტულ საქმეებსა და სასამართლო გადაწყვეტილებებს.

ასევე, კვლევა მიმოიხილავს ევროკავშირის პრაქტიკას პერსონალური მონაცემების დაცვასთან დაკავშირებით, მის რეგულაციებს,კერძოდ : „ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია“ (GDPR) და კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, ევროკავშირის მისწრაფებას უკეთ დაიცვას ადამიანების პერსონალური ინფორმაცია ინტერნეტ სივრცეში.

ნაშრომის მიზანია შეისწავლოს სხვა ქვეყნებში არსებული მდგომარეობა პერსონალური მონაცემების დაცვის კუთხით და პარალელი გავავლოთ საქართველოსთან და შევაფასოთ შესაძლებელი იქნება თუ არა მსგავსი მიდგომების განხორციელება საქართველოში, შევისწავლოთ პრობლემები და მკითხველს დავანახოთ თუ რა საფრთხეები შეიძლება მოჰყვეს მათ მიერ განხორციელებულ ქმედებებს ინტერნეტში.

წინამდებარე ნაშრომი არის ჩემ მიერ დამოუკიდებლად შესრულებული. ნაშრომის ის ნაწილზე, რომელიც არ წარმოადგენს ჩემს პირად ნააზრევს/დასკვნებს, აკადემიური წერის სტანდარტების გათვალისწინებით, მითითებულია შესაბამისი სქოლიოები. აღნიშნული დეტალები ნაშრომს ხდის პლაგიარიზმისგან თავისუფალს.

Protection of Personal Date in Internet space

Annotation

In the wake of the development of digital technologies, the use of the Internet is becoming more and more relevant. The 21st century is considered to be the century of the Internet and technologies. The Internet has become a vital and driving force for society. That is why we must remember that each our actions in the internet space leavses a certain trace and is recorded somewhere. Collecting and processing data on people and their behavior is becoming more and more important challenge every day.

The world society communicates on the Internet every day, they pay taxes, keep records, etc. All these activities in themselves require the sharing of personal data. The development of the Internet and the technological progress are one of the reasons that led to the need to protect personal data. As for the protection of personal data, it has created many problems and, consequently, it became necessary to bring it into the legal framework and regulate it.

The present thesis reviews the current/contemporary challenges and problems of personal data protection, harewith, introduces the precedent cases and court decisions related to this issue.

The present research also reviews the EU's practices regarding the protection of personal data and its regulations, namely: the EU General Data Protection Regulation (GDPR) and the Convention on the Proteciton of Individuals with Regard to Automatic Processing of Personal Data and the EU aspiration to better protect people's personal information on the Internet, as well.

The aim of the present thesis is to study the situation in other contries in terms of personal data protection, draw a parallel with Georgia and assess whether it will be possible to

implement similar approaches in Georgia, also to explore the problems and show the readers what kind of dangers may result from their actions on the Internet.

The present work is independently performed by me. The part of the paper that is not my personal opinion / conclusion, according to the standards of academic writing, has the relevant footnotes. These details make the paper free from plagiarism.

სარჩევი

1.შესავალი

ჩვენ ვცხოვრობთ ისეთ სამყაროში, სადაც თითოეული ადამიანი ყოველი ნაბიჯის გადადგმაზე საკუთარი პერსონალური მონაცემების კვალს ტოვებს. პერსონალური მონაცემების მოუწესრიგებელი და უკონტროლო დამუშავებიდან გამომდინარე საფრთხეების მნიშვნელობა მკვეთრად სცდება ადამიანებისთვის მიყენებულ ფსიქოლოგიურ ტრამვას და დისკომფორტს, რასაც პირადი მონაცემების გამჟღავნება იწვევს.

მონაცემების არაკანონიერი და უკონტროლო დამუშავება ადამიანის უფლებების შეზღუდვის რისკებს შეიცავს,რაც თავის მხრივ საფრთხეს უქმნის თანამედროვე სამართლიანი და დემოკრატიული სახელმწიფოს არსებობას.

ტექნოლოგიური პროგრესის პირობებში ყოველწლიურად უმჯობესდება ინტერნეტი, იქმნება ახალი მოწყობილობები და ამ ყველაფერს მოაქვს ახალი შესაძლებლობები. სწორედ ამიტომ დემოკრატიულ სახელმწიფოში პერსონალური მონაცემების დაცვას ერთ-ერთი მთავარი ადგილი უჭირავს ადამიანის უფლებების დაცვის სფეროში.

პერსონალურ მონაცემთა დაცვას, როგორც ადამიანის ერთ-ერთ ფუნდამენტურ უფლებას დღესდღეობით უდიდესი მნიშვნელობა ენიჭება, შესაბამისად დემოკრატიული სახელმწიფოები მუშაობენ ახლებურ მიდგომებსა და ახალ სამართლებრივ თავდაცვით მექანიზმებზე, თანამედროვე სამყაროში არსებულ გამოწვევებთან გასამკლავებლად. თუმცა, უკვე აღარ არის საკმარისი ამ პრობლებების მხოლოდ საკანონმდებლო დონეზე რეგულირება, სახელმწიფოები უფრო კომპლექსური რეგულაციების შექმნაზე არიან ორიენტირებულნი და მაქსიმალურად ცდილობენ საკუთარი მოსახლეობის ინტერესების და უფლებების დაცვას.

ინტერნეტის ეპოქაში ყოველი ჩვენგანი ყოველდღიურად უამრავ საძიებო სისტემას, აპლიკაციას, ონლაინ მომსახურებას თუ სოციალურ ქსელს იყენებს. როგორც

ვიცით, ინტერნეტ მომსახურების ნაწილი ფასიანია ნაწილი კი უფასო, თუმცა ალბათ არავის უფიქრია,რომ უფასო ინტერნეტ მომსახურებაშიც კი „ვიხდით“ ჩვენს პერსონალურ მონაცემებს.

დღესდღეობით ნებისმიერი საქმიანობის განხორციელება ინტერნეტზეა დამოკიდებული. მთელს მსოფლიოში ნებისმიერ ადამიანს,კერძო კომპანიას თუ საჯარო დაწესებულებას აქვს ლეგიტიმური მოლოდინი, რომ მათ მიერ ინტერნეტ სივრცეში განცორციელებული ქმედებები იქნება სანდო და დაცული ყოველგვარი არამართლზომიერი ჩარევისგან.

ტექნოლოგიების და კიბერ სივრცის განვითარებასთან ერთად სულ უფრო რთული ხდება პერსონალური მონაცემების კონტროლი. სწორედ ამიტომ თანამედროვე მსოფლიოს გამოწვევა გახდა პერსონალური მონაცემების დაცვა, რათა მილიონობით ადამიანის პირადი ინფორმაცია რომელიც ინტერნეტ სივრცეშია გაფანტული იყოს დაცული და ადამიანებს ჰქონდეთ რეალური შესაძლებლობა, რომ თავი იგრძნონ უსაფრთხოდ ნებისმიერი მოქმედების შესრულებისას.

პერსონალური მონაცემების დაცვა ძალიან სწრაფადგანვითარებადი სამართის დარგია.რადგან ტექნოლოგიური პროგრესის და ინტერნეტის ერაში ვცხოვრობთ, რომელიც ყოველრიურად განიცდის ცვლილებებს ამიტომ საჭიროა ფეხი აუწყოს სამართალმა ინტერნეტის განვითარებას და შესაბამისმა კანონმდებლობამ უზრუნველყოს პერსონალური მონაცემების დაცვა.

პერსონალური მონაცემების დაცვის საკითხი საქართველოშიც საკმაოდ აქტუალურია. ჩვენი მოქალაქეები ყოვედღიურად აწყდებიან პრობლემებს პერსონალური მონაცემების დაცვის კუთხით. საქართველოში კი ამ პრობლემების გადაჭრაზე საუბარი 90-იანი წლების მიწურულს დაიწყო, როდესაც სახელმწიფომ დაიწყო საკუთარი კანონმდებლობის შექმნა, თუმცა,პერსონალური მონაცემების დაცვა საქართველოს კონცენტრაციის მთავარ ობიექტად მხოლოდ 2011 წელს, კერძოდ 28 დეკემბერს, იქცა როდესაც საერთაშორისო ვალდებულების შესრულების მიზნით საქართველოს პარლამენტმა მიიღო კანონი : „პერსონალურ

მონაცემთა დაცვის შესახებ „. სპეციალური კანონის მიღებამდე პერსონალური მონაცემების დაცვა საქართველოში „ზოგადი ადმინისტრაციული კოდექსით“ ხდებოდა, თუმცა ევროკავშირისკენ სწრაფვის და განვითარების სურვილმა ამ პრობლემის ცალკე საკანონმდებლო აქტით მოწესრიგება განაპირობა.
„პერსონალური მონაცემების დაცვის შესახებ“ კანონმა პირველად დაამკვიდრა პერონალურ მონაცემთა დაცვის ინსპექტორის ინსტიტუტი, რომელიც 2013 წლიდან მოქმედებს აქტიურად. აღსანიშავია,რომ კანონში „პერსონალური მონაცემების დაცვის შესახებ“ ნაკლებადაა მოხსენიებული ინტერნეტ სივრცეში გავრცელებული მონაცემების დაცვის მექანიზმები და პასუხისმგებლობის ადრესატები,რაც ბუნდოვნებას ტოვებს საქართველოს კანონმდებლობაში.

აღსანიშნავია ასოცირების შეთანხმება,რომელიც 2014 წელს საქართველოსა და ევროკავშირს შორის დაიდო და იგი ძალიან მნიშვნელოვანი დოკუმენტია ჩვენი ქვეყნისთვის. ასოცირების შეთანხმება არის საქართველოს ევროკავშირთან დაახლოების სამოქმედო გეგმა და მოიცავს თითქმის ყველა სფეროს, მათ შორის სამართლებრივ საკითხებს, კერძოდ,პერსონალურ მონაცემების დაცვას. ასოცირების შეთანხმების 14-ე მუხლი ითვალისწინებს რომ საქართველოსთვის სავალდებულოა ჩვენი კანონმდებლობა შევუსაბამოთ ევროკავშირის კანონმდებლობას.[1]

წინამდებარე კვლევის მთავარი მიზანია გამოიკვლიოს რეალური გზები და საშუალებები თუ როგორ შეიძლება დაიხვეწოს და განვითარდეს საქართველოს კანონმდებლობა და მიებაძოს უცხოურ სახელმწიფოებს, რომლებსაც ბევრად მაღალი სტანდარტები აქვთ პერსონალური მონაცემების დაცვის კუთხით,ასევე, ნაშრომის მიზანია განვითარებული ქვეყნების პრაქტიკის და მაგალითების შესწავლა თუ როგორ არეგულირებს პერსონალური მონაცემების დაცვას

[1] ასოცირების შესახებ შეთანხმება ერთის მხრივ, საქართველოსა და მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის, 2014 წ; ბოლო გადამოწმების თარიღი: [09.09.2020]

ევროკავშირი. კვლევა ემყარება შედარებით-საართლებრივ მეთოდს და სასამართლო პრაქტიკის ანალიზს.

ნაშრომში განხილულია ევროკავშირის სპეციალური რეგულაცია : „ევროკავშირის მონაცემთა დაცვის რეგულაცია“ (GDPR). განვიხილავთ ამ რეგულაციას და ვნახავთ თუ რა განსხვავებაა ევროკავშირის და საქართველოს კანონმდებლობას შორის პერსონალური მონაცემების დაცვის კუთხით და ვიმსჯელებთ შესაძლებელი და გამართლებული იქნება თუ არა საქართველოშიც მსგავსი მოქმედებების განხორციელება.

უნდა აღვნიშნოთ, რომ ეს სფერო ახალი გამოწვევაა საქართველოსთვის, შესაბამისად მწირია ქართული ლიტერატურა აღნიღნულ თემასთან დაკავშირებით, სწორედ ამიტომ სამაგისტრო ნაშრომში მიმოვიხილავთ უცხოურ ლიტერატურას და უცხოური პრაქტიკით ვიხელმძღვანელებთ.

2. რას მოიცავს პერსონალური მონაცემები

კვლევის დასაწყებად თავდაპირველად აუცილებელია გავიგოთ თუ რას წარმოადგენს პირის პერსონალური მონაცემები,რატომ არის მისი კონფიდენციალურობის დაცვა მნიშვნელოვანი და რატომ და რა ხერხებით ზრუნავენ სახელმწიფოები თავიანთი მოქალაქეების პერსონალური მონაცემების დაცვას,ასევე, რატომაა საჭირო პერსონალური მონაცემების უსაფრთხოება მნიშვნელოვანი და როგორ დაიწყეს ქვეყნებმა მასზე ზრუნვა. სანამ უშუალოდ პრობლემებს განვიხილავთ ინტერნეტ სივრცესთან დაკავშირებით,მანამდე მნიშვნელოვანია იმის გააზრება თუ რას წარმოადგენს პირის პერსონალური მონაცემები და როგორი მნიშვნელოვანია მისი კონფიდენციალურობის დაცვა.

კონცეფცია "მონაცემთა დაცვა" შემუშავდა თითქმის ოთხი ათეული წლის წინ,რათა მოეხდინა პირების სამართლებრივი დაცვა მათთან დაკავშირებული ინფორმაციის არამართლზომიერი გამოყენებისგან. კონცეფციის შექმნის მიზანი არ ყოფილა პერსონალური მონაცემების დამუშავების აკრძალვა ან საინფორმაციო ტექნოლოგიების გამოყენების შეზღუდვა, არამედ მისი მიზანი იყო უცილებელი თავდაცვითი მექანიზმების შქმნა პერსონალური მონაცემების დამუშავების პროცესში. [2]

ევროკავშირის კანონმდებლობა „პერსონალურ მონაცემებს“ განმარტავს,როგორც ინფორმაციას, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (‘მონაცემთა სუბიექტს’)[3]. იმისათვის, რომ განისაზღვროს შესაძლებელია თუ არა ფიზიკური პირის იდენტიფიცირება, მხედველობაში უნდა იქნეს მიღებული ყველა გონივრული შესაძლო საშუალება, მაგალითად, ფიზიკური პირის ამოცნობა, რაც შესაძლოა გამოყენებული იქნეს მონაცემთა დამმუშავებლის ან სხვა პირის მიერ პირის პირდაპირ ან არაპირდაპირ იდენტიფიცირების მიზნით. იმის დასადგენად, მოხდება თუ არა გონივრული საშუალებების გამოყენება ფიზიკური პირების იდენტიფიცირების მიზნით, მხედველობაში უნდა იქნეს მიღებული ყველა ობიექტური ფაქტორი, როგორიცაა იდენტიფიცირებისათვის საჭირო ხარჯები და დრო, მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიები და ტექნოლოგიის განვითარება. [4]

პერონალური მონაცემები არის ერთობლიობა ინფორმაციებისა რომლის საშუალებითაც პირის იდენტიფიცირება ხდება. საქართველოს კანონი

[2] "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" Peter Hustinx* ბოლო გადამოწმების თარიღი: [09.09.2020]

[3] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (1)

[4] იქვე, პრეამბულა, პუნქტი 26.

„პერსონალური მონაცემების დაცვის შესახებ“ თითქმის მსგავსად განმარტავს პერსონალური მონაცემების არსს. კანონში წერია : „პერსონალური მონაცემი (შემდგომ – მონაცემი) – ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით“[5]

უფრო მარტივი ენით რომ ვთქვათ პერსონალური მონაცემები ესაა პირის მაიდენტიფიცირებადი ნებისმიერი სახის ინფორმაცია, როგორიცაა : სახელი, გვარი, პირადი ან ტელეფონის ნომერი, საბანკო ანგარიშის ნომერი, ფოტოსურათი, ვიდეოჩანაწერი, ელექტრონული ფოსტის მისამართი, დაბადების თარიღი, მისამართი, პირადი მიმოწერა და სხვა.

