კავკასიის საერთაშორისო უნივერსიტეტი

ლუკა კორძაია

პერსონალურ მონაცემთა დაცვა კიბერ სივრცეში

სამართლის ფაკულტეტი

სამაგისტრო ნაშრომი შესრულებულია სამართლის მაგისტრის
აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: ხათუნა ბურკაძე

ასოც. პროფესორი, სამართლის დოქტორი

თბილისი, 2019

ანოტაცია

საქართველოს კანონმდებლობა არ არეგულირებს ციფრულ სამყაროში წარმოშობილ დავებს, არ განმარტავს ვალდებულებებს და არ ადგენს იმ აუცილებელ ნორმებს, რაც უნდა შეასრულონ ფიზიკურმა და იურიდიულმა პირებმა პერსონალურ მონაცემთა დასაცავად.

აღნიშნული ნაშრომი მიმოიხილავს ამერიკის შეერთებულ შტატებში არსებულ მდგომარეობას პერსონალურ მონაცემთა დაცვის შესახებ, რომლითაც, სახელმწიფო ცდილობს, რომ მაქსიმალურად დაიცვას ადამიანების პერსონალური ინფორმაცია კიბერ სივრცეში და გაგაცნობთ საკითხთან დაკავშირებულ გახმაურებულ, მნიშვნელოვან საქმეებსა და სასამართლო გადაწყვეტილებებს.

ასევე, კვლევა მიმოიხილავს ევროკავშირის სპეციალურ რეგულაციებს, როგორიცაა „ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია“ (GDPR) და კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ. ცალკეული ქვეყნების შიდა სახელმწიფოებრივი კანონები, რომლებიც ცდილობენ, რომ ჩამოაყალიბონ კიბერ სივრცეში პერსონალურ მონაცემთა დაცვის მექანიზმები. როგორ ცდილობს ევროკავშირი ჰარმონიზაციას მონაცემთა დაცვის ზოგადი რეგულაციით.

ნაშრომის მიზანია, რომ შევისწავლოთ სხვა ქვეყნებში არსებული მდგომარეობა და ვნახოთ, შესაძლებელია თუ არა საქართველოში იგივე ან მსგავსი ქმედებების განხორციელება. რა თქმა უნდა შეუძლებელია რეგულაციების პირდაპირ გადმოტანა, ამიტომ არის მნიშვნელოვანი ჯერ მათი შესწავლა, ანალიზი და საქართველოს კანონმდებლობაზე მორგება.

Luka Kordzaia

Protection of Personal Data in Cyberspace

Annotation

Georgian legislation does not regulate disputes arising in cyberspace, does not define the obligations and set the necessary regulations for persons and/or firms on how to protect the personal data.

Thesis reviews the personal data protection regulations in United States of America, with which the state is trying to thoroughly protect the personal data of individuals in cyberspace and introduce you to the famous and important court cases and decisions.

The paper also reviews the regulations throughout the European Union, such as General Data Protection Regulation and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Different states inside the EU have different sets of rules regarding the personal data protection.

The goal of my thesis is to acquire the knowledge about the situation around the data protection in technologically and legislatively advanced countries. Is it possible to repeat the same in Georgia? Of course, it is impossible to blindly copy the regulations, disregarding the reality and situation in the specific countries. That is why it is important to first study and analyze them and then think about converting in Georgian legislation.

სარჩევი

1. შესავალი

პერსონალურ მონაცემთა დაცვა ყოველთვის წარმოადგენდა პრობლემატურ საკითხს კანონმდებლებისთვის. მაშინაც კი, როდესაც ინტერნეტი და კიბერ სამყარო საერთოდ არ არსებობდა, რთული იყო დაცვითი მექანიზმების შექმნა, რომლითაც საზოგადოების თითოეული წევრი თავს იგრძნობდა უსაფრთხოდ. ისედაც კომპლექსურად დასარეგულირებელი საკითხი, კიდევ უფრო რთული გახდა ინტერნეტის შექმნასთან ერთად. კიბერ სივრცის განვითარებასთან ერთად კი, უფრო რთული და კომპლექსური გახდა კომპანიების კონტროლი მონაცემთა დამუშავების შესახებ.

კიბერ სივრცის უსაფრთხოების მიზანია, რომ მილიონობით ადამიანის პირადი ინფორმაციის შენახვა მოხდეს დაცულად. არ გავრცელდეს ის სხვადასხვა საშუალებებით. ადამიანის ციფრული კვალი ინახება ყველგან და ყოველთვის, საიტებზე შესვლის დროს, რეგისტრაციის გავლის დროს, ბარათის დეტალების შეყვანის დროს, ელექტრონული ფოსტის მისამართის გაცემის დროს, სოციალურ ქსელში სურათის ატვირთვის ან ბოლო წლებში პოპულარულ ე.წ. ღრუბლოვან საცავში (Cloud Storage) ინფორმაციის შენახვის დროს. ნებისმიერი ნაბიჯი არის საკუთარი პერსონალური ინფორმაციის გავრცელება კიბერ სივრცეში და ჩნდება კითხვები: ვინ არის ან უნდა იყოს პასუხისმგებელი ამ ინფორმაციაზე? ვის შეიძლება, რომ ჩაუვარდეს ხელში ადამიანის ინფორმაცია, თქვენ და სერვის პროვაიდერის გარდა?

90-იანი წლების მიწურულს, როდესაც საქართველოს სახელმწიფომ დაიწყო საკუთარი კანონმდებლობის ჩამოყალიბება, სამართლებრივი სფეროს შექმნა და პირველი ნაბიჯების გადადგმა სახელმწიფოებრივი წყობის ჩამოსაყალიბებლად, პერსონალურ მონაცემთა დაცვა არ იყო კონცენტრაციის მთავარი ობიექტი და მხოლოდ 2011 წელს მიიღო საქართველოს პარლამენტმა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი. მიუხედავად იმისა, რომ კანონი გამოიცა და

ძალაში შევიდა 21-ე საუკუნის შუაში, მასში ნაკლებად არის მოხსენიებული კიბერ სივრცეში გავრცელებული მონაცემების დაცვის მექანიზმები, ვის შეიძლება, რომ დაეკისროს პასუხისმგებლობა სხვისი მონაცემების გავრცელებისთვის. თითქოს ის ვრცელდება კიბერ სივრცეზეც, მაგრამ ტერმინების ნაკლებობა და სამართლებრივი დავების სიმწირე, ბუნდოვანებას ტოვებს საქართველოს კანონმდებლობაში.