დღესდღეობით პერსონალური მონაცემის ცნება გააფართოვა ინტერნეტის განვითარებამ.ინტერნეტ სივრცეში ადამიანები ყოველდღიურად ზედმეტი დაკვირვების გარეშე ავსებენ სხვადასხვა აპლიკაციებსა თუ გვერდებზე საკუთარ პერსონალურ მონაცემებს, საიტებს აძლევენ უფლებას შეინახოს მათი პირადი მონაცემები ისე რომ არც არკვირდებიან საიტის წესებსა და პოლიტიკას. ალბათ ყველას გვქონია შემთხვევა როდესაც „Facebook”- ი არდადეგებზე გაცნობილი ადამიანის დამეგობრებას გვთავაზობს, ან ახალი სამსახური მოშორებით გადავიდა და ტაქსის რეკლამა ხშირად გვხვდება ჩვენს გვერდზე, ან მეგობრის დაბადების დღე მოდის და გვხვდება ზუსტად იმ საათის რეკლამა, რომელიც მეგობარს მოსწონს. ყველაფერი ეს,ჩვენს მიერ ჩვენივე ინფორმაციის გაზიარების შედეგი შეიძლება იყოს. თითოეული აპლიკაცია თუ საძიებო სისტემა ისეა აწყობილი, რომ კარგად იმახსოვრებს ნებისმიერ საძიებო სისტემაში შეყვანილ ტექსტს, ინახავს ლოკაციას და ნანახ საიტებს.

[5] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

ადამიანის პერსონალური მონაცემები კი დღესდღეობით ძალიან დიდი „იარაღია“ და არასწორ ადგილას მოხვედრის შემთხვევაში შეიძლება ძალიან დიდი ზიანი გამოიწვიოს. ამიტომა მნიშვნელოვანია იმის გარკვევა, თუ როგორ ცდილობს სახელმწიფო დაიცვას საკუთარი მოქალაქეების ინტერესები ინტერნეტ სივრცეში.

2.1 პერსონალური მონაცემების განსაკუთრებული კატეგორიები

როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, არსებობს პერსონალური მონაცემების განსაკუთრებული კატეგორიები, რომლებიც, თავიანთი ხასიათიდან გამომდინარე, დამუშავებისას შეიძლება დიდ რისკებს შეიცავდეს მონაცემთა სუბიექტებისათვის. სწორედ ამიტომ, ისინი საჭიროებენ გაძლიერებულ დაცვას. აღსანიშავია, რომ განსაკუთრებული კატეგორიის მონაცემებზე ვრცელდება აკრძალვის პრინციპი და მათი დამუშავება კანონის თანახმად ნებადართულია მხოლოდ შეზღუდული რაოდენობით. [6]

108-ე მოდერნიზებული კონვენციის (მუხლი 6) და GDPR-ის (მუხლი 9) ფარგლებში, სენსიტიურ მონაცემებად მიიჩნევა პერსონალური მონაცემები:

- რასისა და ეთნიკური წარმომავლობის შესახებ;
- პოლიტიკური, რელიგიური ან სხვა შეხედულებების შესახებ ;
- პროფესიული კავშირის წევრობის შესახებ;
- გენეტიკური და ბიომეტრიული მახასიათებლების შესახებ, რომელთა დამუშავებაც ხდება პროვნების იდენტიფიცირების მიზნით;

[6] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

- პიროვნების ჯანმრთელობის მდგომარეობის, სქესობრივი ცხოვრების ან სექსუალური ორიენტაციის შესახებ.[7]

როდესაც საქმე განსაკუთრებული კატეგორიის მონაცემების დამუშავებას ეხება,მათი დაცვის განსაკუთრებით მაღალი სტანდარტებია დაწესებული და შესაბამისაც მათი დარღვევის შემთხვევაში სანქციაც უფრო დიდია, სწორედ ეს განასხვავებს განსაკუთრებულ და ჩვეულებრივ პერსონალურ მონაცემებს,ასევე, მათი დამუშავებისთვის კანონიც განსხვავებულ საფძვლებს ადგენს და მაღალ სტანდარტს აწესებს.

მაგალითი: მართლმსაჯულების ევროპული კავშირის სასამართლოს „Bodil Lindqvist“-ის საქმე შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე ადამიანების იდენტიფიცირებას სახელით ან სხვა საშუალებებით, როგორიცაა ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა: „მითითება იმ ფაქტზე, რომ პიროვნებამ დაიზიანა ფეხი და ნახევარ განაკვეთზე მუშაობს სამედიცინო მიზეზების გამო, პერსონალური მონაცემია ჯანმრთელობის შესახებ.“ [8]. მოცემული გადაწყვეტილებით სასამართლმ, ყურადღება გაამახვილა ცნება „დამუშავების“ საკანონმდებლო ფარგლებსა და მისი ინტერპრეტაციის გზებზე.

[7] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data-CETS 108-Article 6.
Art. 9 GDPR – Processing of special categories of personal data

[8] CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 2003 წლის 6 ნოემბერი, პუნქტი 51. ბოლო გადამოწმების თარიღი: [09.09.2020]

„პერსონალური მონაცემების შესახებ“ კანონი განგვიმარტავს თუ რა არის განსაკუთრებული კატეგორიის პერსონალური მონაცემები : „მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში გაწევრებასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან, აგრეთვე ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა;[9]

ბიომეტრიული მონაცემი არის ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება, მაგალითად : თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი, სახის მახასიათებელი[10].

ბიომეტრიული მონაცემების უნიკალური და მუდმივი ხასიათიდან გამომდინარე აუცილებელია მონაცემთა დამმუშავებლის მხრიდან სიღრმისეული გაანალიზება იმ პრინციპებისა და მოთხოვნებისა,რომლებიც საერთაშორიო თუ ქვეყნის შიდა კანონმდებლობით არის დადგენილი. პრაქტიკაში ბიომეტრიულ მონაცემებს დიდი დატვირთვა აქვს ძირითადად საიდუმლო ინფორმაციის დაცვის, ინფორმაციული სისტემების უსაფრთხოებისთვის, სახელმწიფო საზღვრების კონტროლისა და პასპორტების დამზადებისთვის გამოიყენება.

[9] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ბ“ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

[10] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „გ“ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

ბიომეტრიული მონაცემების დამუშავების კანონიერება და პროპორციულობა წარმოადგენს სწორედ საქართველოს კანონის : „პერსონალური მონაცემების შესახებ“ რეგულირების სფეროს. აღნიშნული კანონი ამომწურავად განსაზღვრავს ბიომეტრიული მონაცემების მიზნებს, კანონიერს საფუძვლებს, პრინციპებს, სუბიექტის უფლებებსა და პერსონალური მონაცემების დაცვის ინსპექტორისადმი ინფორმაციის მიწოდების ვალდებულებას.

გასათვალისწინებელია ის გარემოებაც, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, ბიომეტრიული მონაცემი განსაკუთრებული კატეგორიის მონაცემს წარმოადგენს მხოლოდ მაშინ, როდესაც ის იძლევა ფიზიკური პირის იდენტიფიცირების საშუალებას განსაკუთრებული კატეგორიის მონაცემის ნიშნით, როგორიცაა რასობრივი ან ეთნიკური კუთვნილება, ჯანმრთელობის მდგომარეობა, ნასამართლობა და სხვა. შესაბამისად მათი დამუშავების დროს აუცილებელია კანონის მე-6 მუხლით გათვალისწინებული ერთ-ერთი საფუძვლის არსებობა მაინც - მაგალითად მონაცემთა სუბიექტის წერილობითი თანხმობა. [11]

რაც შეეხება გენეტიკურ მონაცემებს იგი ინფორმაციას იძლევა –მონაცემთა სუბიექტის უნიკალური და მუდმივი მონაცემი გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება.[12] გენეტიკური მონაცემების კატეგორიას მიეკუთვნება ღეროვანი უჯრედი, რომლის გამოყენებაც დღესდღეობით სამედიცინო მიზნების გარდა პირის იდენტიფიცირების საშუალებას იძლევა.

[11] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „გ “ ქვეპუნქტი N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.
“პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

[12] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „გ1 “ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

2.2 ანონიმირებული და ფსევდონიმირებული მონაცემები

მონაცემთა დაცვის ზოგადი რეგულაცია და მოდერნიზებული 108-ე კონვენცია მოიცავს პერსონალურ მონაცემთა შენახვის პრინციპს. ამ პრინციპის თანახმად, მონაცემები „შენახული უნდა იყოს ისეთი ფორმით, რომ მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას იძლეოდეს მხოლოდ მათი დამუშავების მიზნებისთვის აუცილებელ დროში.“ [13] შესაბამისად, თუ დამმუშავებელს მონაცემების შენახვა სურს იმ ვადის გასვლის შემდეგაც, რაც საჭირო იყო თავდაპირველი მიზნის მისაღწევად, მონაცემები უნდა იქნეს ანონიმირებული.

2.2.1 ანონიმირებული მონაცემები

ანონიმირებულია მონაცემი, როდესაც იგი აღარ შეიცავს რაიმე იდენტიფიკატორს, რომლის საშუალებითაც ხდებოდა მონაცემის სუბიექტის იდენტიფიცირება. მონაცემთა ანონიმიზაციისათვის, ინფორმაციაში არ უნდა დარჩეს არცერთი ელემენტი, რომელიც, გონივრული ძალისხმევის შედეგად, შესაბამისი პირის ხელახალი იდენტიფიცირების შესაძლებლობას იძლევა.[14]

როდესაც მონაცემი წარმატებით იქნება ანონიმიზებული იგი პერსონალურ მონაცემად აღარ ჩაითვლება და შესაბამისად მასზე პერსონალურ მონაცემთა დაცვის კანონმდებლობა აღარ გავრცელდება.

[13] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ე); 108-ე მოდერნიზებული კონვენცია, მუხლი 5(ე)

[14] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 26.

2.2.2 ფსევდონიმირებული მონაცემები

ფსევდონიმირებულია მონაცემი, როდესაც მონაცემის სუბიექტის იდენტიფიკატორები არის დაშიფრული. პერსონალური მონაცემები მოიცავს :სახელს, გვარს, პირად ნომერს, დაბადების თარიღს და სხვა ელემენტებს. ფსევდონიმიზაციის პროცესი გულისხმობს ზუსტად ამ მახასიათებლების დაშიფრვას და ფსევდონიმით ჩანაცვლებას.

ევროკავშირის სამართალში ფსევდონიმიზაცია ნიშნავს „პერსონალური მონაცემების იმგვარ დამუშავებას, როდესაც, დამატებითი ინფორმაციის გამოყენების გარეშე, შეუძლებელია მათი დაკავშირება კონკრეტულ მონაცემთა სუბიექტთან, იმ პირობით, რომ ეს დამატებითი ინფორმაცია შენახულია ცალკე, და მონაცემები, ტექნიკური და ორგანიზაციული ზომების მეშვეობით, არ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.“[15]

ანონიმიზებული მონაცემებისაგან განსხვავებით, ფსევდონიმიზებული ინფორმაცია კვლავ პერსონალური მონაცემია ანუ მასზე ვრცელდება მონაცემთა დაცვის კანონმდებლობა.
ფსევდონიმიზაცია პირდაპირ არ არის მოხსენიებული მოდერნიზებულ 108-ე კონვენციაში, თუმცა, კონვენციის განმარტებითი ბარათი მკაფიოდ აცხადებს, რომ „ფსევდონიმის ან ნებისმიერი სხვა სახის ციფრული იდენტიფიკატორის/ციფრული იდენტობის გამოყენება არ იწვევს მონაცემთა ანონიმიზაციას, ვინაიდან მონაცემთა სუბიექტი შეიძლება კვლავ იდენტიფიცირებადი ან ინდივიდუალიზებული იყოს.“[16]

მონაცემთა ფსევდონიმიზაციის ერთ-ერთი საშუალებაა მათი დაშიფვრა.

[15] მონაცემთა დაცვის ზოგადი რეგულაცია,მუხლი 4 (5).
[16] 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი, პუნქტი 18.

პერსონალური მონაცემები ხშირად გამოიყენება დაშიფრული იდენთიფიკატორებით, როდესაც პიროვნების ვინაობა უნდა იქნებს საიდუმლოდ შენახული. ფსევდონიმიზაციის პროცესი განსხვავდება ანონიმიზაციისგან იმითაც,რომ ანონიმიზაციის პროცესში პირის იდენტიფიცირებისათვის საჭირო ნებისმიერ ინფორმაციასთან კავშირი გაწყვეტილია.

ფსევდონიმიზაციის მაგალითია : წინადადება - „გიორგი გიორგაძე, დაბადებული 1957 წლის 31 აგვისტოს არის ხუთი შვილის, ორი გოგოს და სამი ბიჭის მამა“ - შეიძლება შემდეგნაირად იყოს ფსევდონიმიზებული:
„გ.გ. 1957 არის ხუთი შვილის, ორი გოგოს და სამი ბიჭის მამა“; ან
„923 არის ხუთი შვილის, ორი გოგოს და სამი ბიჭის მამა“; ან
„YESn2342 არის ოთხი შვილის, ორი გოგოს და ორი ბიჭის მამა.“

ადამიანი, რომელსაც ფსევდონიმიზებულ მონაცემებზე ექნება წვდომა, ვერ შეძლებს „გიორგი გიორგაძე, დაბადებული 1957 წლის 31 აგვისტოს დაუკავშიროს 923-ს ან YESn2342-ს. შესაბამისად, ფსევდომინიზებული მონაცემები დაცულია ბოროტად გამოყენებისგან და ძლიერი იარაღია ინფორმაციის დაცვის თვალსაზრისით.

2.3 Big Data- დიდი მონაცემები

ტერმინის,,დიდი მონაცემების” სიახლის მიუხედავად, მისი კონცეფცია არც ისე ცოტა ხანია რაც არსებობს.კომპანიები ამ ტერმინის გამოჩენამდეც კარგად ხვდებოდნენ მონაცემთა ანალიზის არსს და მათი შეგროვებით მიღებული სარგებლის „გემოს“, თუმცა, ამ სფეროს ახალი სარგებელი მონაცემების უსწრაფესად და ეფექტურად დამუშავებაა. თუკი ათეული წლების წინ კომპანიები

ჯერ ინფორმაციას აგროვებდნენ, შემდეგ აანალიზებდნენ და ასე იღებდნენ გადაწყვეტილებებს ახლა „Big Data" ტექნოლოგიის დახმარებით შეუძლიათ ეს პროცესი სწრაფი გახადონ და გადაწყვეტილებაც დაუყოვნებლივ მიიღონ.

დიდი მონაცემების ანალიზი იძლევა ფართო მასშტაბის შესაძლებლობებს. ერთი შეხედვით, რატომ უნდა იყოს საინტერესო ადამიანის ტელეფონში ან კომპიუტერში „Google Maps"-აპლიკაციის და ადგილმდებარეობის სერვისის (GPS) ერთობლივი მუშაობით დადებული სტატისტიკა, მაგალითად: 5 წლის წინ „A" 50 -ჯერ იმყოფებოდა ერთ ქალაქში და 100-ჯერ სხვა ქალაქში ან იმავე პერიოდში, „The Rolling Stones"- ის 20 სიმღერას მოუსმინა, „The Beatles" -ის კი - მხოლოდ 12-ს. უნდა აღვნიშნოთ, რომ ციფრული ტექნოლოგიების მომხმარებლისთვის შეიძლება სულაც არიყოს საინტერესო ბოლო 5 წელიწადში კონკრეტულმა ადამიანმა რომელ ფილმს უყურა, ან სოციალურ ქსელებში რა აქტივობებით გამოირჩეოდა, რა „დაალაიქა" ყველაზე ხშირად. აღნიშული ინფორმაციები არსად იკარგება, ისინი ილექება საინფორმაციო ბაზებში და რიგითი მომხმარებლისთვის თუ არა, ბიზნესისთვის იგი ნამდვილი „განძია" და მისი სწრაფად დამუშავება კომპანიის საქმეს ბევრი მიმართულებით წასწევს წინ კონკურენტულ ბაზარზე.
სწორედ ასე, შეიქმნა „დიდი მონაცემების" (BigData) კონცეფცია, რომელიც სხვადასხვა წყაროებიდან დაგროვილი მონაცემების კონსოლიდაციას და მიღებული შედეგების ბიზნეს ანალიზის ამოცანებისთვის გამოყენებას გულისხმობს.