ნაშრომის მთავარი მიზანია, რომ გამოიკვლიოს რეალური გზები, თუ როგორ შეიძლება საქართველოში განვითარდეს და დაიხვეწოს მოქმედი კანონმდებლობა პერსონალურ მონაცემთა დაცვის შესახებ, რადგან დღევანდელი რეგულაციებით, სახელმწიფოში არ არსებობს მოქალაქეთა დაცვის მექანიზმები კიბერ სივრცეში. შესაბამისად, მნიშნველოვანია განვითარებული ქვეყნების განსხვავებული მიდგომების შესწავლა, როგორ არეგულირებს ევროკავშირი და ცალკეულად, როგორ უყურებს პერსონალურ მონაცემთა დაცვის საკითხს აშშ. კვლევის შედეგად გამოიკვეთა, რომ ევროკავშირისა და აშშ-ს კანონმდებლებს მუდმივად უწევთ ერთმანეთთან თანამშრომლობა, რადგან მონაცემთა ბაზები, ხშირ შემთხვევაში, ინახება სხვადასხვა ქვეყნებში და მნიშნველოვანია მათი ერთად მუშაობა. ხოლო ეს თანამშრომლობა საკმაოდ რთულია, რადგან აშშ-ს დამოკიდებულება პერსონალურ მონაცემთა დაცვის შესახებ არ არის ისეთივე მკაცრი, როგორიც ევროკავშირის.

ნაშრომში განხილულია ევროკავშირის სპეციალურ რეგულაციები, როგორიცაა „ევროკავშირის მონაცემთა დაცვის რეგულაცია“ (GDPR) და დირექტივა პერსონალურ მონაცემთა დაცვის შესახებ. რა განსხვავება ევროკავშირის რეგულაციებსა და აშშ-ს კანონმდებლობას შორის და რამდენად არის შესაძლებელი და გამართლებული ასეთი სახის რეგულაციების იმპლემენტაცია საქართველოში.

რა თქმა უნდა, თითოეულ ქვეყანას აქვს საკუთარი მიდგომა კიბერ სივრცეში პერსონალურ მონაცემთა დაცვისადმი და ზოგს უკვე მრავალწლიანი გამოცდილებაც დაუგროვდა, მაგრამ შეუძლებელია სხვა სახელმწიფოს რეგულაციების ბრმად გადმოტანა საქართველოს კანონმდებლობაში.

პერსონალური მონაცემების დაცვის გარკვეული მექანიზმები საქართველოში ამოქმედდა 2011 წლიდან და მას შემდეგ მიმდინარეობს კანონის დახვეწა. მაგრამ, თავისუფლად შეგვიძლია იმის თქმა, რომ ეს სფერო არის საკმაოდ ახალი გამოწვევა სახელმწიფოსთვის და მხოლოდ ბოლო ორი-სამი წელია, რაც აქტიურად დაიწყო მუშაობა პერსონალურ მონაცემთა დაცვის შესახებ სხვადასხვა პროექტებზე. აქედან გამომდინარე, ქართული ლიტერატურა თითქმის არ არსებულია, ასევე არ მოიძებნება ქართული სასამართლოების პრეცედენტი პერსონალურ მონაცემებთან დაკავშირებით და შეუძლებელია, მხოლოდ საქართველოში არსებულ ვითარებაზე საუბარი, შესაბამისად სამაგისტრო ნაშრომი მიმოიხილავს უცხოურ ლიტერატურას, აკეთებს სხვადასხვა ქვეყნების კანონმდებლობების შედარებას და სისტემურ ანალიზს.

2. პერსონალურ მონაცემთა დაცვის საწყისები

თუ გვსურს, რომ დავიწყოთ კვლევა პერსონალურ მონაცემთა დაცვის შესახებ კიბერ სივრცეში, საჭიროა იმის გაგება, რას წარმოადგენს ინდივიდის პერსონალური მონაცემები, რატომ არის მისი უსაფრთხოება მნიშვნელოვანი და როგორ დაიწყეს განვითარებულმა სახელმწიფოებმა მასზე ზრუნვა. მნიშვნელოვანია იმის გამოკვლევა თუ რა შეცდომები დაუშვეს მათ გზა და გზა და რის განმეორება შეგვიძლია, რომ ავირიდოთ თავიდან ციფრულ ინფორმაციულ ხანაში. მაგრამ, პირველ რიგში, სანამ განვიხილავთ ტექნოლოგიურ სამყაროსთან არსებულ პრობლემებს, მნიშვნელოვანია იმის გააზრება, თუ ზოგადად რას წარმოადგენს პერსონალური მონაცემები, როგორ განმარტავენ მას სხვადასხვა სახელმწიფოები და რატომ არის ადამიანის კონფიდენციალურობის დაცვა მნიშვნელოვანი. მხოლოდ ამის შემდეგ გახდება იმის გააზრება შესაძლებელი, თუ რა სახის ახალი გამოწვევები შექმნა, ბოლო 20 წლეულში, საინფორმაციო ტექნოლოგიების განვითარებამ.

2.1. რას მოიცავს პერსონალური მონაცემები

ინდივიდის პერსონალური მონაცემი მოიცავს ყველაფერს, საიდანაც შეიძლება ამ პირის გამომჟღავნება.[1] საქართველოს კანონი პერსონალურ მონაცემს განმარტავს შემდეგნაირად:

„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."[2]

[1] An Introduction to Data Protection, Edited by EDRi and Digital Caurage, Germany, 2012, 4.

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

ასეთი ტიპის მონაცემების მარტივ მაგალითებად შეგვიძლია მივიჩნიოთ სახელი, მისამართ, პირადი ნომერი, სურათი და ა.შ., რაც აშკარად კვეთს პირის იდენტიფიცირების საშუალებას.

ევროკავშირის მიერ, 2018 წელს მიღებული „მონაცემთა დაცვის ზოგადი რეგულაციაც“-ც აკეთებს პერსონალური მონაცემების მსგავს განმარტებას. მთავარი არის, რომ შესაძლებელი იყოს პირის იდენტიფიცირება, მიღებული მონაცემების საშუალებით. თუ ეს მონაცემები არის გარკვეულ წილად დაფარული ან შემცირებული და ამით ვერ გამოიკვეთება კონკრეტული პირი, მაშინ ის აღარ ჩაითვლება პერსონალურ მონაცემად.

იმავე სახის განმარტება გააკეთა პერსონალურ მონაცემზე, სტანდარტებისა და ტექნოლოგიის ნაციონალურმა ინსტიტუტმა, 2007 წლის გამოშვებულ მემორანდუმში და იგი აისახა აშშ პერსონალურ მონაცემთა დაცვის ოფიციალურ წინამძღვარში:

„ინფორმაცია, რომლითაც შეიძლება პირის იდენტიფიცირება, მაგალითად სახელი, სოციალური დაცვის ნომერი, ბიომეტრიული ჩანაწერი და ა.შ. ცალ-ცალკე ან სხვა პერსონალურ ან მაიდენტიფიცირებელ ინფორმაციასთან ერთად, რომელიც შეიძლება რომ დაუკავშირდეს კონკრეტულ პიროვნებას, მაგალითად დაბადების თარიღი, ადგილი, დედის სახელი და ა.შ.“[3]

მაგრამ პერსონალური მონაცემის ცნება გააფართოვა ინტერნეტის განვითარებამ და ის აღარ შეიძლება ჩაითვალოს, როგორც მხოლოდ ერთი კონკრეტული ინფორმაცია, რომელიც ავლენს პირის ვინაობას. კიბერ სივრცეში ადამიანის პერსონალური მონაცემის შეგროვება შესაძლებელია ბევრნაირად. ტექნოლოგიურ სამყაროში, ადამიანები გაუაზრებლად, ზედმეტი დაკვირვების გარეშე ავსებენ ფორმებს, აძლევენ საიტებს საკუთარი ინფორმაციების შენახვის უფლებას, არასდროს

[3] National Institute of Standards and Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), C-1; იხ. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.

არ აკვირდებიან საიტების წესებს და პირდაპირ ეთანხმებიან მას. მაგალითად რომ მოვიყვანოთ, საძიებო სისტემების ლიდერი და გიგანტური ტექნოლოგიური კომპანია - “Google” (გუგლი), შეუმჩნეველი გაფრთხილების საფუძველზე, ნახულობს საიტზე შესული მომხმარებლის ლოკაციას, იმახსოვრებს ადამიანის მიერ საძიებო სისტემაში შეყვანილ ტექსტს, ნანახ საიტებს. შემდეგ, კომპანია ამუშავებს მიღებულ ინფორმაციას და აძლევს მესამე პირებს ამ ინფორმაციის ყიდვის საშუალებას ე.წ. მორგებული რეკლამისთვის. ასეთი ტიპის ინფორმაციამ შეიძლება არ გამოავლინოს პირის სახელი და გვარი, მაგრამ ის ავლენს სხვა დეტალებს, როგორიცაა პირის ინტერესის სფერო, ადგილმდებარეობა და ა.შ., რაც თავისუფლად შედის ადამიანის პერსონალურ მონაცემებში.

თუ მომხმარებელს გუგლში შეუძლია საკუთარი სახელისა და სხვა მაიდენტიფიცირებელი პერსონალური ინფორმაციის გამხელისგან თავის არიდება, ასეთ შესაძლებლობას არ იძლევიან სოციალური ქსელის გიგანტები, რომელთა ბიზნეს გეგმა მთლიანად ადამიანთა პერსონალურ მონაცემებზეა აწყობილი. ასევე, შეგვიძლია ვისაუბროთ ისეთ საიტებზე, რომლებიც ინახავენ არამარტო ადამიანის სახელსა და გვარს, არამედ ისეთ მგრძნობიარე ინფორმაციასაც, როგორიცაა ბანკის ანგარიშის ნომრები ან ადამიანის პირადი ნომრები.

შესაბამისად, ინტერნეტის ბაზა გრანდიოზულია, მომხმარებელთა რაოდენობა კი ყოველდღიურად იზრდება. ადამიანის პერსონალური მონაცემები კი იქცა ძალიან დიდ და ძვირად ღირებულ იარაღად კომპანიების ხელში, რომლითაც მათ შეუძლიათ, რომ აკონტროლონ ყველაფერი ადამიანის შესახებ და ივაჭრონ ამ ინფორმაციით. ამიტომ არის მნიშვნელოვანი იმის გარკვევა, თუ როგორ ცდილობენ კომპანიები ამ ინფორმაციის დაცვას და რას აკეთებენ სახელმწიფოები, რომ დაიცვან საკუთარი მოქალაქეების ინტერესები კიბერ სივრცეში.

2.2. პერსონალურ მონაცემთა დაცვა, როგორც აქტუალური პრობლემა

საქართველომ, შეიძლება გვიან დაიწყო მოცემულ საკითხზე ზრუნვა, მაგრამ პერსონალურ მონაცემთა დაცვა, მსოფლიოს უფრო თავისუფალ და განვითარებულ ქვეყნებში, აქტუალურ პრობლემად იქცა ჯერ კიდევ 20-ე საუკუნის 70-იან წლებში. რა თქმა უნდა, მანამდეც არ ედო ტაბუ პერსონალურ მონაცემთა დაცვას ევროპულ ქვეყნები და თვლიდნენ, რომ ადამიანთა პერსონალური მონაცემები მნიშვნელოვანი საზრუნავი იყო, მაგრამ მხოლოდ 1970-იან წლებში დაიწყო მონაცემთა დაცვის გამოყოფა, როგორც ცალკეული კატეგორია სამართლებრივ დისკუსიებსა და პრაქტიკაში[4], შესაბამისად, არც ევროკავშირის კომისიები არ ფიქრობდნენ ამ საკითხის მიმართებით დირექტივებისა და მინიმალური რეგულაციების შემუშავებაზე.

1970 წელს, გერმანიამ გადადგა პირველი ნაბიჯი და შეიმუშავა კანონი მონაცემთა დაცვის შესახებ. ამას მოყვა შვედეთის კანონი 1973 წელს და შემდეგ უკვე ქვეყნების დიდმა ნაწილმა დაიწყო მონაცემთა დაცვის შესახებ კანონებზე მუშაობა.[5] ეს იყო პერიოდი, როდესაც ნელ-ნელა შესაძლებელი ხდებოდა მონაცემთა დამუშავება და შენახვა ტექნოლოგიურ დონეზე, მაგრამ ჯერ კიდევ ნაადრევი იყო საუბარი მის გაცვლასა და სხვა შესაძლებლობებზე.

პერსონალურ მონაცემთა დაცვის შესახებ, საჭირო რომ იყო რეგულაციებისა და დირექტივების შემუშავება, ევროკავშირმა ორი მსოფლიო მოვლენისგან გაიაზრა. პირველი ფაქტი მოხდა საფრანგეთში, სადაც, 1978 წელს გამოქვეყნდა და ძალაში შევიდა „მონაცემთა დაცვისა და თავისუფლების კანონი“.[6] საფრანგეთის პარლამენტის მიერ მიღებული კანონი კრძალავდა, ნებისმიერი კომპანიის ან სახელმწიფო სამსახურის მხრიდან ფიზიკური პირის პერსონალური მონაცემის მიღებასა და დამუშავებას ნებართვის გარეშე. ამის საწინააღმდეგო ქმედება კი, იყო დასჯადი - ექვსი

[4] Katrin N.M., The Right to Privacy as a Human Right and Everyday Technologies, Legal Aspects of Privacy Law and Data Protection, 83.
[5] იქვე, 84.
[6] M. Guiness, France Maintains Long Tradition of Data Protection, იხ <https://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711> [26.01.2011].