ინტერნეტის ეპოქაში თითოეული ჩვენგანი უამრავ აპლიკაციას, ონლაინ მომსახურებასა თუ საძიებო სისტემა იყენებს, რაშიც ფულის გადახდა არ გვჭირდება, თუმცა ნაკლებად თუ ვფიქრობთ იმას,რომ ამ მომსახურებაში ფულის მაგივრად ჩვენს პერსონალურ მონაცემებს „ვიხდით" და ნებისმიერი განხორციელებული ქმედება ტოვებს ციფრულ კვალს, რომლის შეგროვება, დამუშავება და ანალიზი შესაძლებელია.ჩვენი ნებით ვაძლევთ კომპანიებს წვდომას ჩვენს პერსონალურ მონაცემებზე, რომლებიც ჩვენს ციფრულ პორტრეტს

ქმნის. სწორედ ეს მილიარდობით მონაცემი ქმნის ინფორმაციის იმ უზარმაზარ ერთობლიობას, რომელსაც „Big Data“-ს უწოდებენ. სწორედ ამიტომ არაა გასაკვირი, თუ ბოლო პერიოდში საძიებო სისტემაში მოძებნილი ნივთები რეკლამების სახით ბუმერანგივით უკან გვიბრუნდება რეკლამების სახით. დიდი მონაცემების პოტენციალი იმდენად მასშტაბურია, რომ მისი საშუალებით ადამიანზე ნებისმიერი სახის ზემოქმედება შეიძლება და ეს პოტენციალი ინტერნეტის და ტექნოლოგიების განვითარებასთან ერთად იზრდება. სწორედ ამიტომ ითვლება დიდი მონაცემები ერთ-ერთ დიდ გამოწვევად პერსონალური მონაცემების დაცვის კუთხით.

3. პერსონალურ მონაცემთა გამოქვეყნება სუბიექტის მიერ

ტექტონოგიური განვითარების და ინტერნეტის ეპოქაში მონაცემთა დამუშავება ფართოდ არის გავრცელებული, ხოლო ადამიანებისთვის კი სულ უფრო და უფრო რთულდება მისი მნიშვნელობის გააზრება და იმ შედეგების გათვლა, რაც პერსონალური მონაცემების გამჟღავნებას შეიძლება მოჰყვეს. სუბიექტის მიერ პერსონალური მონაცემების გამოქვეყნება პირთა განუსაზღვრელი წრისადმი გულისხმობს ამ პეროსნალური მონაცემების გასაჯაროებას. ხშირ შემთხვევაში პიროვნება სრულიად გაუაზრებლად აკეთებს ამას. მაგალითად როდესაც ინტერნეტში,სოციალურ ქსელში, ქმნის ანგარიშს და შეჰყავს საკუთარი პერსონალური მონაცემები, ან ეთანხმება საიტის პირობებსა და წესებს მათი გაცნობის გარეშე და ამით ავტომატურად აქვეყნებს საკუთარ მონაცემებს. სწორედ ამიტომ,ყოველთვის წინასწარ უნდა იქნეს ის შედეგები განსაზღვრული, რაც საკუთარი პერსონალური მონაცემების გამოქვეყნებას შეიძლება მოჰყვეს.

3.1 თანხმობა ინტერნეტში მონაცემების გასაჯაროებაზე

ევროკავშირის კანონმდებლობა აკეთებს მითითებას რამდენიმე ელემენტზე,რომელთა საფუძველზეც თანხმობა არის დასაბუთებული, რაც მიზნად ისახავს იმის დადასტურებას, რომ მონაცემთა სუბიექტს ნამდვილად სურდა თავისი მონაცემების გარკვეული სახით გამოყენება. თანხმობა დასაბუთებული/მოქმედია: [17]

- თანხმობა უნდა იყოს მკაფიოდ და გასაგებად გამოხატული და დგინდებოდეს მონაცემთა სუბიექტის ნებაყოფლობითი, კონკრეტული და ინფორმირებული სურვილი მის მონაცემების დამუშავების შესახებ.
- მონაცემთა სუბიექტი უფლებამოსილია, ნებისმიერ დროს გამოითხოვოს თანხმობა, თანხმობის გათხოვა არ ახდენს გავლენას მის გათხოვამდე, მონაცემთა სუბიექტის თანხმობის საფუძველზე განხორციელებული დამუშავების კანონიერებაზე.
- წერილობითი განცხადების კონტექსტში, თანხმობაზე მოთხოვნა უნდა იყოს მკაფიო, მარტივი ენით დაწერილი, გასაგები, მარტივად აღქმადი და ადვილად ხელმისაწვდომი, თანხმობა კი ნათლად იყოს გამოყოფილი სხვა საკითხებისგან; თუ ეს განაცხადი არღვევს GDPR-ს, მას არ ექნება შესასრულებლად სავალდებულო ძალა.

მონაცემთა დაცვის კანონმდებლობის კონტექსტში, თანხმობა მოქმედია მხოლოდ მაშინ, თუ შესრულდება ყველა ზემოაღნიშნული მოთხოვნა. მონაცემთა დამმუშავებლის პასუხისმგებლობაში შედის იმის დადასტურება, რომ მონაცემთა სუბიექტმა გამოხატა თანხმობა მისი მონაცემების დამუშავებაზე.[18]

[17] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 7

[18] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 7(1)

თანხმობა არის პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი, და იგი აუცილებლად უნდა იყოს ნებაყოფლობითი, ინფორმირებული და კონკრეტული, მკაფიოდ გამოხატავდეს დამუშავებაზე თანხმობის სურვილს. „პერსონალური მონაცემების შესახებ“ საქართველოს კანონის 2 მუხლის „ზ“ ქვეპუნქტი განმარტავს თუ რა არის თანხმობა : "თანხმობა – მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე ზეპირად, და ტელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით გამოხატული ნებაყოფლობითი თანხმობა, რომლითაც შესაძლებელია ნათლად დადგინდეს მონაცემთა სუბიექტის ნება [19]. მოცემული მუხლის ფარგლებში „სხვა შესაბამის საშუალებად“ შეიძლება მივიჩნიოთ ნებისმიერი რამ, რაც შესაძლოა პირის თანხმობად მივიჩნიოთ. ეს შესაძლებელია იყოს ნაგულისხმევი თანხმობა ინფორმაციის გასაჯაროებაზე. ნაგულისხმევი თანხმობის ერთ-ერთ მაგალითად შეგვიძლია მოვიყვანოთ ნებისმიერ სოციალურ ქსელში არსებულ ჯგუფში გაწევრიანების შემთხვევა. მაგალითად ჯგუფი განკუთვნილია კონკრეტული უნივერსიტეტის სამართლის მაგისტრებისთვის და მისი ადმინისტრატორიც მხოლოდ იმ პირებს ამატებს ჯგუფში,ვინც ფლობს კონკრეტული უნივერსიტეტის სამართლის მაგისტრის დამადასტურებელ ხარისხს. ასეთ შემთხვევაში პირის მიერ ინფორმაციის, მისი პერსონალური მონაცემების გასაჯაროება ხდება საკუთარი ნების გამოვლენისა და ადმინისტრატორის მიერ ჯგუფში დამატებით. ამ ქმედების შედეგად პირის პერსონალური მონაცემები საჯაროვდება მხოლოდ პირთა განსაზღვრული წრისთვის და ადამიანს წარმოეშობა გონივრული მოლოდინი,რომ მის მიერ გასაჯაროებული ინფორმაცია დარჩება საიდუმლოდ.

[19] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 2, „ზ“ ქვეპუნქტი

3.2 მონაცემთა სუბიექტის მოთხოვნა დაბლოკვაზე, წაშლასა და განადგურებაზე.

ტექნოლოგიური პროგრესის და ინტერნეტის ეპოქაში,სადაც მონაცემთა სუბიექტები ყოველდღიურად საკუთარ პერსონალურ მონაცემებს დაკვირვებით თუ დაკვირვების გარეშე ამჯღავნებენ ინტერნენტში სჭირდებათ დაცვის მექანიზმები,რათა მეტად შეძლონ თავიანთი პერსონალური მონაცემების დამუშავების კონტროლი. სწორედ ამიტომ მონაცემთა სუბიექტებს ენიჭებათ გარკვეული უფლებები.

საკუთარ მონაცემებზე წვდომისა და მათი შესწორების უფლებები დაცულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლის მეორე პუნქტით [20]. ასევე „პერსონალური მონაცემების შესახებ“ საქართველოს კანონის 21 და 22 მუხლებით.

მონაცემთა სუბიექტებს უნდა ჰქონდეთ შემდეგი უფლებები:

- შეეძლოთ საკუთარ პერსონალურ მონაცემებზე ჰქონდეთ წვდომა და მიიღონ კონკრეტული ინფორმაცია მონაცემების დამუშავების შესახებ; [21]
- მოითხოვონ თავიანთი მონაცემების შესწორება მონაცემთა დამმუშავებლის მიერ, თუკი ისინი არაზუსტია;
- მონაცემთა დამმუშავებელს მოსთხოვონ თავიანთი მონაცემების წაშლა, თუ იგი ამ მონაცემებს უკანონოდ ამუშავებს;
- მოითხოვონ დამუშავების დროებით დაბლოკვა;
- მოითხოვონ პერსონალური მონაცემების განადგურება; [22]

განვიხილოთ მონაცემთა სუბიექტის უფლებები მონაცემების დაბლოკვასა, წაშლასა და განადგურებასთან მიმართებით. მონაცემთა დაბლოკვის უფლება

[20] ქარტია ევროპის კავშირის ფუნდამენტური უფლებების შესახებ,8-ე მუხლი.ბოლო გადამოწმების თარიღი: [09.09.2020]

[21] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 21-ე მუხლის 1 ნაწილი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

[22] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 22-ემუხლის 1 ნაწილი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011.

რეალიზებულია ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციია 18 მუხლში, მის თანახმად, მონაცემთა სუბიექტს აქვს უფლება დამმუშავებლისაგან მოითხოვოს მონაცემთა დაბლოკვა თუ სახეზეა ერთ-ერთი შემდეგი გარემოება:

- სადავოდ მიაჩნიათ მონაცემთა სიზუსტე;
- მონაცემთა დამუშავება უკანონოა და, წაშლის ნაცვლად მონაცემთა სუბიექტი ითხოვს მათ დაბლოკვას;
- მონაცემები აღარ არის საჭირო მათი დამუშავების მიზნის მისაღწევად, თუმცა მონაცემთა სუბიექტს მონაცემები ესაჭიროება სამართლებრივი მოთხოვნის შესასრულებლად ან დასაცავად;
- განიხილება საკითხი თუ რამდენად აღემატება მონაცემთა დამმუშავებლის კანონიერი ინტერესები მონაცემთა სუბიექტის ინტერესებს, გადაწყვეტილება ამის შესახებ კი,ჯერ არ მიღებულა.[23]

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის 17-ე მუხლი კი ეხება მონაცემთა წაშლის უფლებას („დავიწყების უფლება“, რომელზეც მოგვიანებით,შემდეგ თავში გვექნება დეტალურად საუბარი), რომლის მიხედვითაც მონაცემების სუბიექტს უფლება აქსვ დაუყოვნებლივ მოითხოვოს მის შესახებ არსებული ინფორმაციის წაშლა და ორგანიზაცია ვალდებულია წაშალოს მონაცემები, თუ, მაგალითად :

- მონაცემები უკვე აღარაა საჭირო იმ მიზნის მისაღწევად, რისთვისაც მოხდა მათი შეგროვება ან დამუშავება;
- დამუშავება განხორციელდება არაკანონიერად;
- პირი გაითხოვს თანხმობას, რომლის საფუძველზეც მუშავდებოდა მონაცემები.[24]

[23] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 18
[24] მონაცემთა დაცვის ზოგადი რეგულაცია,მუხლი 17

აქ აუცილებლად აღსანიშნია, რომ საქართველოს პარლამენტში ინიცირებულია კანონპროექტი, რომელიც წაშლის/დავიწყების უფლებას GDPR-ს მსგავსად აწესრიგებს, თუმცა მისი მიღება სამწუხაროდ ჯერ არ მომხდარა და იმედია სულ მალე ვიხილავთ ჩვენს კანონმდებლობაშიც „დავიწყების“ უფლებას.[25]

სპრაქტიკაში ხშირადაა შემთხვევები, როდესაც სუბიექტი პერსონალურ მონაცემთა დაბლოკვას, წაშლას და განადგურებას ითხოვს. მაგალითად შეგვიძლია მოვიყვანოთ შემთხვევა, როდესაც სუბიექტმა (ვთქვათ, საქართველოს მოქალაქემ, საქართველოდან) წაშალა „Google-ის“ საკუთარი ანგარიში,რომელიც ალბათ ყველა ადამიანს გააჩნია ვინც იყენებს ამ გიგანტ საძიებო სისტემას, მიმართა „Google-ს“ ადმინისტრაციას, რათა წაეშალა მისი მონაცემები რომელიც შენახულია „Google-ის“ მიერვე. შემდგომ ვთქვათ, „Google „-სგან მას მოუვიდეს დადებითი პასუხი (რომ წაშლილია მისი მონაცემები), რამდენად სარწმუნოდ შეიძლება ჩაითვალოს იგი? რადგანაც გადამოწმების ბერკეტი არ არსებობს, პერსონალური მონაცემების დაცვის სრულყოფილი გარანტია სამართლებრივ დონეზე არ არის განმტკიცებული. მართალია, მოწესრიგებული არის ვალდებულების ნაწილი და ამ ვალდებულებითი ნაწილით ქართული რეალობის გათვალისწინებით, ზედამხედველობის უფლებამოსილება გააჩნია სახელმწიფო ინსპექტორს, მაგრამ პრაქტიკული თვალსაზრისით მისი აღსრულებადობა სირთულეებს წარმოშობს. შესაბამისად კარგი იქნება არსებობდეს გადამოწმების სასუალება, და ამ შემთხვევაში პირის უფლება და ინტერესი რომ წაიშალოს საკუთარი მონაცემები სრულყოფილად იქნებოდა რეალიზებული.

პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა სუბიექტს ანიჭებს ფართო უფლებებს, რომელთა რეალიზებისათვისაც გარკვეული ვალდებულებები მონაცემების დამმუშავებელ ორგანიზაციებს ეკისრებათ. ასეთ

[25] კანონპროექტი : „პერსონალურ მონაცემთა დაცვის შესახებ“.2019წ.ბოლო გადამოწმების თარიღი: [09.09.2020]

ვალდებულებებს ხშირ შემთხვევებში წარმოშობს მონაცემთა სუბიექტის მოთხოვნები, ხოლო ზოგიერთ შემთხვევაში კი კანონი. მონაცემთა დამუშავების ნებისმიერი სახე არის პირდაპირ კავშირში სუბიექტის უფლებებთან. მონაცემთა დაცვის მაღალი სტანდარტები უზრუნველყოფს მონაცემის სუბიექტის უფლებების ეფექტურ დაცვას, ხოლო არაკანონიერად მონაცემების დამუშავება, პირიქით, ლახავს მონაცემის სუბიექტის პირადი ცხოვრების ხელშეუხებლობის უფლებას.

"პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 22-ე მუხლში რეალიზებულია მონაცემთა სუბიექტის მიერ მონაცემთა გასწორების, განახლების, დამატების, დაბლოკვის, წაშლისა და განადგურების მოთხოვნის უფლება, მისი მიხედვით : „მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში მონაცემთა დამმუშავებელი ვალდებულია გაასწოროს, განაახლოს, დაამატოს, დაბლოკოს, წაშალოს ან გაანადგუროს მონაცემები, თუ ისინი არასრულია, არაზუსტია, არ არის განახლებული ან თუ მათი შეგროვება და დამუშავება განხორციელდა კანონის საწინააღმდეგოდ."[26], ასევე, „მონაცემთა დამმუშავებელმა მონაცემთა ყველა მიმღებს უნდა აცნობოს მონაცემთა გასწორების, განახლების, დამატების, დაბლოკვის, წაშლის ან განადგურების შესახებ, გარდა იმ შემთხვევისა, როდესაც ასეთი ინფორმაციის მიწოდება შეუძლებელია მონაცემთა მიმღებების სიმრავლისა და არაპროპორციულად დიდი ხარჯების გამო. ამ უკანასკნელი გარემოების შესახებ უნდა ეცნობოს სახელმწიფო ინსპექტორის სამსახურს"[27].

საინტერესოა სახელმწიფო ინსპექტორის სამსახურის მიერ მომზადებული 2020 წლის საქმიანობის ანგარიში, რომელშიც ნათლად ჩანს,თუ როგორ ირღვევა მონაცემების სუბიექტის უფლებები. მონაცემთა სუბიექტის უფლებათა რეალიზების უზრუნველსაყოფად, სახელმწიფო ინსპექტორის სამსახურმა,

[26] "პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 22-ე მუხლის 1 ნაწილი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011
[27] "პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 22-ე მუხლის 2 ნაწილი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

მოქალაქეთა განცხადების/შეტყობინების საფუძველზე, შეისწავლა მონაცემთა დამუშავების 36 პროცესი, სამსახურის მიერ შესწავლილი საქმეების საფუძველზე, ადმინისტრაციული პასუხისმგებლობა დაეკისრა 12 პირს სამართალდარღვევისთვის. სანქციის სახით 5 პირის მიმართ გამოყენებულია გაფრთხილება, ხოლო 7 პირის მიმართ - ჯარიმა. საჯარო და კერძო დაწესებულებებში მონაცემთა სუბიექტის უფლებების დაცვისათვის, ადმინისტრაციული სახდელების პარალელურად, სამსახურმა გასცა შესასრულებლად სავალდებულო 14 დავალება და 1 რეკომენდაცია. სახელმწიფო ინსპექტორის სამსახურმა მონაცემთა სუბიექტის უფლებათა რეალიზების პროცესები შეისწავლა საგანმანათლებლო დაწესებულებებში, სააფთიაქო ქსელებში, საფინანსო ორგანიზაციებში. [28]

მონაცემთა სუბიექტების უფლებათა სავარაუდო დარღვევის შესახებ შესწავლილმა პროცესებმა გამოავლინა შემდეგი ნაკლოვანებები:

- კერძო და საჯარო დაწესებულებები მონაცემთა სუბიექტს არ აწვდიან ინფორმაციას, რა მიზნითა და რომელი სამართლებრივი საფუძვლით მუშავდება მათი პერსონალური მონაცემები და ვის გადაეცემა ისინი, რაც მონაცემთა სუბიექტისთვის მონაცემების დამუშავების პროცესს გაუმჭვირვალეს და არაგანჭვრეტადს ხდის;
- გამოვლინდა არაერთი შემთხვევა, როდესაც ორგანიზაციები ჯეროვნად არ აღრიცხავდნენ, რა გზითა და საშუალებით მოიპოვეს პერსონალური მონაცემები. ასევე ვერ აწვდიდნენ შესაბამის ინფორმაციას მონაცემთა სუბიექტს დაინტერესების შემთხვევაში. შესაბამისად, მონაცემთა სუბიექტი ვერ ადგენს საიდან გახდა ორგანიზაციისთვის ხელმისაწვდომი მისი მონაცემები, რაც აჩენს ეჭვს მათი შეგროვების არაკანონიერებასთან დაკავშირებით;

[28] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში 2020 წ..ბოლო გადამოწმების თარიღი: [09.09.2020]

- რიგ შემთხვევებში, როცა არ დაკმაყოფილდა მონაცემთა სუბიექტის მოთხოვნა პერსონალური მონაცემების განახლებაზე, მას არ მიეწოდა ინფორმაცია უარის თქმის საფუძვლებზე;
- რიგ შემთხვევებში, არ დაკმაყოფილდა მონაცემთა სუბიექტის მოთხოვნა, რომ დაწესებულებას განემარტა მის შესახებ დაცული პერსონალური მონაცემების შენახვის საფუძველი;
- ხშირად კერძო და საჯარო დაწესებულებები უსაფუძვლოდ ეუბნებოდნენ უარს მონაცემთა სუბიექტს მისი პერსონალური მონაცემების შემცველი დოკუმენტების ასლების გაცემაზე ან არაგონივრულად აჭიანურებდნენ მათ გადაცემას. ეს ზღუდავს პირის უფლებას, ჰქონდეს ინფორმაცია მის შესახებ მონაცემების დამუშავებაზე და, საჭიროების შემთხვევაში, სადავო გახადოს მისი კანონიერება.[29]

ამ ხარვეზებთან დაკავშირებით სახელმწიფო ინსპექტორის დაცვის სამსახურმა გასცა შემდეგი რეკომენდაციები : მონაცემთა სუბიექტების უფლებათა დაცვისათვის არსებითად მნიშვნელოვანია ორგანიზაციებში მონაცემთა დაცვის მაღალი სტანდარტის დამკვიდრება. სახელმწიფო ინსპექტორის სამსახური მიესალმება სხვადასხვა საჯარო და კერძო დაწესებულებაში მონაცემთა დაცვის ოფიცრის თანამდებობის შემოღებას. ამგვარი ინსტიტუტის დანერგვა მიუთითებს ორგანიზაციის სურვილზე, სათანადოდ დაიცვას მასთან არსებული მონაცემები და, შესაბამისად, მონაცემთა სუბიექტების უფლებები. მონაცემთა სუბიექტის უფლებათა რეალიზებისთვის საჭიროა, მონაცემთა დამმუშავებელმა ორგანიზაციებმა:

- შეიმუშაონ და მონაცემთა სუბიექტებისათვის ხელმისაწვდომი გახადონ დოკუმენტები, სადაც დეტალურად იქნება აღწერილი მონაცემთა დამუშავების პროცესები, მათ შორის, რა მონაცემები გროვდება, რა მიზნით და რა ვადით ინახება;

[29] იქვე

- დანერგონ მონაცემთა დამუშავების ისეთი პროცესი, რომელიც იძლევა მონაცემთა სუბიექტის უფლებათა რეალიზების ქმედით შესაძლებლობას;
- აღრიცხონ, რა გზით, რა მიზნითა და რომელი სამართლებრივი საფუძვლით მოიპოვეს პერსონალური მონაცემები;
- მონაცემთა სუბიექტს კანონმდებლობით გათვალისწინებული ინფორმაცია მიაწოდონ გასაგები ფორმით, თუკი კანონმდებლობა მათ ამ ვალდებულებისაგან არ ათავისუფლებს;
- მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, გაასწორონ, განაახლონ და, საჭიროების შემთხვევაში, წაშალონ კანონსაწინააღმდეგოდ შეგროვებული მონაცემები, ხოლო უარის თქმისას - ნათლად და მკაფიოდ განუმარტონ მას უარის საფუძველი;
- დროულად უპასუხონ მონაცემთა სუბიექტის მოთხოვნას, რადგან გაჭიანურების შემთხვევაში ხშირად აზრი ეკარგება მონაცემთა სუბიექტის უფლების რეალიზებას. რეაგირების გაჭიანურების ან უარის თქმისას, აცნობონ მას შეფერხების მიზეზი/უარის საფუძველი;
- იზრუნონ მონაცემთა დამუშავების პროცესში ჩართული პირების ცნობიერების ამაღლებაზე. [30]

ნათელია, რომ აღნიშნული ხარვეზები ქმნის მონაცემების კანონის დარღვევით დამუშავების საფრთხეებს და არაკნონიერი დამუშავების კონკრეტული შემთხვევევბი ჩნდება სახეზე. ამის საპასუხოდ აუცილებელია სახელმწიფო ინსოექტორის სამსახურის მუშაობასთან ერთად კონკრეტული ნაბიჯები გადაიდგას მონაცემთა დაცვის მდგომარეობის გასაუმჯობესებლად როგორც კერძო, ასევე, საჯარო დაწესებულებების მხრიდან.

[30] იქვე

4. ევროკავშირის რეგულაციები პრაქტიკა და პრობლემები პერსონალურ მონაცემების დაცვასთან დაკავშირებით.

„1960-იან წლებში ინფორმაციული ტექნოლოგიების გამოჩენასთან ერთად, გაჩნდა მზარდი მოთხოვნა პერსონალურ მონაცემთა დაცვის დეტალურ წესებზე. 70-იან წლების შუა პერიოდისათვის, ევროპის საბჭოს მინისტრთა კომიტეტმა არაერთი რეზოლუცია მიიღო პერსონალურ მონაცემთა დაცვის შესახებ, რომლებიც ევროპული კონვენციის მე-8 მუხლზე მიუთითებდა. 1981 წელს ხელმოსაწერად გაიხსნა კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია). ეს დოკუმენტი იყო და რჩება სავალდებულო იურიდიული ძალის მქონე ერთადერთ საერთაშორისო ინსტრუმენტად მონაცემთა დაცვის სფეროში. კონვენცია ვრცელდება ყველა სახის მონაცემთა დამუშავებაზე - როგორც კერძო, ისე საჯარო სექტორის, მათ შორის, მართლმსაჯულებისა და სამართალდამცველი ორგანოების მიერ. იგი ადამიანის უფლებებს იცავს პესონალურ მონაცემთა დამუშავებასთან დაკავშირებული დარღვევებისგან და, ამავდროულად, მიზნად ისახავს მათი საერთაშორისო გადაცემის რეგულირებას... კონვენცია, გარდა იმისა, რომ უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების გარანტიებისა და უსაფრთხოების ვალდებულებებს, კრძალავს განსაკუთრებული კატეგორიის მონაცემთა (როგორიცაა: პიროვნების რასობრივი კუთვნილება, პოლიტიკური შეხედულებები, ჯანმრთელობის მდგომარეობა, რელიგია, სქესობრივი ცხოვრება და ნასამართლობა) დამუშავებას დაცვის სათანადო სამართლებრივი მექანიზმის გარეშე. ასევე, იგი იცავს ფიზიკური პირის უფლებას, იცოდეს, თუ რა ინფორმაცია ინახება მასზე და, საჭიროების შემთხვევაში, მოითხოვოს მისი შესწორება.“[31]

[31] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო,2018 წ..ბოლო გადამოწმების თარიღი: [09.09.2020]

სწორედ 108-ე კონვენციის შექმნა აღიბეჭდა შემდგომში ევროკავშირის მიერ 2000 წელს მიღებული ქარტიის „ევროპული კავშირის ფუნდამენტური უფლებების“ მე-7 და მე-8 მუხლებში.[32]

„ქარტია მოიცავს ევროპელ მოქალაქეთა სამოქალაქო, პოლიტიკური, ეკონომიკური და სოციალური უფლებების სრულ სპექტრს და ეყრდნობა წევრ სახელმწიფოთა კონსტიტუციურ ტრადიციებსა და ერთიან საერთაშორისო ვალდებულებებს. ამ დოკუმენტით დაცული უფლებები იყოფა 6 კატეგორიად: ღირსება, თავისუფლებები, თანასწორობა, სოლიდარობა, მოქალაქეთა უფლებები და სამართლიანობა...ქარტია იცავს არა მხოლოდ პირადი და ოჯახური ცხოვრების (მუხლი 7), არამედ პერსონალურ მონაცემთა დაცვის უფლებასაც (მუხლი 8)...ქარტიის მე-8 მუხლი, რომელიც მონაცემთა დაცვის დირექტივის შექმნიდან რამდენიმე წელიწადში ჩამოყალიბდა, მოიცავს მანამდე არსებულ ევროკავშირის კანონმდებლობას მონაცემთა დაცვის შესახებ. შესაბამისად, ქარტია მკაფიოდ მიუთითებს არა მხოლოდ მონაცემთა დაცვის უფლებაზე (მუხლი 8(1)), არამედ, მათი დაცვის ძირითად პრინციპებზეც (მუხლი 8(2)); „[33]

90-იანი წლების დასაწყისიდან შეიცვალა სამუშაო გარემო,რადგან განვითარება დაიწყო ინფორმაციულმა ტექნოლოგიებმა,დაიწყეს ინტერნეტის გამოყენება და საჭირო გახდა ახალი რეგულაციები, შსაბამისად, 1981 წლის 108-ე კონვენცია გამოუსადეგარი ხდებოდა არსებულ სიტუაციასთან მიმართებით. სწორედ ამიტომ,1995 წელს საბჭომ შეიმუშავა ახალი დირექტივა : „ინდივიდების დაცვა

[32] ქარტია ევროპის კავშირის ფუნდამენტური უფლებების შესახებ, (მიღებულია 2000 წლის 2 ოქტომბერს, ძალაში შევიდა 2000 წლის 7 დეკემბერს)..ბოლო გადამოწმების თარიღი: [09.09.2020]

[33] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო,2018 წ..ბოლო გადამოწმების თარიღი: [09.09.2020]

პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით“ (დირექტივა მონაცემთა დაცვის შესახებ)[34].

აღნიშნული დირექტივის შექმნა ევროკავშირისთვის იყო პირველი მცდელობა პერსონალური მონაცემების ზოგადი წესების შესაქმნელად, რათა დაეცვა საკუთარი მოქალაქეების უფლებები პერსონალურ მონაცემებთან მიმართებით. თუმცა, უნდა აღინიშნოს, რომ დირექტივის შექმნის დროს ინტერნეტ სივრცე ჯერ კიდევ არიყო საკმარისად განვითარებული და პერსონალური მონაცემების განმარტებაც საკმაოდ შეზღუდული იყო. 1990-იანი წლების შუა პერიოდში დირექტივის შემუშავების შედგომ, მნიშვნელოვნი ცვლილებები მოხდა ინტერნეტ სივრცეში, იმ დროინდელი ინტერნეტ სივრცის შესაძლებლობები დღევანდელ რეალობასთან ახლოსაც კი არ იყო.სწორედ ამ წინაპირობებმა წარმოშვა ევროკავშირის მონაცემთა დაცვის კანონმდებლობის რეფორმის საჭიროება. ეს რეფორმა საბოლოოდ 2016 წელს აპრილში დამთავრდა მონაცემთა დაცვის ზოგადი რეგულაციის მიღებით.