თვით თავისუფლების აღკვეთა ან 20 000 ფრანკის, ანუ 3 000 ევროს ანაზღაურება.[7] ამასთან ერთად, საფრანგეთის კანონი იყო პირველი მაგალითი, რომელიც შედარებით კონკრეტულად განმარტავდა თუ რას მოიცავს პერსონალური მონაცემები და როგორ შეიძლება მათი დაცვა. საფრანგეთის კანონი იყო საპასუხო ქმედება, სახელმწიფოში დამდგარი, სერიოზული პრობლემისთვის, რომელსაც ვერ გაექცა ქვეყანა: საფრანგეთის მთავრობაში დამკვიდრებული იყო საკუთარი მოქალაქეების შესახებ პერსონალური ინფორმაციის სისტემატიური და უხეში დარღვევა და ინფორმაციის საიდუმლოება აღარ იყო მნიშნველოვანი მათთვის. მეორე მოვლენა, რის გამოც ევროკავშირმა დაიწყო პერსონალურ მონაცემთა დაცვაზე ფიქრი, იყო ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის მიერ გამოშვებული, ოფიციალური „სახელმძღვანელო პირადი მონაცემების დაცვა და მათი ტრანსასაზღვრო მოძრაობა“.[8]

სწორედ ამას შეგვიძლია, რომ დავარქვათ პირველი ნაბიჯების გადადგმა და აღიარება ევროპაში, რომ ადამიანთა პერსონალურ მონაცემთა უსაფუძვლო და შეუთანხმებელი დამუშავება იყო სერიოზული დანაშაული და არამარტო კერძო კომპანია, არამედ სახელმწიფო ორგანოებიც არ იყვნენ უფლებამოსილნი, რომ ნებართვის გარეშე განეხორციელებინათ აღნიშნული საქმიანობა. გერმანიის, შვედეთისა და საფრანგეთის ქმედებების შემდეგ, 1981 წელს, ევრო საბჭომ შეიმუშავა პირველი საერთაშორისო კონვენცია “ინდივიდების დაცვა პერსონალური მონაცემების ავტომატური დამუშავებისგან“. ევროპის საბჭოს მიერ შემუშავებული კონვენცია გარკვეულწილად არეგულირებდა არამარტო შიდა სახელმწიფოების ქმედებებს, არამედ ცდილობდა პერსონალურ მონაცემთა საზღვრებს შორის გაცვლის შესაძლებლობის მოგვარებასაც. კონვენციამ, ხელმომწერი სახელმწიფოების მოქალაქეებს მისცა უფლება, რომ მათ იცოდნენ ნებისმიერი ინფორმაციის შესახებ,

[7] იქვე.
[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

რომელიც ინახება და საჭიროებისამებრ, მოითხოვონ მათი შეცვლა ან საერთოდ წაშლა, თუ ეს შესაძლებელია.[9]

მაგრამ 1970-80-იანი წლებისთვის, სამყარო არ იყო ტექნოლოგიურად ისეთი განვითარებული, როგორიც არის ის დღეს და როგორიც გახდა ის 21-ე საუკუნის დასაწყისიდან, როდესაც ინტერნეტის რევოლუციამ მოიცვა ყველაფერი. აქედან გამომდინარე, მე-20 საუკუნეში შემუშავებული კანონები და საერთაშორისო ხელშეკრულებები მორგებული იყო იმ დროის რეალობასთან. სახელმწიფოთა შორის მონაცემთა გაცვლა და გავრცელება წარმოადგენდა ძალიან გრძელვადიან, შრომატევად და დატვირთულ სამუშაოს. მაგრამ, ეს მაინც შესაძლებელი იყო, ამიტომ, 1981 წლის რეგულაცია ემსახურებოდა შედარებით მარტივ მიზანს და ითხოვდა შესაბამისს შედეგსაც. მართალია, მაშინაც საჭირო იყო ასეთი რეგულაციებისა და დირექტივების შემუშავება, მაგრამ არა ისე, როგორი საჭიროც არის ის დღეს.[10]

ბოლო 20 წლეულის მანძილზე სრულიად შეიცვალა საინფორმაციო და საკომუნიკაციო ტექნოლოგიები. მათი არარეალური სისწრაფით განვითარების საფუძველი იყო, პირველ რიგში თავისუფლება და შემდეგ, ამ თავისუფლებაზე დაფუძნებული, კერძო სოციალური ქსელებისა და სხვა მონაცემთა გავრცელების შესაძლებლობის შექმნა. დღეს ყველაფერი სხვანაირადაა. კერძო იურიდიული კორპორაციები ფლობენ მონაცემთა ძალიან დიდ ბაზებს ინდივიდებზე. აქედან ზოგი ინფორმაცია მათ ხელში ხვდება პირდაპირი გზით, მაგალითად, როდესაც ადამიანი დებს საკუთარ ინფორმაციას სოციალურ ქსელ „ფეისბუქზე“ ან როგორც ზემოთ კვლევაშია ნახსენები, როდესაც ადამიანი ეძებს რამეს პოპულარულ საძიებო სისტემაში. ეს მონაცემები, ხშირ შემთხვევაში განუსაზღვრელი ვადით ინახება და გამოიყენება კომპანიებს შორის, მონაცემთა ვაჭრობის დროს. მულტინაციონალური ტექნოლოგიური კომპანიების დიდი ნაწილი ქმნის საკუთარ, შიდა ეთიკურ ნორმებსა

[9] 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), მუხლი 8.
[10] იხ. შენიშვნა 5, გვერდი 10-ე ნაშრომში.