„2016 წელს, მონაცემთა დაცვის ზოგადი რეგულაციის მიხედვით, მოხდა ევროკავშირის შესაბამისი კანონმდებლობის მოდერნიზება. შედეგად, კანონმდებლობას მიენიჭა ფუნდამენტურ უფლებათა დაცვის შესაძლებლობა ციფრული ეპოქის ეკონომიკური და სოციალური გამოწვევების კონტექსტში. GDPR ითვალისწინებს და ავითარებს მონაცემთა სუბიექტის ძირითად უფლებებსა და პრინციპებს, რაც მოცემულია მონაცემთა დაცვის დირექტივაში. ამასთან, იგი ადგენს ახალ ვალდებულებებს, რომელთა თანახმადაც ორგანიზაციებმა უნდა დანერგონ მონაცემთა დაცვის სტანდარტები ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა განსაზღვრონ პირველად პარამეტრად (by default); გარკვეულ შემთხვევებში მათ უნდა დანიშნონ მონაცემთა დაცვის

[34] საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით [1995].ბოლო გადამოწმების თარიღი: [09.09.2020]

ოფიცერი, შეასრულონ მონაცემთა პორტირების ახალი უფლების მოთხოვნები და დაემორჩილონ ანგარიშვალდებულების პრინციპს. ევროკავშირის კანონმდებლობის თანახმად, რეგულაციები ვრცელდება პირდაპირ და ეროვნულ კანონმდებლობაში გადატანას არ საჭიროებს. ამრიგად, მონაცემთა დაცვის ზოგადი რეგულაცია ქმნის მონაცემთა დაცვის ერთიანი წესების კრებულს, რომელიც ევროკავშირის მასშტაბით მოქმედებს. შედეგად, ევროკავშირში ჩამოყალიბდა მონაცემთა დაცვის ერთიანი წესები და სამართლებრივად განჭვრეტადი გარემო, რაც მოქმედებს ეკონომიკური ოპერატორებისა და ფიზიკურ პირების, როგორც „მონაცემთა სუბიექტების“ სასარგებლოდ“[35]

დირექტივამ მონაცემთა დაცვის შესახებ (GDPR) მოგვცა ე.წ. „დავიწყების უფლება“, რაც ძალიან მნიშვნელოვანი შენაძენია, აუცილებელია განვმარტოდ თუ, რას წარმოადგენს დავიწყების უფლება, რატომ არის მისი არსებობა დღევანდელ საყაროში მნიშვნელოვანი და ასევე პრობლემატური. და რა იყო ის ახალი რეგულაციის ამოქმედებამდე.

4.1 დავიწყების უფლება -(Right to be forgotten)

ტექნოლოგიური პროგრესის კვალდაკვალ, პირადი მონაცემების დამუშავება გარკვეული ოპერაციების შესასრულებლად და ინფორმაციაზე წვდომის ერთ-ერთ გზად განიხილება. პერსონალური მონაცემების გასაჯაროება უკვე ჩვეულებრივ მოვლენად ითვლება. ასეთ რეალობაში ცხოვრებისას, ალბათ, სამართლიანი იქნებოდა რომ ყოველ ადამიანს გააჩნდეს იმის უფლება, რომ თავად განსაზღვროს თუ რა დოზით უნდა ჰქონდეს წვდომა მის პერსონალურ მონაცემებზე სამყაროს. შესაბამისად, ჰქონდეს უფლება საჭიროებისამებრ დაბლოკოს ან წაშალოს იგი.

[35] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო,2018 წ..ბოლო გადამოწმების თარიღი: [09.09.2020]

ასეთი რეგულირების საკითხი ცალკეულ სახელმწიფოებში დიდი ხნის განმავლობაში იდგა. "დავიწყების უფლება" საერთაშორისო სამართლებრივად საბოლოოდ განმტკიცდა 2014 წლის 13 მაისს, როდესაც მართლმსაჯულების ევროპულმა სასამართლომ აღნიშნა, რომ "დავიწყების უფლება" არის ადამიანის ერთ-ერთი მნიშვნელოვანი უფლება, რომლის გამოც შესაძლოა, შეიზღუდოს ინფორმაციის თავისუფლებს პასიური ასპექტი - ინფორმაციის მიღების უფლება. სასამართლომ კოსტეჯას საქმეზე Google- ის საწინააღმდეო გადაწყვეტილება მიიღო. [36]

Google Spain vs AEPD (Spanish Data Protection Agency) and Mario Costeja Gonsalez

1998 წელს ესპანურმა გაზეთმა გამოქვეყნა ორი განცხადება,რომელიც უძრავი ქონების ძალით გაყიდვას ეხებოდა სოციალური ვალების გამო.
ერთ-ერთი ადამიანი, მოვალე, რომლის სახელიც გამოჩნდა ამ ორ განცხადებებში იყო მოპასუხე მარიო გონზალესი. იგი 2009 წელს დაუკავშირდა გაზეთს და მოითხოვა ამ მონაცემის წაშლა, მისი აზრით ეს ინფორმაცია უკვე აღარ იყო რელევანტური, რადგანაც საქმე იყო დასრულებული, ხოლო გუგლის საძიებო სისტემა მის სახელის მოძებნისას სწორედ ამ ინფორმაციას აჩვენებდა. გაზეთმა მონაცემების წაშლაზე უარი უთხრა მარიო გონზალესს, იმ მიზეზით რომ ეს სამინისტროს 1998 წლის ბრძანება იყო.

2010 წელს, მოპასუხემ მოსთხოვა ესპანეთში გუგლის კომპანიას - Google Spain, რომ შეეზღუდა წვდომა აღნიშნულ ბმულებთან. ესპანურმა კომპანიამ კი მოთხოვნა აშშ-

[36] Case C-131/12. Google Spain vs AEPD and Mario Costeja Gonsalez [2014].ბოლო გადამოწმების თარიღი: [09.09.2020]

ში გადააგზავნა, კალიფორნიის შტატში რეგისტრირებულ გუგლის ოფისში და მათ გადააბარა საქმეში გარკვევა, რადგან მიიჩნია რომ გუგლის პასუხისმგებლობა იყო საძიებო სისტემის მუშაობა. ამასთან ერთად, 2010 წლის 5 მარტს მარიო გონზალემა საჩივრით მიმართა „ესპანეთის მონაცემთა დაცვის სააგენტოს“ (Agencia Española de Protección de Datos) ესპანეთი ბეჭდური მედიის (La Vanguardia Ediciones SL) ერთ-ერთი ყოველდღიური გაზეთის, გუგლი ესპანეთისა და გუგლის კორპორაციის წინააღდეგ. საჩივრის ავტორი ხაზგასმით მიუთითებდა, რომ მისი სახელის მოძებნისას „Google Search“-ში ხსენებული გაზეთის ორი გვერდის ბმული იძებნებოდა და ამ ბმულების არარელევანტურობაზე აკეთებდა მითითებას. მისი მოთხოვნა იყო გაზეთის გვერდების ამოღება, შეცვლა ან საძიებო სისტემის საშუალებით მისი პერსონალური მონაცემები ყოფილიყო დაცული. მარიო გონზალეზი მოითხოვდა საკუთარი პერსონალური მონაცემების იმგვარად დაფარვას, რომ იგი საძიებო სისტემის შედეგებში არ ყოფილიყო ნაჩვენები აღნიშული ბმულებიდან.[37]

„ესპანეთი მონაცემთა დაცვის სააგენტომ“ განიხილა მარიო გონზალესის საჩივარი და ბეჭდური მედიის მიმართ დაყენებული მოთხოვნა არ დააკმაყოფილა, რადგან გაზეთში ინფორმაციის გამოქვეყნება გაამართლა იმით, რომ სამინისტროს ბრძანება და მიზნად ისახავდა აუქციონის შესახებ ინფორმაციის საჯაროდ გავრცელებას, რათა რაც შეიძლებოდა მეტ ადამიანს მიეღო მასში მონაწილეობა. თუმცა, საჩივარი დაკმაყოფილდა გუგლი ესპანეთისა და გუგლის კორპორაციის მიმართ და დაადგინა, რომ გუგლს სასწრაფოდ უნდა გადაედგა ნაბიჯები,წაეშალა მონაცემების ინდექსი და შეეზღუდა სამომავლოდ წვდომა, ევროკავშირის დირექტივის საფუძველზე. ასევე, „ესპანეთის მონაცემთა დაცვის სააგენტომ“ ჩაითვალა,,რომ საძიებო სისტემის ოპერატორები ახორციელებენ მონაცემთა დმაუშავებას და მათზე ვრცელდება ის პასუხისმგებლობა რაც დადგენილია პერსონალურ მონაცემთა დაცვის კანონმდებლობით. მან განმარტა, რომ პერსონალური მონცემის დაცვის უფლება პირის უბრალო სურვილსაც კი მოიცავს, რომ მის შესახებ

[37] იქვე

არსებული ნებისმიერი სახის ინფორმაცია არ იყოს ხელმისაწვდომი მესამე პირთათვის და ამის უზრუნველყოფის ვალდებულება უნდა დაეკისროთ საძიებო სისტემის ოპერატორებს.[38]

გუგლის კალიფორნიულმა და ესპანურმა კომპანიებმა გაასაჩივრეს ესპანეთის სასამართლოში და მიუთითეს, რომ კალიფორნიაში დაფუძნებული გუგლი ვალდებული არ იყო ევროკავშირის მონაცემთა დაცვის დირექტივას დამორჩილებოდა. ესპანეთის სასამართლომ საქმე გადასცა მართლმსაჯულების ევროპულ სასამართლოს და მოსთხოვა მათ პასუხი გაეცათ კითხვებზე : 1) დირექტივის მოქმედების არეალი ; 2) საძიებო სისტემის პროვაიდერი კომპანიის სამართლებრივი პოზიცია თუ შეიძლება ჩათვლილიყო მონაცემების მაკონტროლებლად ; 3) დირექტივა აწესებს თუ არა ე.წ „ დავიწყების უფლებას“[39].

ევროკავშირის მართლმსაჯულების სასამართლომ სამივე საკითხზე იმსჯელა და GDPR-ის ძალაში შესვლამდე,მონაცემთა დაცვის დირექტივის საფუძველზე დაადგინა, რომ პირს აქვს უფლება,,იყოს დავიწყებული“. დავიწყების უფლება გულისხმობს, რომ შესაძლოა პერსონალური მონაცემები თავის დროზე კონკრეტული პირის შესახებ საჯარო გახდა კანონიერი საფუძვლით, თუმცა ამის მიუხედავად პირს აქვს უფლება, გარკვეული დროის შემდეგ მოითხოვოს საკუთარი პერსონალური მონაცემების შემცველი ინფორმაცია აღარ იყოს ხელმისაწვდომი. სასამართლომ განმარტა, რომ „Google” როგორც საძიებო სისტემა არის მონაცემთა მაკონტროლებელი იურიდიული პირი, რომელიც აკონტროლებს იმ წესებსა და მიზეზებს თუ რატომ და რა ფორმით მუშავდება ესა თუ ის მონაცემი. სასამართლომ ასევე დაადგინა, რომ რადგან ესპანურ გუგლზე ვრცელდება დირექტივა, მაშინ ის ვრცელდება მის მფლობელზეც, რადგანაც კალიფორნიაში რეგისტრირებული გუგლის იურიდიული პირი ფლობს ესპანეთში რეგისტრირებული გუგლს, შესაბამისად ის ვრცელდება მის მფლობელზეც.[40]

[38] იქვე
[39] იქვე
[40] იქვე

აღსანიშნავია, რომ სასამართლომ მოსარჩელის ის არგუმენტი არ გაიზიარა, რომ ესპანეთში არ ხდებოდა მონაცემთა დამუშავება, რადგან ამის დადასტურება ადამიანის ძირითადი უფლებების შელახვას გამოიწვევდა და ამით, ფაქტობრივად, დირექტივის მთელი არსი დაიკარგებოდა. [41] სასამართლოს აზრით,მნიშვნელოვანია, რომ დაცული იყოს ორივე მხარის უფლება-მონაცემთა მაკონტროლებლის და მონაცემთა სუბიექტის. დირექტივის მე-14 მუხლი საშუალებას აძლევს პირს, რომ გარკვეულ შემთხვევებში შესაძლებლობა აქვს გაასაჩივროს მის შესახებ არსებული მონაცემთა დამუშავება. ეს საჩივარი უნდა შევიდეს პირდაპირ მონაცემთა მაკონტროლებელთან, ამ უკანასკნელმა კი საფუძვლიანად უნდა შეასრულოს მიზეზები და შესაბამისად მოიქცეს, საჭიროების შემთხვევაში კი შეწყვიტოს მონაცემების დამუშავება. [42]

„დავიწყების უფლებას“ რაც შეეხება, საინტერესოა, რომ გარდა გუგლის კომპანიებისა,საბერძნეთის, ავსტრიისა და პოლონეთის სახელმწიფოებმა, აგრეთვე ევროპის კომისიამ ურჩია სასამართლოს, რომ არ დაემკვიდრებინა ეს უფლება. მათ მხოლოდ რჩევა შეეძლოთ, რაც სასამართლომ არ გაითვალისწინა და განმარტა, რომ არსებობს ისეთი მონაცემები, რომელიც შეუსაბამობაში მოდის დირექტივასთან და სწორედ ასეთი მონაცემები უნდა წაიშალოს მონაცემის სუბიექტის მოთხოვნის შესაბამისად. როდესაც მონაცემი არის არასწორი, არაზუსტი, ზედმეტად ინფორმატიული ან არა რელევანტური, მაშინ მონაცემის მაკონტროლებელმა უნდა წაშალოს ასეთი ინფორმაცია ან როგორც მინიმუმ შეზღურდოს მასზე წვდომა. [43]

ევროპის მართლმსაჯულების სასამართლოს ზემოხსენებულ გადაწყვეტილებაზე დაყრდნობით, აღნიშნული საქმე მნიშვნელოვანი პრეცედენტი გახდა პერსონალურ მონაცემთა დაცვის სფეროში.

[41] იქვე, 50-58
[42] იქვე,77
[43] იქვე, 94

დავიწყების უფლება ძალიან დელიკატური საკითხია და შეუძლებელია მისი ბრმად აღსრულება. აღსრულებისთვის საჭიროა, რომ საძიებო სისტემებმა გაითვალისწინონ, როგორც ადამიანის პირადი უფლებები, ასევე,საჯარო ინტერესები. სასამართლოს მიერ მიღებული გადაწყვეტილება ერთის მხრივ საშუალებას აძლევს ადამიანებს, რომ შეზღუდონ საკუთარ პერსონალურ მონაცემებზე წვდომა, მაგრამ, თუ რა ტიპის მონაცემები უნდა შეიზღუდოს სწორედ ეს ხდება განხილვის საგანი.

იმისათვის, რათა დაცული იყოს ადამიანის ფუნდამენტური უფლებები აუცილებელია მას გააჩნდეს თავისუფლად ცხოვრების შესაძლებლობა. ინტერნეტსივრცეში განთავსებული წარსულში მომხდარი ქმედებისთვის პირის ინტერესებს საფრთხე არ უნდა დაემუქროს, სწორედ ამ მიზნით აუცილებელია, კიდევ უფრო მეტად დაიხვეწოს დავიწყების უფლება.

4.2 ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR)

2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია („General Data Protection Regulation“)[44], აღნიშნულმა რეგულაციამ ახალ საფეხურზე გადაიყვანა პერსონალურ მონაცემთა დაცვა. რეგულაციის მთავარი მიზანია ადამიანის უფლებების სათანადო დაცვა ტექნოლოგიური პროგრესის და გამოწვევების პირობებში. რეგულაცია ამკვიდრებს ისეთ ახალ პრინციპებს, როგორიცაა მონაცემთა დამმუშავებელი ორგანიზაციების ანგარიშვალდებულება, მონაცემთა უსაფრთხოების დარღვევის შეტყობინების ვალდებულება, მონაცემთა პორტირება და სხვა. 2018 წელს როდესაც რეგულაცია ძალაში შევიდა ყველა

[44] https://eur-lex.europa.eu/eli/reg/2016/679/oj.ბოლო გადამოწმების თარიღი: [09.09.2020]

სახელმწიფოსთვის გახდა სავალდებულო გახდა ამ რეგულაციის ქვეშ მუშაობა და მან სრულებით ჩაანაცვლა, 1995 წელს გამოშვებული, მონაცემთა დაცვის დირექტივა.

პრობლემები, რომელთა გადასაჭრელადაც GDPR გახდა საჭირო, ტექნოლოგიების და ინტერნეტის განვითარებამ წარმოშვა, შეიძლება ითქვას,რომ იგი კარგ დროს შეიქმნა. მთავარია გავარკვიოთ თუ რამდენად სწორი იყო ის ცვლილებები, რითაც განსხვავდება ახალი რეგულაცია ძველი გაუქმებული დირექტივისგან (მონაცემთა დაცვის დირექტივა 1995 წ.)

„ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია ვრცელდება ევროკავშირში რეგისტრირებულ ნებისმიერ ორგანიზაციაზე, რომელიც საქმიანობის ფარგლებში ამუშავებს პერსონალურ მონაცემებს. სხვა ქვეყნებში, მათ შორის, საქართველოში რეგისტრირებულ ორგანიზაციებზე, რეგულაცია ვრცელდება იმ შემთხვევაში, თუ მათ აქვთ ფილიალი/წარმომადგენლობა ევროკავშირის ტერიტორიაზე ან:

- ამუშავებენ ევროკავშირის ტერიტორიაზე მყოფი პირების მონაცემებს მათთვის მომსახურების ან პროდუქციის შეთავაზების მიზნით, იმის მიუხედავად, ფასიანია თუ არა ეს მომსახურება ან პროდუქტი;
- მონიტორინგს უწევენ პირთა ქცევას ევროკავშირის ტერიტორიაზე.“[45]

შესაბამისად, მარეგულირებელი ორგანიზაციები აღარ დაიწყებენ იმის გარკვევას, უცხოურ კომპანიებს მათ ტერიტორიაზე რაიმე სახის ორგანიზაცია ხომ არ აქვთ შექმნილი.

აღსანიშავია, რომ მონაცემთა დაცვის გაუქმებული დირექტივის თანახმად,მხოლოდ მონაცემთა მაკონტროლებელი პირი იყო პასუხისმგებლობის სუბიექტი თუ ამას საჭიროება მოითხოვდა, ხოლო ახალმა რეგულაციამ (General

[45] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაცია : „რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ“.ბოლო გადამოწმების თარიღი: [09.09.2020]

Data Protection Regulation) შეცვალა მიდგომა პასუხისმგებლობასთან დაკავშირებით და თქვა, რომ ჩადენილი ქმედებისთვის პასუხისმგებლობა უნდა დაეკისროს იმ პროცესოს კომპანიას, რომელსაც მაკონტროლებელის მონაცემთა დამუშავება ევალებოდა. [46]

„მონაცემთა დაცვის ზოგადი რეგულაცია“ არსებითად არ ცვლის მონაცემთა დამუშავების 1995 წლის 95/46/EC დირექტივით[47] განსაზღვრულ პრინციპებს. ორგანიზაციებმა მონაცემები უნდა დაამუშავონ შემდეგი პრინციპების დაცვით:

- მონაცემები უნდა დამუშავდეს კანონიერად და სამართლიანად; დამუშავების შესახებ ინფორმაცია მარტივად ხელმისაწვდომი უნდა იყოს პირისთვის;
- მონაცემები უნდა შეგროვდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის;
- მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია კონკრეტული კანონიერი მიზნის მისაღწევად;
- მონაცემები უნდა იყოს ზუსტი და, საჭიროების შემთხვევაში, განახლებული;
- იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა ინახებოდეს პირის იდენტიფიცირების გამომრიცხავი ფორმით;
- მონაცემების დამუშავებისას უზრუნველყოფილი უნდა იყოს მათი უსაფრთხოება და დაცვა უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვის, განადგურებისა და დაზიანებისგან. სიახლეს წარმოადგენს ანგარიშვალდებულების პრინციპი, რომელიც მკაფიოდ

[46] The main differences between the DPD and the GDPR and how to address those moving forward.ბოლო გადამოწმების თარიღი: [09.09.2020]

[47] ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივა პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამ მონაცემთა თავისუფალი მიმოცვლის შესახებ.ბოლო გადამოწმების თარიღი: [09.09.2020]

მიუთითებს, რომ ორგანიზაცია პასუხისმგებელია დამუშავების ყველა პრინციპის დაცვაზე და უნდა შეეძლოს ამის დადასტურება.[48]

ძალიან მნიშვნელოვანია და როგორც ჩვენი კვლევის წინა თავშია ნახსენები, ევროკომისიამ გააფართოვა პერსონალურ მონაცემთა განმარტება. თუ დირექტივა ითვალისწინებდა მხოლოდ სახელს, გვარს,ფოტოს, ელექტრონული ფოსტის მისამართს, მისამართს, ტელეფონის ნომერსა და პირად ნომერს, მონაცემთა დაცვის ზოგადმა რეგულაციამ დაამატა რამდენიმე მნიშვნელოვანი პუნქტი, კერძოდ: აი-პი მისამართი, მობილური მოწყობილობის იდენტიფიკატორი, ლოკაცია, ბიომეტრიული მონაცემები, ასევე, ფსიქოლოგიური და გენეტიკური იდენტობა, ეკონომიკური სტატუსი, კულტურული და სოციალური იდენტურობა.[49]

მონაცემთა დაცვის ზოგად რეგულაციაში მნიშვნელოვანია 17-ე მუხლი, რომელიც დავიწყების უფლებას ეხება, მისი მიხედვით : „ორგანიზაცია ვალდებულია წაშალოს მონაცემები, თუ, მაგალითად:

- მონაცემები აღარ არის საჭირო იმ მიზნის მისაღწევად, რისთვისაც მოხდა მათი შეგროვება ან დამუშავება;
- დამუშავება განხორციელდება არაკანონიერად;
- პირი გაითხოვს თანხმობას, რომლის საფუძველზეც მუშავდებოდა მონაცემები.“[50]

[48] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაცია : „რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ“.ბოლო გადამოწმების თარიღი: [09.09.2020]

[49] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს), მუხლი 4.ბოლო გადამოწმების თარიღი: [09.09.2020]

[50] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაცია : „რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ“.ბოლო გადამოწმების თარიღი: [09.09.2020]

აღნიშნულმა მუხლმა ძველი დირექტივის კიდევ ერთი პრობლემა მოაგვარა და დეტალურად განმარტა თუ კონკრეტულად რა შემთხვევაში არ შეიძლება დავიწყების უფლების გამოყენება. დავიწყების/წაშლის უფლება არ გამოიყენება როდესაც მონაცემის დამუშავება აუცილებელია :

- გამოხატვის თავისუფლებისა და ინფორმაციის მიღების უფლების განხორციელებისათვის;
- ევროკავშირის ან წევრი სახელმწიფოს კანონის შესაბამისად დამმუშავებლის კანონისმიერი ვალდებულების შესასრულებლად, ან საჯარო ინტერესის სფეროში შემავალი ფუნქციების შესასრულებლად ან დამმუშავებლისათვის კანონით მინიჭებული უფლებამოსილების განსახორციელებლად;
- საჯარო ინტერესის მიზნებისათვის საყოველთაო ჯანმრთელობის დაცვის სფეროში;
- საჯარო ინტერესებისათვის არქივირების მიზნით;
- სამართლებრივი მოთხოვნის დადგენის, განხორციელების ან დაცვის მიზნებისთვის.[51]

ჩვენს სამყაროში ისეთი მნიშვნელოვანი ინფორმაცია, როგორიცაა პერსონალური მონაცემები, მაქსიმალურად დაცული უნდა იყოს ნებისმიერი ხელყოფისგან, თუმცა ეს ყოველთვის შესაძებელი არაა. ძალიან ძლიერ კორპორაციებსაც მაქსიმალურად აქვთ გააზრებული პერსონალურ მონაცემთა შენახვისა და დამუშავების რისკები და ის შედეგები რაც მათთვის შიძლება მონაცემების უკანონო დამუშავება-გავრცელებამ მოიტანოს. დღესდღეობით არც ერთ სახელმწიფოში მონაცემთა მაკონტროლებლებს (პროცესორებს) არ აქვთ ილუზია იმისა, რომ მათი მონაცემთა ბაზა არის აბსოლიტურად დაცული ნებისმიერი კიბერ შეტევისგან. ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია მიუთითებს :"პერსონალურ მონაცემთა უსაფრთხოების დარღვევა“ ნიშნავს უსაფრთხოების დარღვევას, რომელიც

[51] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს),მუხლი 17(3).ბოლო გადამოწმების თარიღი: [09.09.2020]

გადაცემული, შენახული, ან სხვაგვარად დამუშავებული მონაცემების შემთხვევით ან უკანონო განადგურებას, დაკარგვას, შეცვლას, მათ უკანონო გამჟღავნებას ან მონაცემებზე არასანქცირებულ წვდომას.[52]

აღნიშნული რეგულაციისთვის გადამწყვეტი არ არის თუ რა სახით მოხდება „მონაცემთა უსაფრთხოების დარღვევა“. ევროკავშირის მონაცემთა ზოგადი რეგულაცია ყურადღებას ამახვილების ბაზის გატეხვის შემდგომ შესასრულებელ აუცილებელ მოქმედებებსა და ნაბიჯებზე, თუ რა უნდა მოიმოქმედონ კომპანიებმა ნაკლები ზარალისთვის. GDPR-ს აქვს ერთი მნიშვნელოვანი წესი, რომელიც რეგულაციის 33-ე მუხლშია რეალიზებული და მისი მიხედვით, პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში მონაცემთა დამმუშავებელმა დაუყოვნებლივ და თუ შესაძლებელია დარღვევის შესახებ შეტყობიდან არაუგვიანეს 72 საათისა უნდა შეატყობინოს აღნიშნულის თაობაზე კომპეტენტურ საზედამხედველო ორგანოს. ხოლო, თუ შეტყობინება 72 საათის განმავლობაში არ განხორციელდა, მას აუცილებლად თან უნდა დაერთოს განმარტება დაყოვნების მიზეზების თაობაზე.

ასევე, რეგულაციის შედეგად წარმოშობილი ახალი ვალდებულებაა პერსონალური მონაცმების ანონიმიზაცია და ფსევდონიმიზაცია, რის შესახებაც კვლევაში უკვე გვქონდა დეტალურად საუბარი. GDPR ავალდებულებს კომპანიებს, რომ მხოლოდ საჭირო მონაცემები შეინახოს და დაამუშაოს რეგულაციის პრინციპების შესაბამისად, წინააღმდეგ შემთხვევაში კომპანიებს დაეკისრებათ ჯარიმა თუ ისინი არ დაემორჩილებიან ევროკავშირის მიერ მიღებულ რეგულაციებს.

მონაცემთა დაცვის დირექტივა, რომელიც გაუქმდა GDPR -ს ძალაში შესვლის შემდეგ, ჯარიას საერთოდ არ ითვალისწინებდა. დირექტივა წევრ ქვეყნებს უფლებას ანიჭებდა, რომ შიდა სახელმწიფოებრივი კანონმდებლობით

[52] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს)მუხლი 4,ნაწილი 12..ბოლო გადამოწმების თარიღი: [09.09.2020]

დაერეგულირებინათ აღნიშნული საკითხი. [53] ევროკომისიამ ახალი რეგულაციების ქვეშ მოექცა ჯარიმებიც. რეგულაციის წესების დარღვევები იყოფა ორ კატეგორიად, პირველი კატეორია არის შედარებით მსუბუქი დარღვევები როდესაც ოგანიზაციამ არ შასრულა მონაცემთა უსაფრთხოების დარღვევისას შეტყობინების ვალდებულება ან ევროკავშირის ტერიტორიის გარეთ დარეგისტრირებულმა ორგანიზაციამ არ დანიშნა წარმომადგენელი ევროკავშირში და ასეთ შემთხვევაში ჯარიმის მაქსიმალური ოდენობა არის 10,000,000 ევრო ან კომპანიის წლიური ბრუნვის 2%;

მეორე კატეგორია არის მძიმე დარღვევები, ასეთად შეიძლება ჩაითვალოს თუ დაირღვა მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებული წესები ან ორგანიზაციამ დაარღვია პირის თანხმობასთან დაკავშირებული წესები და სხვა. ამ შემთხვევაში კომპანიისთვის ჯარიმის მაქსიმალური ოდენობა არის 20,000,000 ევრო ან კომპანიის წლიური ბრუნვის 4%.[54]

შეიძლება სანქციები შორიდან ძალიან დიდი ჩანდეს, თუმცა ასეთი თანხები პატარა კომპანიებს უქმნის განწყობას,რომ მუდმივად აკონტროლონ პეროსნალური მონაცემების კანონიერება ევროკავშირის კანონმდებლობის შესაბამისად, ხოლო დიდ კომპანიები რეგულაციის დარღვევისთვის სამაგალითოდ იქნებიან დასჯილნი.

თითქმის საყოველთაო კონსენსუსი არსებობს, რომ საქართველოში კანონმდებლობით გათვალისწინებული პერსონალურ მონაცემთა დარღვევისთვის გათვალისწინებული ჯარიმები არის არაფექტური. საჯარიმო სანქციები იწყება 100

[53] The main differences between the DPD and the GDPR and how to address those moving forward.ბოლო გადამოწმების თარიღი: [09.09.2020]

[54] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) მუხლი 83..ბოლო გადამოწმების თარიღი: [09.09.2020]

ლარიდან და ადის 10 000 ლარამდე,თუმცა აღნიშული სანქციები ვერ აიძულებს კომპანიებს რომ იზუნონ საკუთარი მომხმარებლების მონაცემთა დაცვაზე. კომპანიები ამჯობინებენ გადაიხადონ ფულადი ჯარიმები იმის მაგივრად, რომ საკუთარ ბიზნეს პროცესების მართვას გადახედონ და მეტი ხარჯი გაიღონ მონაცემთა დაცვის უზრუნველსაყოფად.ასეთი ვითარების ფონზე განსაკუთრებით თვალშისაცემია GDPR-ს მიერ შემოთავაზებული სანქციების ახალი სტანდარტი. ევროკავშირის პერსონალურ მონაცემთა დაცვის ზოგადი რეგულაციის მიღებას თან გარკვეული სკეპტიციზმი ახლდა, ეს სკეპტიცისმი განსაკუთრებით იგძნობოდა საქართველოს გადმოსახდიდან, რადგან მილიონიანი ჯარიმები საკმაოდ არარეალური ჩანდა. ეს გასაკვირი არც იყო, რადგანაც თავად ევროპაც ეჭვის თვალით უყურებდა თუ პრაქტიკაში რამდენად იმუშავებდა რეგულაცია. პრაქტიკაში კი მოხდა შემდეგი : 2019 წლის იანვარში საფრანგეთში, მონაცემთა დაცვის მარეგულირებელმა ტექნოლოგიური კომპანია Google 50 მილიონი ევროს ოდენობით დააჯარიმა თანხმობების არასწორად მოპოვებისა, რადგან ადამიანებმა არ იცოდნენ რაზე თანხმდებოდნენ და მომხმარებლებისათვის არასაკმარისი ინფორმაციის მიწოდებისათვის. მარეგულირებელმა ჩათვალა, რომ კომპანია მომხმარებლებს არ აძლევდა საკმარის კონტროლს მათი მონაცემების გამოყენებაზე და გარდა შთამბეჭდავი ჯარიმისა, დარღვევების გამოსწორებაც დაავალა. [55]ეს იყო GDPR-ის პირველი რეალური გამოყენება და გუგლის სახით შეიქმნა პრეცედენტი, რომ ევროკავშირის მიერ დადგენილ ზოგად რეგულაციებს ვერავინ გაექცევა.

4.3 ევროკავშირის პრობლემები და გამოწვევები

[55] პერსონალურ მონაცემთა დაცვის ახალი რეალობა ევროპაში - საჯარიმო სანქციები GDPR -ის ამოქმდების შემდეგ, 2019 წ..ბოლო გადამოწმების თარიღი: [09.09.2020]

ევროკავშირის მონაცემთა დაცვის გენერალური რეგულაციის (GDPR) დანერგვით, 2018 წლის 25 მაისს, დაიწყო მარეგულირებელი ახალი რეჟიმი ბიზნესისთვის ევროპაში და ასევე მის ფარგლებს გარეთ. შეგვიძლია ვთქვათ, რომ GDPR– ის საერთაშორისო მიღწევაა ის, რომ იგი ევროკავშირის მოქმედების სფეროს სცდება და მიუხედავად იმისა, რომ GDPR არის ევროკავშირის რეგულაცია, მისი მოქმედების არეალი უფრო ფართოა. რეგულაცია ვრცელდება არა მხოლოდ ევროკავშირში რეგისტრირებულ ორგანიზაციებზე, არამედ იმ ორგანიზაციებზეც, რომლებიც არ არიან ევროკავშირში რეგისტრირებული, თუმცა ამუშავებენ ევროკავშირში მყოფი პირების მონაცემებს.