და რეგულაციებს. რა თქმა უნდა, კომპანიები შეიძლება გახდნენ პასუხისმგებლები თუ ისინი არ დაემორჩილებიან სახელმწიფო რეგულაციებს, მაგრამ, როდესაც საუბარი გვაქვს ასეთი ტიპის კორპორაციებზე, რთული ხდება მართლმსაჯულების აღსრულება განსჯადობის პრობლემატურობის გამო, სხვადასხვა სახელმწიფოში განსხვავებული ტიპის რეგულაციების გამო და როდესაც მონაცემთა ბაზების გაცვლა ხდება ქვეყნებს შორის, საკმაოდ რთული ხდება კანონმდებლობაში გარკვევა. საბოლოოდ, ტექნოლოგიური გიგანტების დიდი ნაწილი, საკუთარი ნების საფუძველზე ექცევიან ეთიკური ნორმების ქვეშ. მაგალითად, თუ შევხედავთ ამერიკის შეერთებულ შტატებს, რომელზეც ცალკე დეტალურად იქნება ნაშრომში საუბარი, აშშ-ს მხრიდან შექმნილი კანონმდებლობა, სექტორებად ყოფს ბიზნესებს და პერსონალურ მონაცემთა დაცვის რეგულაციებიც განსხვავებულია და ერგება კონკრეტულ სფეროს. ესეთი მიდგომა დიდ ხარვეზებს აჩენს კანონმდებლობაში და საშუალებას აძლევს აშშ-ში რეგისტრირებულ და მოღვაწე მონაცემთა მაკონტროლებლებს, რომ დარჩნენ დაურეგულირებელნი. ეს კი, კომპანიების მხრიდან, მხოლოდ კეთილი ნების საფუძველზე თვით-რეგულაციის საშუალებას იძლევა.

პერსონალური მონაცემების განმარტება, მათი მოპოვება, დამუშავება და გავრცელება, მნიშვნელოვნად შეიცვალა მას შემდეგ, რაც სახელმწიფოებმა დაიწყეს ფიქრი ამ კონკრეტული სამართლებრივი კატეგორიის დარეგულირებაზე. ამასთან ერთად, საკომუნიკაციო ტექნოლოგიების ყოველდღიური განვითარება და კომპანიების საერთაშორისო სტატუსი, ნამდვილად არ უწყობს ხელს კანონმდებლებს, რომ შეიმუშაონ ერთიანი და ჰარმონიზებული ნორმები, რომლებიც საფუძვლიანად დაიცავენ ინდივიდის უფლებებს.

3. ევროკავშირის რეგულაციები, პრაქტიკა და პრობლემები

ევროპის საბჭოს მიერ მიღებული 1981 წლის კონვენციის შემდეგ, ევროკავშირმა დიდი მნიშვნელობა მიანიჭა პერსონალური მონაცემების დაცვას და მიიჩნია, რომ ეს არის ადამიანის ერთ-ერთი ფუნდამენტური უფლება. სწორედ ეს აღიბეჭდა ევროკავშირის მიერ მიღებულ 2000 წლის ქარტიის „ევროპული კავშირის ფუნდამენტური უფლებების“ მე-7 და მე-8 მუხლებში.[11] მიუხედავად იმისა, რომ დოკუმენტი ოფიციალურად 2009 წლიდან გახდა სავალდებულო ხელმომწერი სახელმწიფოებისთვის[12], მიზანი ნათელი იყო. ევროპის მიერ გამოვლილი ისტორიის შემდეგ, ტოტალიტარული რეჟიმების აღზევებისა და დამხობის ფონზე, ევროპის ლიდერი ორგანიზაციისთვის უაღრესად მნიშვნელოვანი იყო, რომ მაქსიმალურად მოეპოვებინა პოლიტიკოსებისა და ევროკავშირის ქვეყნების მოქალაქეების ნდობა, ხოლო პერსონალურ მონაცემთა დაცვა კი ერთ-ერთ მნიშვნელოვან საფახერუს წარმოადგენდა, ნდობის მოპოვების პროცესში.

1981 წლის კონვენცია “ინდივიდების დაცვისთვის პერსონალური მონაცემების ავტომატური დამუშავების“ შესახებ, სულ რამდენიმე წელიწადში გახდა უფუნქციო და გამოუსადეგარი, რადგან სწორედ ამ პერიოდში დაიწყო ინფორმაციული ტექნოლოგიების განვითარება და 90-იანი წლების დასაწყისიდან მნიშვნელოვნად შეიცვალა სამუშაო გარემო, როგორც სახელმწიფო ორგანოებისთვის, ასევე ინდივიდებისა და იურიდიული პირბეისთვის, ყველამ დაიწყო ინტერნეტის გამოყენება. ევროკავშირში მყოფი ქვეყნების მიერ, დროთა მანძილზე შემუშავებული რეგულაციები, ძალიან რომ არ ყოფილიყო აცდენილი და მომხდარიყო კანონების ერთგვარი ჰარმონიზაცია, 1995 წელს საბჭომ შეიმუშავა ახალი დირექტივა

[11] ქარტია ევროპის კავშირის ფუნდამენტური უფლებების შესახებ, (მიღებულია 2000 წლის 2 ოქტომბერს, ძალაში შევიდა 2000 წლის 7 დეკემბერს), მუხლი 7.
[12] Weiss M.A., Archick K., U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, 2016, 2.

„ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით“ (დირექტივა მონაცემთა დაცვის შესახებ).[13]

აღნიშნული დირექტივა იყო პირველი მცდელობა, რომ ევროკავშირს შეექმნა ზოგადი წესები, როგორც საჯარო, ასევე კერძო იურიდიული პირებისთვის, რათა დაეცვა ევროკავშირის მოქალაქეების პერსონალური მონაცემების დამუშავება და სახელმწიფოთა შორის გაცვლა. მაგრამ, მონაცემთა დაცვის შესახებ დირექტივას ჰქონდა ორი დიდი პრობლემა, ის ვერ ეწყობოდა აშშ-ში არსებულ სიტუაციას და დირექტივის გამოცემამდე და შემდეგაც, წარმოშობილი ტექნოლოგიური კომპანიების ძალიან დიდი ნაწილი სწორედ აშშ-ს ტერიტორიაზეა დაარსებული[14], რაც ავტომატურად ქმნიდა საფრთხეს ევროკავშირის მოქალაქეების უსაფრთხოებისთვის. ამას ემატებოდა აშშ-ს გაფუჭებული რეპუტაცია, როდესაც ჯულიან ასანჟის მიერ, 2013 წელს, საჯარო გახდა ნაციონალური დაცვის სააგენტოს ქმედებები, რაშიც სწორედ ამ კომპანიების მიერ მოპოვებულ მონაცემებს იყენებდა.[15] ევროკავშირი ძალიან მკაცრად უყურებს პერსონალურ მონაცემთა დაცვას, აღიარებას მას, როგორც ადამიანის ფუნდამენტურ უფლებას და შესაბამისად ცდილობს დაიცვას ის, როგორც ადამიანის სიცოცხლის უფლება, ხოლო აშშ-სთვის ამ უფლებაზე მეტად ადამიანის სხვა ფუნდამენტური უფლებები უფრო აინტერესებს, საკუთარი მოქალაქეებისთვის. აშშ, სოციალური გამოწვევებიდან გამომდინარე, მიიჩნევს, რომ მთავარი არის სიტყვის თავისუფლება, ხოლო პოლიტიკური გამოწვევებიდან კი მიიჩნევს, რომ მთავარია ეკონომიკური თავისუფლება და ესენი არ უნდა შეზღუდოს არავინ. პერსონალურ მონაცემთა კონფიდენციალურობის დაცვა კი თეორიულად, საფრთხის ქვეშ აყენებს ორივეს. მეორე დიდი პრობლემა დირექტივისთვის კი იყო, ისევ და ისევ, მსოფლიოს სწრაფი ტექნოლოგიური განვითარება. 1995 წელს, დირექტივის მიღების დროს, კიბერ

[13] საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით [1995]

[14] Tassanakunlapan T., Verdugo M.A., Protection of Personal Data in Cyberspace: The EU-US E-Market Regime, ASEAN Journal of Legal Studies, Vol. 1, 2018, 53.

[15] იქვე.

სივრცე ჯერ კიდევ არ იყო ისეთი განვითარებული, რაც დღეს არის, პირდაპირ, რომ ვთქვათ, ახლოსაც არ იყო დღევანდელ რეალობასთან. პერსონალურ მონაცემთა განმარტებაც კი, იყო ძალიან შეზღუდული და მოიცავდა მხოლოდ პირის სახელს, სურათი, ელექტრონული ფოსტის მისამართი, ტელეფონის ნომერი, ეს კი ვეღარ აკმაყოფილებდა დღევანდელ შესაძლებლობებს.[16] არსებული პრობლემების გამო, ევროკომისიის მიერ გამოქვეყნებულმა ანგარიშმა აჩვენა, რომ მოქალაქეთა 67% არ გრძნობდა თავს დაცულად და თვლიდა, რომ ვერ აკონტროლებს პერსონალურ ინფორმაციას, რომელიც გავრცელებულია ინტერნეტში.[17]

მიუხედავად ბევრი ნაკლისა, დირექტივამ მონაცემთა დაცვის შესახებ მოგვცა ე.წ. „დავიწყების უფლება“. დირექტივის მე-12 და მე-14 მუხლებმა საფუძველი დაუდო ინდივიდის უფლებას, რომ კანონიერად დაიცვას თავი ინტერნეტშიც.[18] ტერმინი უფრო დეტალურად განიმარტა ევროკავშირის ახალ „ზოგადი მონაცემთა დაცვის რეგულაციაში“, რომელიც ამოქმედდა 2018 წელს და რომელიც უფრო დეტალურად იქნება განხილული კვლევის მომდევნო ნაწილებში. მანამდე კი საჭიროა იმის განმარტება თუ, რას წარმოადგენს დავიწყების უფლება, რატომ არის მისი არსებობა მნიშვნელოვანი და პრობლემატური და რა იყო ის ახალი რეგულაციის ამოქმედებამდე.

3.1. „დავიწყების უფლება“ და მისი მნიშვნელობა

ინტერნეტის ინფორმაციული ბაზა შეიცავს ყველაფერს, რასაც ადამიანები საკუთარი ნებით ტვირთავენ საიტებზე და არც ის არის საიდუმლო, რომ კიბერ სივრცე ძალიან დაურეგულირებელია, ნებისმიერ ადამიანს შეუძლია სხვის შესახებ ბევრი

[16] საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით [1995], მუხლი 2, 19.

[17] Special Eurobarometer 431, Data Protection Report, 03.2015, 12; იხ. <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf> [05.2015]

[18] საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით [1995], მუხლი 12, 14.

ინფორმაციის გაგება მარტივი საძიებო საშუალებებით. ამას ემატება ის ფაქტიც, რომ საინფორმაციო მედია კომპანიები მუდმივად ცდილობენ საკუთარი ბაზის გაზრდას და დღევანდელი მდგომარეობით, უკვე შესაძლებელია 80-იანი წლების სტატიების ნახვა ინტერნეტში, ცნობილ მედია საიტებზე.

მონაცემთა დაცვის შესახებ დირექტივის მე-12 მუხლის იმპლემენტაცია სხვადასხვა სახელმწიფოებმა სხვადასხვანაირად განახორციელეს და განსხვავებული საზღვრები მიანიჭეს მას, სწორედ ასე წარმოიშვა დავიწყების უფლების საფუძველი. ამას დაემატა 2014 წლის ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება საქმეში: Google Spain vs AEPD and Mario Costeja Gonsalez[19], ჯერ კიდევ მაშინ, სანამ კანონიერ ძალას მიიღებდა GDPR. ნებისმიერ ადამიანს, რეალური საფუძვლის არსებობის შემთხვევაში, აქვს უფლება, რომ მოითხოვოს მასთან დაკავშირებული ინტერნეტ ბმულების წაშლა და რაც მთავარია, გუგლი არის მონაცემთა მაკონტროლებელი კომპანია.

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

1998 წელს ესპანურმა გაზეთმა გამოქვეყნა ორი განცხადება, რომელიც ეხებოდა უძრავი ქონების ძალით გაყიდვას სოციალური ვალების გამო. ეს განცხადება გამოქვეყნდა ესპანური სამინისტროს დავალებით და ინტერნეტის განვითარებასთან ერთად, მოხდა განცხადებების ელექტრონული ვერსიის შექმნაც. ერთ-ერთი ადამიანი, რომლის სახელიც, როგორც მოვალე, გამოჩნდა ამ განცხადებებში, იყო საქმეში მოპასუხე - მარიო გონზალესი. 2009 წელს იგი დაუკავშირდა გაზეთს და მოითხოვა ამ მონაცემის წაშლა, რადგან გუგლის საძიებო სისტემა მის სახელზე სწორედ ამ ინფორმაციას აჩვენებდა, ხოლო მოპასუხის აზრით ეს ინფორმაცია აღარ იყო რელევანტური, საქმე იყო დასრულებული და არ იყო საჭირო, რომ ხალხს ენახა ეს.

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

გაზეთის განცხადებით, ისინი ვერ წაშლიდნენ ამ მონაცემებს, რადგან ეს იყო სამინისტროს ბრძანება, ჯერ კიდევ 1998 წელს.