ევროკავშირის გარეთ მყოფი ქვეყნის მთავრობები ადგენენ დაცვის ახალ რეგულაციებს ან აძლიერებენ არსებულ წესებს, რათა ისინი მიებაძოს GDPR– ს. ევროკავშირი ყოველდღიურად მიიწევს წინ ჰარმონიზაციისკენ,რასაც სჭირდება, რომ ქყეყნები იყვნენ ერთ აზრზე და ერთი კანონის მოქმდების სფეროს ფარგლებში ეწეოდნენ საქმიანობას. ამაში GDPR-ს რეგულაციები გარკვეულწილად დაეხმარა ევროკავშირს, როდესაც ხელმოწმერ სახელმწიფოებს გარკვეულ საკითხებში შეუმცირა არჩევანის თავისუფლება და ისინი ახალი რეგულაციის ნაწილად აქცია. მიუხედავად უფლებამოსილებების შემცირებისა, ევროკავშირმა ხელმომწერ ქვეყნებს მაინც დაუტოვა გარკვეული შესაძლებლობები. მაგალითად : GDPR-ში ვერ ვიპოვით მუხლს, რომელშიც წერია თუ როდის შეუძლია ხელმომწერ ქვეყანას შეიმუშაოს დამატებითი შიდა კანონმდებლობა, რაც გარკვეულ შემთხვევებში გაურკვევლობას გამოიწვევს. თუ ეპანეთის მოქალაქე პირი გადაწყვეტს გამოიყენოს დაივწყების უფლება ესპანეთში, მაგრამ

მისი პერსონალური მონაცემები მუშავდება საბერძნეთში და ბერძნული კომპანია იყენებს ისეთ განსხვავებულ კანონმდებლობას, რომლის საშუალებითაც შესაძლებელია პერსონალური მონაცემის დამუშავების უფლების შენარჩუნება, საინტერესოა რა მოხდება ასეთ შემტხვევაში და როგორ გადაჭრის პრობლემურ საკითხს ზოგადი რეგულაციები.

ევროკავშირის ზოგადმა რეგულაციამ ბევრი ახალი ვალდებულება შემოიღო კომპანიებისთვის და კომპანიები დღემდე ცდილობენ თავიანთი შიდა პროცესების ადაპტირებას GDPR-ის დებულებებთან. ერთ -ერთი ყველაზე ღრმა სირთულეს წარმოადგენს კომპანიებისთვის არსებული სარეზერვო პროცედურების შესაბამისობა GDPR-თი აღიარებულ „დავიწყების უფლებასთან ". ტექნოლოგიების განვითარებასთან ერთად კომპანიები ვალდებულნი არიან რეგულარულად შეინარჩნუნონ თავიანთი მონაცემების სარეზერვო ასლები უსაფრთხოების ინციდენტების ან ფიზიკური კატასტროფების შემთხვევაში.GDPR–ის კანონმდებლობის თანახმად ჩნდება დიდი კითხვა, თუ როგორ უნდა მოიქცნენ ორგანიზაციები თავიანთ სარეზერვო ასლებს მას შემდეგ, რაც მომხმარებელი ითხოვს „დავიწყების უფლების „ გამოყენებას საკუთარ პერსონალურ მონაცემებზე. როგორც ჩანს, GDPR– ის თანახმად, ეს წაშლა უნდა განხორციელდეს სარეზერვო ასლებშიც, რაც თავის თავად დამატებით ხარჯებს მოიცავს.[56]

ევროკავშირის მთავარი მიზანია,რომ მაქსიმალურად დაიცვას საკუთარი მოქალაქეების პერსონალური მონაცემები და ხელი შეუწყოს კანონის ჰარმონიზაციას, თუმცა ამ შედეგის მიღწევა საკმაოდ რთულია, რადგან კომპანიები ერთი ქვეყნის ტერიტორიით აღარ არიან შეზღუდულნი და მონაცემთა ბაზების გაცვლა და დამუშავება გახდა ძალიან მარტივი და სწრაფი პროცესი. GDPR ყველანაირად ცდილობს, რომ გაუმკლავდეს არსებულ პრობლემებს და დაავალდებულოს „მესამე სახელმწიფოები", რომ მეტი გააკეთონ პერსონალურ მონაცემთა დაცვისთვის. მესამხე სახელმწიფოებთან იფნორმაციის მიმოცვლას და სამართლებრივ საკითხებს ცალკე V თავი ეძღვნება GDPR-სი, რომელიც ძალადაკარგული დირექტივის მიერ დაწესებული პრინციპებისგან დიდად არ განსხვავდება. [57]

[56] Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions,2018.ბოლო გადამოწმების თარიღი: [09.09.2020]

[57] მონაცემთა დაცვის ზოგადი რეგულაცია, V თავი;.ბოლო გადამოწმების თარიღი: [09.09.2020]

ევროკავშირის მიერ მიღებული რეგულაციის სიმკაცრე რაღაც კუთხით ნამდვილად კარგია. მთავარია, რომ სახელმწიფოები გაერთიანდნენ ერთი არსებული მიზნის მისაღწევად, რომ უკეთ დაიცვან საკუთარი მოქალაქეების პერსონალური მონაცემები. მნიშვნელოვანია იმის გააზრება, რომ ინდივიდის პერსონალური მონაცემები არის დღევანდელი ინფორმაციული სამყაროს განუყოფელი ნაწილი, ხოლო ევროკავშირის მოქალაქეების პერსონალური მონაცემები კი წარმოადგენს მონაცემთა ძალიან დიდ ბაზას და მათი გამოყენება საჭიროა ევროკავშირის გარეთ სხვადასხვა ქვეყნებისთვის და კომპანიებისთვის, ამიტომაც ევროკავშირის დამოკიდებულება ამ ქვეყნების მიმართ არ უნდა იყოს მკაცრი და საშუალება უნდა მიეცეთ შეერთდნენ ევროკავშირს მოქალაქეების პეროსნალურ მონაცემებთა გაცვლა-გამოცვლის საქმიანობაში.

5.საქართველო და პერსონალური მონაცემების დაცვა.

საქართველოში სპეციალური კანონის მიღებამდე,2012 წლამდე, პერსონალურ მონაცემთა დაცვისა და დამუშავების წესს განსაზღვრავდა „საქართველოს ზოგადი ადმინისტრაციული კოდექსი“[58], ასევე,,კომერციული ბანკების საქმიანობის შესახებ” კანონი[59] და „საქართველოს სამოქალაქო კოდექსი“[60]. თუმცა,როგორც უკვე

[58] „საქართველოს ზოგადი ადმინისტრაციული კოდექსის“ მესამე თავი, 25/06/1999 წლის რედაქცია.ბოლო გადამოწმების თარიღი: [09.09.2020]

[59] კომერციული ბანკების საქმიანობის შესახებ“ საქართველოს კანონის 171 მუხლი..ბოლო გადამოწმების თარიღი: [09.09.2020]

[60] საქართველოს სამოქალაქო კოდექსი.ბოლო გადამოწმების თარიღი: [09.09.2020]

კვლევაში აღვნიშეთ,ევროკავშირისკენ სწრაფვის და განვითარების სურვილმა ამ პრობლემის ცალკე საკანონმდებლო აქტით მოწესრიგება განაპირობა და პერსონალური მონაცემების დამუშავების, ადამიანის უფლებათა და თავისუფლებათა, მათ შორის პირადი ცხოვრების ხელშეუხებლობის დაცვის უზრუნველსაყოფად 2012 წელს ძალაში შევიდა საქართველოს კანონი,,პერსონალურ მონაცემთა დაცვის შესახებ“

2013 წელს საქართველოში უკვე იქმნება პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, როგორც სახელმწიფოს საზედამხედველო ორგანო., რაც იმ დროისტვის ნოვაციას წარმოადგენდა. აღსანიშნავია ის გარემოებაც, რომ საქათველოს მოქალაქეებმა ძალიან სწრაფად და აქტიურად დაიწყეს თანამედროვე ინფორმაციული ტექნოლოგიების ათვისება, იმის მიუხედავად, რომ ინტერნეტ სივრცე საქართველოში შედარებით გვიან განვითარდა. ასევე უნდა აღინიშნოს, რომ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ცალკეული დებულებების ამოქმედება ეტაპობრივად განხორციელდა[61].

საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 აწესებს პერსონალურ მონაცემთა დაცვის ძირითად სახელმძღვანელო პრინციპებს, რომელიც ეყრდნობა ევროკავშირის მიერ შექმნილ პრინციპებს:

„ა) მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად;

ბ) მონაცემები შეიძლება დამუშავდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველ მიზანთან შეუთავსებელი მიზნით;

[61] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 56-ე მუხლი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

გ) მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელი ც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდ ება ისინი;

დ) მონაცემები ნამდვილი და ზუსტი უნდა იყოს და, საჭიროების შემთხვევაში, უნდა განახლდეს. კანონიერი საფუძვლის გარეშე შეგროვებული და დამუშავების მიზნის შეუსაბამო მონაცემები უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს;

ე) მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს ან შენახული უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით, თუ კანონით სხვა რამ არ არის დადგენილი.“[62]

აღსანიშნავია, რომ„პერსონალურ მონაცემთა დაცვის შესახებ“ ამონაცემთა სუბიექტს საშუალებას ანიჭებს საშუალებას, რომ მოითხოვოს საკუთარი ინფორმაციის წაშლა: „მონაცემთა სუბიექტის უფლება, მიიღოს ინფორმაცია მის შესახებ დამუშავებულ მონაცემთა თაობაზე, მოითხოვოს მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა და განადგურება.“[63] ამით, საქართველოს კანონი, გარკვეულწილად აღიარებს „დავიწყების უფლების“ პრინციპს, რომელიც რეალიზებულია GDPR-ს 17-ე მუხლში.

[62] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

[63] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 15-ე მუხლი „დ“ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

როგორც უკვე აღვნიშნეთ, „პერსონალური მონაცემების დაცვის შესახებ“ კანონმა პირველად დაამკვიდრა პერონალურ მონაცემთა დაცვის ინსპექტორის ინსტიტუტი საქარველოში, რომელიც 2013 წლიდან მოქმედებს აქტიურად. იგი „ პასუხისმგებელია მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულების ზედამხედველობისთვის“[64], აღსანიშნავია რომ „სახელმწიფო ინსპექტორის სამსახური ვალდებულია აწარმოოს ფაილურ სისტემათა კატალოგების რეესტრი.“[65] ნებისმიერი ბიზნესი, რომელიც საქართველოს ტერიტორიაზე ამუშავებს „ფაილურ კატალოგს“, ვალდებულია, რომ შეავსოს სპეციალური ფორმა პერსონალურ მონაცემთა დაცვის ინსპექტორის საიტზე და თუ მიუთითებს მონაცემთა შენახვის ვადასა, მიზეზს და დაცვის ზოგად წესებს,პრობლემების გარეშე შეუძლია საქმიანობის გაგრძელება[66]. ვალდებულება აკისრია ნებისმიერ ბიზნესს, რომელიც რეგისტრირებულია საქართველოში და ამუშავებს მონაცემებს ან არ არის რეგისტრირებული საქართველოში, მაგრამ იყენებს საქართველოს ტერიტორიაზე არსებულ ტექნიკურ საშუალებებს, ინფორმაციის დამუშავებისთვის. [67]

კანონის ნაკლოვანებად უნდა ჩაითვალოს ის ფაქტი,რომ საქართველოს კანონი მკაცრად ერგება საქართელოს ტერიტორიას და არა ამ ტერიტორიაში მცხოვრებ პირებს. ეს დათქმა უცნაურ მდგომარეობაში აყენებს როგორც კერძო ბიზნესებს, ასევე საჯარო იურიდიულ პირებსაც. წარმოვიდგინოთ ასეთი შემთხვევა, მაგალითად საქართველოს განათლებისა და მეცნიერების სამინისტრომ გადაწყვიტა გამოიყენოს უცხოეთსი არსებული კომპანია მონაცემების მარეგულირებლად, ამასთან ერთად გამოიყენოს ისეთი ქვეყანა რომელსაც

[64] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლი „ტ“ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

[65] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 19-ე მუხლის 1^1 ნაწილი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011,.

[66] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 19-ე მუხლის 1 ნაწილი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011,.

[67] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011, მუხლი 3 (1,2)

პერსონალური მონაცმეების დაცვის შესახებ კანონმდებლობა არ გააჩნია, რა მოხდება ამ შემთხვევაში ?!
ნებისმიერი საჯარო იურიდიული პირი შეძლებს საქართველოს კანონს აუაროს გვერდი და ყველანაირი შეზღუდვის გარეშე დაამუშავებს და საკუთარ ნებაზე გამოიყენებს პერსონალურ მონაცემებს.

“პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მეორე სისუსტეს ვაწყდებით საერთაშორისო ასპარეზზე, როდესაც მულტი-ნაციონალური კომპანიები ამუშავებენ მთელი მსოფლიოს მოსახლეობის პერსონალურ მონაცემებს. მაგალითად წარმოვიდგინოთ ასეთი შემთხვევა, ერთ-ერთი აქტიური სოციალური ქსელი „Instagram“-ი ამუშავებს მსოფლიოს მოსახლეობის პერსონალურ მონაცემებს, მათ შორის საქართველოს მოსახლეობის მონაცემებსაც. საქართველოს არ იცას ევროკავშირის რეგულავია, მას იცავს მხოლოდ ქართული კანონი “პერსონალურ მონაცემთა დაცვის შესახებ“. დღევანდელი კანონმდებლობის მიხედვით, როდესაც „Instagram“-ი საქართველოდან პერსონალურ მონაცემებს აგროვებს, თუ იგი ამ ინფორმაციას უშუალოდ საქართველოს ტერიტორიაზე არ ამუშავებს, მაშინ ჩვენი კანონის მიხედვით,მას შეუძლია, რომ შეუზღუდავად შეაგროვოს ყველაფერი რაც მოესურვება და საკუთარი სურვილისამებრ გამოიყენოს იგი. ანუ ამ შემთხვევაში გამოდის, რომ კომპანიის ერთადერთი მარეგულირებელი არის საკუთარი თავი.

ამ მაგალითებით ნათელი ხდება, რომ საქართველოს კანონი საერთოდ არ არის მორგებული საერთაშორისო რეალობას და მისი მთავარი მიზანია საქართველოს ტერიტორიაზე გააკონტროლოს პერსონალური მონაცემების დაცვა. საქართველოს მოსახლეობა ვერ იაზრებს პერსონალური მონაცემების დაცვის მნიშვნელობას და ვერ იაზრებენ იმ რისკებს რაც შეიძლება მათი პეროსნალური მონაცემების უკანონო დამუშავებას მოჰყვეს. სწორედ ამიტომ აუცილებელია შეიქმნას პერსონალური მონაცემების დაცვის თანამედროვეობას მორგებული მეთოდები, რომლებიც

საქართველოს მოსახლეობის პერსონალურ მონაცმეებს დაიცავს საქართველოს ტერიტორიის ფარგლებს გარეთაც.
განსაკუთრებული საყურადღებოა GDPR-ის მაღალ სტანდარტებზე ყურადღების გამახვილება, რადგანაც საქართველოს მიზანია ევროკავშირის კანონმდებლობასთან საქართველოს კანონმდებლობის მაქსიმალურად მიახლოება და მომავალში აღნიშნულ ორგანიზაციაში წევრობა.

საინტერესოა პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის პრაქტიკა საქართველოში. 2020 წელს საქართველოსა და მთელი მსოფლიოსთვის COVID-19-ის პანდემია ძალიან სერიოზულ გამოწვევად იქცა. მოქალაქეების ჯანმრთელობის დასაცავად დაწესებული გადაადგილებისა და პირადი კომუნიკაციის შეზღუდვის გამო, აუცილებელი გახდა მონაცემთა დამუშავების ახალი პროცესების დანერგვა და უკვე დანერგილი პროცესების დისტანციურ-ონლაინ სივრცეში გადანაცვლება. აღსანიშნავია, რომ 2020 წელს სახელმწიფო ინსპექტორის სამსახურს სამუშაო პროცესი არ შეუჩერებია და იგი დისტანციურ რეჟიმში (მობილური აპლიკაცია, ვებგვერდი და ელექტრონული ფოსტა),
მიმდინარეობდა. 2020 წელს სახელმწიფო ინსპექტორის სამსახურმა დაადგინა 123 ფაქტი პერსონალურ მონაცემთა არაკანონიერი დამუშავებისა. ყველაზე ხშირი იყო მონაცემთა უსაფრთხოების დაცვის მოთხოვნათა შეუსრულებლობა,რაც გამოწვეული იყო დაწესებულებათა მიერ მიღებული ზომების შეუსაბამობასთან მონაცემთა დაცვის უსაფრთხოებისთვის. ასევე, ბევრი შემთხვევა იყო, როდესაც მონაცემები კანონით გათვალისწინებული საფუძვლების და შესაბამისი პრინციპების დარღვევით დამუშავდა. 2020 წელს სახელმწიფო ინსპექტორის სამსახურმა ასევე დეტალურად შეისწავლა ელექტრონულ ბაზებში მონაცემების დამუშავების 40 შემთხვევა [68]. შესწავლილმა პროცესებმა გამოავლინა შემდეგი სახის დარღვევები :

[68] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში 2020წ ;

- „საჯარო და კერძო დაწესებულებებს, როგორც წესი, არ აქვთ შემუშავებული წერილობითი დოკუმენტი, რომლითაც რეგულირდება დანერგილი ელექტრონული ბაზის ფუნქციონირების საკითხები...
- მონაცემთა დამმუშავებლები თანამშრომლებს არ აწვდიან ინფორმაციას და არ უზრუნველყოფენ მათ გადამზადებას მონაცემთა დამუშავების პროცედურულ და შინაარსობრივ საკითხებზე...
- არ აღირიცხება ბაზებში არსებულ მონაცემთა მიმართ შესრულებული მოქმედებები....
- დაწესებულებები ნაკლებ ყურადღებას აქცევენ ელექტრონულ ბაზებში არსებული მონაცემების სიზუსტეს და მონაცემთა ბაზებს პერიოდულად არ აახლებენ...
- ხშირ შემთხვევაში, ორგანიზაციებს არ აქვთ განსაზღვრული მონაცემთა შენახვის ვადები. ელექტრონულ ბაზებში მონაცემები არ კლასიფიცირდება მათი შინაარსისა და დამუშავების მიზნის მიხედვით. შესაბამისად, მონაცემები ინახება და, რიგ შემთხვევებში, საჯაროვდება მას შემდეგაც, რაც უკვე მიღწეულია მონაცემთა დამუშავების მიზანი“[69]

ამ დარღვევების საპასუხოდ სახელმწიფო ინსპექტორის სამსახურმა გასცა რეკომენდაციები და იგი აგრძელებს განვითარებას და დგამს ნაბიჯებს ეფექტიანობის ასამაღლებლად. ასევე საინტერესოა სახელმწიფო ინსპექტორის 2015 წლის ანგარიშიდან ერთი შემთხვევა, კერძოდ :

2015 წელს ინსპექტორს რეაგირებისთვის მიმართა მოქალაქემ, რომელიც ამბობდა, რომ ერთ-ერთმა მიკროსაფინანსო ორგანიზაციამ მისი თანხმობის გარეშე გადაამოწმა მონაცემები სს „კრედიტინფო საქართველოს“ მონაცემთა ბაზაში. გარემოებების გამოკვლევის შემდგომ დადგინდა, რომ მიკროსაფინანსო ორგანიზაციას მოქალაქის თანხმობა გააჩნდა მხოლოდ საკრედიტო ხელშეკრულების საფუძველზე მონაცემთა დამუშავების შესახებ სასესხო ურთიერთობის ფარგლებში ჰქონ-

[69] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში 2020წ;.ბოლო გადამოწმების თარიღი: [09.09.2020]

და მოპოვებული, მაგრამ როდესაც სესხის ხელშეკრულებას ვადა გაუვიდა და სასესხო ვალდებულებაც ამოიწურა, მიკროსაფინანსო ორგანიზაციამ, ახალი საკრედიტო პროდუქტის შეთავაზების მიზნით, აღნიშნული პირის პეროსნალური მონაცემები კვლავ გადაამოწმა მოქალაქის თანხმობის გარეშე. ინსპექტორმა აღნიშნულ ფაქტზე მსჯელობისას დადგინდა, რომ მიკროსაფინანსო ორგანიზაცია გასცდა მოქალაქის თანხმობით მინიჭებულ უფლებამოსილებას და დაარღვია კანონის მოთხოვნები, რადგან მას არ ჰქონდა მონაცემთა დამუშავების შესაბამისი საფუძველი თანხმობის სახით. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა სუბიექტის თანხმობას განმარტავს, როგორც : „მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე ზეპირად, სა ტელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით გამოხატული ნებაყოფლობითი თანხმობა, რომლითაც შესაძლებელია ნათლად დადგინდეს მონაცემთა სუბიექტის ნება“[70]

ასევე ინსპექტორმა აღნიშნა იმისთვის, რომ მონაცემთა სუბიექტი სათანადოდ იყოს ინფორმირებული მონაცემთა დამუშავების შესახებ თანხმობის გაცემის მიზნისა და შედეგების თაობაზე, აუცილებელია მას ნების გამოვლენამდე მიეწოდოს ნათელი და მკაფიო ინფორმაცია იმის შესახებ, თუ რა მიზნით შეიძლება დამუშავდეს მისი მონაცემები. მხოლოდ ასეთი ინფორმაციის მიღების შემდგომ გამოვლენილი ნება შეიძლება იქნას მიჩნეული მონაცემთა დამუშავების საფუძვლად.[71]

როგორც უკვე აღვნიშნეთ, საქართველოს კანონი „პერსონალურ მონაცემთა შესახებ“ ზედმეტად ვიწროა და მხოლოდ საქართველოზეა მორგებული. აუცილებელია კანონის დახვეწა და ევროკავშირის სტანდარტებთან მიახლოება, რაც საქართველოს მოქალაქეებს პირადი მონაცემების არკანონიერი დამუშავებისგან დაიცავს.

[70] “პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლი „ზ“ ქვეპუნქტი, N5669- რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

[71] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში 2015წ;.ბოლო გადამოწმების თარიღი: [09.09.2020]

6. დასკვნა

ნაშრომში განხილული ძირითადი საკითხები ემსახურებოდა პერსონალურ მონაცემთა დაცვის, როგორც ადამიანის ძირითადი უფლებების მნიშვნელობას და მის საზოგადოებრივ დანიშნულებას.

აღნიშნული კვლევიდან ნათლად დავინახეთ, რომ საქართველოს კანონმდებლობა პერსონალურ მონაცემთა დაცვის შესახებ ჯერ კიდევ ძალიან შორსაა ევროპული სტანდარტებისგან და იგი დახვეწას საჭიროებს. თუმცა, ევროკავშირის მაგალითების მომიხილვითაც გამოჩნდა, რომ არც სხვა ქვეყნები არიან ჯერ ბოლომდე ჩამოყალიბებულნი. GDPR ევროკავშირის ტერიტორიაზე სულ რამდენიმე წლის წინ შევიდა ძალაში და ჯერ მხოლოდ ერთი- საფრანგეთის საქმეა მის ფარგლებში განხილული რომლითაც „Google“ დააჯარიმა და ალბათ ჯერ კიდევ ძალიან შორია იმაზე საუბარი, თუ რა შედეგებს მოიტანს ევროკავშირის რეგულაცია მოსახლეობისთვის. როგორც ვნახეთ GDPR-ც დგას პრობლელმებისა და გამოწვევების წინაშე, რომლის გადაჭრაც ალბათ დროის საკითხია და შესაძლებელია ოდესღაც ეს რეგულაციაც დავიწყებას მიეცეს და სხვა ახალი რეგულაციით ჩანაცვლდეს ან სულაც მოდიფიცირება განიცადოს ტექნოლოგიური პროგრესის კვალდაკვალ.

ევროკავშირისთვის უძვირფასესია საკუთარი მოქალაქეების პერსონალური მონაცემების დაცვა და იგი ყველაფერს ცდილობს,რათა დაიცვას პერსონალური მონაცემების კონფიდენციალურობა. კვლევისას გამოჩნდა რომ სახელმწიფოები, მათ შორის საქართველოც არასწორად აღიქვამენ და ბოლომდე ვერ ითავისებენ

პერსონალური მონაცემების მნიშვნელობას ვერ განსაზღვრავენ პრიორიტეტულად. სწორედ ამიტომ,პერსონალურ მონაცემთა დაცვის საკანონმდებლო ბაზის ჰარმონიზაცია წარმოადგენს საქართველოს მიერ ევროკავშირთან 2014 წელს დადებული ასოცირების შეთანხმებითა ნაკისრ ერთ-ერთ უმნიშვნელოვანეს ვალდებულებას.

აღნიშნული კვლევისას დავინახეთ, რომ საქართველოშიც პერსონალური მონაცემების დაცვის სტანდარტი შედარებით ამაღლდა ბოლო წლების განმავლობაში, განსაკუთრებით, პერსონალური მონაცემების დაცვის ინსპექტორის თანამდებობის დანერგვის შემდეგ. თუმცა, ამ სფეროში კვლავაც რჩება გარკვეული პრობლემები და გამოწვევები. ამ გამოწვევების საპასუხოდ კი აუცილებელია საკანონმდებლო დონეზე აღმოიფხვრას ხარვეზები, რათა პერსონალური მონაცემების, დაცვის სტანდარტი და გარანტიები უფრო გამყარდეს.

როგორც კვლევაში აღვნიშეთ, საქართელოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“ საერთოდ არ არის მორგებული საერთაშორისო რეალობას და მისი მთავარი მიზანია საქართველოს ტერიტორიაზე გააკონტროლოს პერსონალური მონაცემების დაცვა, ხოლო ევროკავშირთან ინტეგრაციის პროცესში არსებული სამართლებრივი ურთიერთობიდან გამომდინარე კი საქართველოს საწარმოებისათვის ახლა განსაკუთრებით მნიშვნელოვანია ევროკავშირის კანონმდებლობასათან ჰარმონიზებული საკანონმდებლო ბაზის საფუძველზე საქმიანობის წარმართვა, რათა მათ საქმიანობას ევროკავშირის ტერიტორიაზე უფრო მეტად შეეწყოს ხელი.

ამიტომ აუცილებელია იმგვარი ახალი საკანონმდებლო აქტის მიღება, რომელიც ერთი მხრივ, სრულად გაითვალისწინებს ევროკავშირის კანონმდებლობის

მოთხოვნებს, ხოლო მეორე მხრივ კი უზრუნველყოფს გამჭვირვალე სამართლებრივი რეგულაციების შემოღებას, პერსონალურ მონაცემთა დაცვის საერთაშორისოდ აღიარებული პრინციპების რეალიზაციასა და საუკეთესო პრაქტიკის დამკვიდრებას. აუცილებელია „დავიწყების უფლება „ გაიწეროს ჩვენს კანონში,რათა მაქსიმალურად მოვახდინოთ ევროკავშირის კანონმდებლობასთან ჰარმონიზაცია.

ასევე აუცილებლად უნდა გაიზარდოს პერსონალური მონაცემების საზედამხედველო ორგანოს გამჭვირვალობა და ანგარიშვალდებულება და კანონმდებლობა იყოს ჩვენი მოქალაქეების პერსონალური მონაცემების დაცვაზე მაქსიმლურად ორიენტირებული და მორგებული.

კვლევისას განვიხილეთ სახელმწიფო ინსპექტორის სამსახურის აპარატი, რომელიც სულ რამდენიმე წელია გამოჩნდა საქართველოში და ამ მოკლე დროში ძალიან დიდი საქმე გააკეთა ჩვენი მოქალაქეების პერსონალური მონაცემების დაცვის კუთხით და ასევე ინსპექტორის ანგარიშების გამოკვლევისას ნათელი გახდა, რომ მონაცემთა სუბიექტებს ზოგ შემთხვევაში ინფორმაციაც კი არ აქვთ იმის შესახებ,თუ რა უფლებები ენიჭებათ მათ და რა საშუალებებით შეუძლიათ დაიცვან საკუთარი უფლებები. ასევე ნათლად გამოჩნდა ისიც, რომ დამმუშავებელი ორგანიზაციები უხეშად არღვევენ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით გათვალისწინებულ მოთხოვნებს და უფრო მეტ უფლებებს ანიჭებენ საკუთარ თავს ვიდრე მათ ეს რეალურად კნონით აქვთ მინიჭებული.

კონფიდენციალურობის უფლება არის ყველა ადამიანისთვის ისევე მნიშვნელოვანი, როგორც სიცოცხლის,თავისუფალი განვითარების, გამოხატვის უფლება, ამიტომ ადამიანები და კომპანიები ორმხრივად უნდა იაზრებდნენ თუ რას გასცემენ და რას იღებენ სანაცვლოდ. ევროკავშირმა შეძლო რომ არ ჩამორჩენოდა ტექნოლოგიური განვითარების ეტაპებს და ფეხი აუწყო მას საკუთარი სტანდარტების შექმნით, ამდენად, მნიშვნელოვანია რომ

საქართველომაც გადადგას ნაბიჯი კანონმდებლობის დახვეწის კუთხით და სწორედ პერსონალური მონაცემების დაცვის მაღალი სტანდარტებით გადადგას ნაბიჯი ევროკავშირში გაწევრიანებისკენ.

ბიბლიოგრაფია

გამოყენებული სამართლებრივი წყაროები :

- პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011;
- General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2016 წლის 24 მაისს);
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, (მიღებულია 1981 წლის 28 იანვარს, ძალაში შევიდა 1985 წლის 1 ოქტომბერს);
- საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით [1995];
- ასოცირების შესახებ შეთანხმება ერთის მხრივ, საქართველოსა და მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის, საქართველოს საკანონმდებლო მაცნე, 27.06.2014;
- 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი -CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]- Draft explanatory report;
- ქარტია ევროპის კავშირის ფუნდამენტური უფლებების შესახებ, (მიღებულია 2000 წლის 2 ოქტომბერს, ძალაში შევიდა 2000 წლის 7 დეკემბერს);

- კანონპროექტი : „პერსონალურ მონაცემთა დაცვის შესახებ“ 2019წ ;

- „საქართველოს ზოგადი ადმინისტრაციული კოდექსი“;
- „კომერციული ბანკების საქმიანობის შესახებ“ საქართველოს კანონი;
- საქართველოს სამოქალაქო კოდექსი;
- პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიში;
- პერსონალურ მონაცემთა დაცვის ინსპექტორის 2020 წლის ანგარიში;

გამოყენებული ლიტერატურა :

- მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო,2018 წ.

- პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაცია : „რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ

- The main differences between the DPD and the GDPR and how to address those moving forward

- პერსონალურ მონაცემთა დაცვის ახალი რეალობა ევროპაში - საჯარიმო სანქციები GDPR -ის ამოქმედების შემდეგ, 2019 წ.

- Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions,2018

- საქმე Case C-131/12. Google Spain vs AEPD and Mario Costeja Gonsalez [2014]

- საქმე C-101/01, Criminal proceedings against Bodil Lindqvist, 2003 წლის 6 ნოემბერი (იხ.https://curia.europa.eu/juris/liste.jsf?num=C-101/01)