2010 წელს, მოპასუხემ მოსთხოვა ესპანეთში დარეგისტრირებულ გუგლის კომპანიას - Google Spain, რომ შეეზღუდათ წვდომა აღნიშნულ ბმულებთან. ესპანურმა კომპანიამ მოთხოვნა გადააგზავნა აშშ-ში, კალიფორნიის შტატში რეგისტრირებულ გუგლის ოფისში და მათ გადააბარა საქმეში გარკვევა, რადგან სწორედ გუგლის მთავარი ოფისის პასუხისმგებლობა იყო საძიებო სისტემის მართვა და მუშაობა. ამასთან ერთად, მოპასუხემ შეიტანა საჩივარი ესპანეთის მონაცემთა დაცვის სააგენტოში და მოთხოვა, როგორც გაზეთს, ასევე გუგლს, რომ მთლიანად წაშლილიყო ეს განცხადებები ინტერნეტიდან. აღნიშნული საქმე გადაწყვიტა ესპანურმა სააგენტომ და დაადგინა, რომ გუგლს სასწრაფოდ უნდა გადაედგა ნაბიჯები, რომ წაეშალა მონაცემების ინდექსი და შეეზღუდა სამომავლოდ წვდომა, ევროკავშირის დირექტივის საფუძველზე. გუგლის კალიფორნიულმა და ესპანურმა კომპანიებმა გაასაჩივრეს ესპანეთის სასამართლოში და განმარტეს, რომ კალიფორნიაში დაფუძნებული გუგლი არ იყო ვალდებული, რომ დამორჩილებოდა ევროკავშირის დირექტივას მონაცემთა დაცვის შესახებ. ესპანეთის სასამართლომ გადააგზავნა საქმე მართლმსაჯულების ევროპულ სასამართლოში და მოსთხოვა მათ სამ კითხვაზე პასუხის გაცემა: 1. დირექტივის ტერიტორიული ფარგლები; 2. ინტერნეტის საძიებო სისტემის პროვაიდერი კომპანიის სამართლებრივი პოზიცია, შეიძლება თუ არა, რომ ის ჩაითვალოს მონაცემის მაკონტროლებლად; 3. აწესებს თუ არა დირექტივა ე.წ. დავიწყების უფლებას.

ევროკავშირის მართლმსაჯულების სასამართლომ სამივე საკითხზე იმსჯელა და GDPR-ის ძალაში შესვლამდე, მონაცემთა დაცვის დირექტივის საფუძველზე დაადგინა დავიწყების უფლების არსებობა. სასამართლომ პირველ რიგში განმარტა, რომ გუგლი, როგორც საძიებო სისტემა არის მონაცემთა მაკონტროლებელი, ანუ იურიდიული პირი, რომელიც აკონტროლებს წესსა და მიზეზებს, როგორ და რატომ

მუშავდება ესა თუ ის მონაცემი. სასამართლომ ასევე დაადგინა, რომ კალიფორნიაში რეგისტრირებული გუგლის იურიდიული პირი ფლობს ესპანეთში რეგისტრირებული გუგლის 100%-ს, შესაბამისად, რადგან ესპანურ გუგლზე ვრცელდება დირექტივა, მაშინ ის ვრცელდება მის მფლობელზეც.[20] სასამართლომ არ გაიზიარა მოსარჩელის არგუმენტი, რომ ესპანეთში არ ხდებოდა მონაცემთა დამუშავება, რადგან ამის დადასტურება გამოიწვევდა ადამიანის ფუნდამენტური უფლებების შელახვასა და დირექტივის მთელი არსი დაიკარგებოდა.[21] სასამართლოს აზრით, ძალიან მნიშვნელოვანია, რომ დაცული იყოს ორივე მხარის უფლება, როგორც მონაცემთა მაკონტროლებლის, ასევე მონაცემთა სუბიექტისაც. ევროკავშირის ფუნდამენტური უფლებების ქარტიის მე-7 და მე-8 მუხლები იცავენ მონაცემთა სუბიექტის, ამ შემთხვევაში მოპასუხის უფლებებს. ხოლო, დირექტივის მე-14 მუხლი საშუალებას აძლევს პირს, რომ გარკვეულ შემთხვევებში გაასაჩივროს მის შესახებ არსებული მონაცემთა დამუშავება. ეს საჩივარი უნდა შევიდეს პირდაპირ მონაცემთა მაკონტროლებელთან, ამ უკანასკნელმა კი საფუძვლიანად უნდა შეასრულოს მიზეზები და შესაბამისად მოიქცეს.[22]

რაც შეეხება „დავიწყების უფლებას“, საინტერესოა, რომ გუგლის კომპანიების გარდა, საბერძნეთის, ავსტრიისა და პოლონეთის სახელმწიფოებმა, ასევე ევროპის კომისიამ, ურჩია სასამართლოს, რომ არ დაემკვიდრებინა ეს უფლება. მაგრამ, რადგან მათ მხოლოდ რჩევა შეეძლოთ, სასამართლომ განმარტა, რომ არსებობს ისეთი მონაცემები, რომელიც შეუსაბამობა დირექტივასთან და უნდა წაიშალოს მოთხოვნის შესაბამისად. მაგალითად, თუ მონაცემი არის არასწორი, ზედმეტად ინფორმატიული ან არა რელევანტური, მაშინ მონაცემის მაკონტროლებელმა შესაძლებელი უნდა გახადოს ასეთი ინფორმაციის წაშლა ან მინიმუმ წვდომის შეზღუდვა.[23]

[20] საქმე C-131/12 Google Spain vs AEPD and Mario Costeja Gonsalez [2014], 48-49
[21] იქვე, 50-58
[22] საქმე C-131/12 Google Spain vs AEPD and Mario Costeja Gonsalez [2014], 77
[23] იქვე, 94

აღნიშნული საქმე მნიშვნელოვანი პრეცედენტი გახდა პერსონალურ მონაცემთა დაცვის სფეროში. გუგლის საძიებო სისტემას დაევალა სპეციალური ფორმის შექმნა ევროკავშირის მოქალაქეებისთვის, რომლითაც პირებს შეეძლებათ გარკვეული ბმულების ინდექსების წაშლა საძიებო სისტემიდან. სასამართლომ განმარტა მნიშვნელობა საჯარო, ცნობად პირებსა და სხვა ინდივიდებს შორის. მაგალითად, 2018 წელს, ადამიანის უფლებების ევროპულმა სასამართლომ არ დააკმაყოფილა გერმანელი პირის საჩივარი, რომელმაც 90-იან წლებში მოკლა ადამიანი და საქმე იყო ძალიან გახმაურებული, რომ მომხდარიყო მისი სახელის წაშლა ვიკიპედიის გვერდიდან. სასამართლომ განმარტა, რომ საქმის სპეციფიკიდან გამომდინარე, მოსარჩელე არ იყო კერძო პირი და იგი საკუთარი საქციელის გამო იქცა ცნობად საჯარო პირად, ხოლო მისი სახელის ვიკიპედიაზე არსებობა წარმოადგენდა ჟურნალისტურ თავისუფლებას და სიტყვის თავისუფლებას. ამასთან ერთად, ვერ ჩაითვლება, რომ გერმანელი დამნაშავის სახელი არის არასწორი, არა რელევანტური ან ზედმეტად მგრძნობიარე მონაცემი.[24] აღსანიშნავია ის ფაქტი, რომ დირექტივა არ ეხებოდა ევროკავშირის გარეთ მყოფ კომპანიებს და მხოლოდ გამართლების საფუძველზე შეძლო სასამართლომ ამ საქმის განხილვა და დირექტივით ახალი პრეცედენტის დადგენა, რადგან გუგლს, რომ არ ჰქონოდა დარეგისტრირებული ესპანეთში კომპანია, ეს შესაძლებლობა არ მიეცემოდა სასამართლოს.

მიუხედავად იმისა, რომ აშშ-აც აქვს სასამართლო პრეცედენტები დავიწყების უფლებასთან დაკავშირებით, ისინი უკავშირდება 1920-იან წლებს და მისი იმპლემენტაცია არ მომხდარა კანონმდებლობაში ინტერნეტთან მიმართებით. აქედან გამომდინარე, ამერიკაში ფუნქციონალური საძიებო სისტემები და მონაცემთა სხვა მაკონტროლებლები, არ დგამენ იგივე ნაბიჯებს მონაცემთა დაცვისა და წაშლისთვის, რასაც ევროკავშირის ქვეყნების ტერიტორიაზე. ამერიკაში დავიწყების უფლება სერიოზულ კონფლიქტი მოდის კონსტიტუციის პირველ შესწორებასთან, რომელიც

[24] ადამიანის უფლებათა ევროპული სასამართლოს 2018 წლის 28 ივნისის განჩინება საქმეზე, Wolfgang Werle and Manfred Lauber v. Wikipedia

ქადაგებს სიტყვის თავისუფლებას.[25] ხოლო ეს არის ზღვარი, რომელსაც ამერიკა არ გასცდება.

დავიწყების უფლება დელიკატური საკითხია. შეუძლებელია მისი ბრმად აღსრულება. საჭიროა, რომ საძიებო სისტემებმა გაითვალისწინონ, როგორც ადამიანის პირადი უფლებები და პერსონალური მონაცემების დაცვა, ასევე საჯარო ინტერესები, რადგან ხშირ შემთხვევაში ისინი იკვეთებიან ერთმანეთში. სასამართლოს მიერ მიღებული გადაწყვეტილება და გაკეთებული განმარტება ერთის მხრივ საშუალებას აძლევს მოქალაქეებს, რომ შეზღუდონ წვდომა მათ პერსონალურ მონაცემებზე, მაგრამ, თუ რა ტიპის მონაცემები უნდა შეიზღუდოს ხდება განხილვის საგანი. ერთის მხრივ სწორია 15 წლის წინანდელი განცხადების წაშლა ინტერნეტიდან, რომელსაც არავითარი კავშირი აღარ აქვს ადამიანთან და მხოლოდ და მხოლოდ მის პერსონალურ მონაცემად ითვლება, ხოლო მეორეს მხრივ, უნდა შეიზღუდოს თუ არა წვდომა ინფორმაციაზე ექიმის მიერ დაშვებულ შეცდომაზე, რომელიც ასევე რამდენიმე წლის წინ მოხდა. სწორედ ეს გააკეთა გუგლმა 2015 წელს.[26] ამის გარდა, პრობლემა იქმნება ქვეყნებს შორის არსებულ განსხვავებულ რეგულაციებში, განსაკუთრებით ევროკავშირისა და აშშ-ს შემთხვევაში. კიბერ სივრცის განვითარებასთან ერთად, ძალიან ბუნდოვანი გახდა ტერიტორიული საზღვრები. რადგანაც აშშ არ არეგულირებს დავიწყების უფლებას და განმარტავს, რომ სიტყვის თავისუფლება არის უმნიშვნელოვანესი, იქმნება პრობლემა და განსხვავებული დამოკიდებულება, თუ რა რეგულაციების ქვეშ უნდა მოექცეს ამერიკული კომპანია, რომელიც ითვლება ევროკავშირის მოქალაქეების მონაცემების მაკონტროლებლად.

[25] Walker R., The Right to be Forgotten, Hashtings Law Journal, Vol 64, 2012, 261.

[26] Google Transparency Report, Search removals under European privacy law; იხ.: <https://transparencyreport.google.com/eu-privacy/overview> [03.2015]

3.2. ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR)

2012 წელს ევროკომისიამ წარადგინა ახალი რეგულაცია მონაცემთა დაცვის შესახებ, როდესაც უკვე აშკარა ხდებოდა, რომ ყოფილი დირექტივა ვეღარ აკმაყოფილებდა თანამედროვე გამოწვევებს, განმარტებები ვეღარ ასოცირდებოდა ახალ საინფორმაციო ტექნოლოგიებთან და რაც მთავარია, დირექტივა დიდ დისკრეციულ უფლებამოსილებას ანიჭებდა სახელმწიფოებს, რომლებსაც შეეძლოთ, თითონ განემარტათ დირექტივის ნაწილები და მისი სხვაგვარი იმპლემენტაცია განეხორციელებინათ. 2015 წლის დეკემბერში, ევროპის პარლამენტმა ხმა მისცა ახალ რეგულაციას, 2016 წელს მიიღო რეგულაცია, ხოლო 2018 წელს კი ყველა სახელმწიფოსთვის სავალდებულო გახდა ამ რეგულაციის ქვეშ მუშაობა და მან სრულებით ჩაანაცვლა, 1995 წელს გამოშვებული, მონაცემთა დაცვის დირექტივა.

მონაცემთა დაცვის ზოგადი რეგულაცია ძალიან ახალია და იმ პერიოდშია შემუშავებული და ძალაში შესული, როდესაც კიბერ სივრცის შესაძლებლობებმა, პერსონალურ მონაცემთა მიღებისა და დამუშავების ასპექტში, მაქსიმალურ ნიშნულს მიაღწია და ბოლო ორი-სამი წლის მანძილზე მნიშვნელოვანი ცვლილება ან განახლება, ამ მხრივ, აღარ მომხდარა. ამიტომაც შეგვიძლია ვთქვათ, რომ კარგი დრო იყო ახალი რეგულაციის მისაღებად. მთავარია გავარკვიოთ, რამდენად სწორი იყო ის ცვლილებები, რითაც განსხვავდება ახალი რეგულაცია, აწ უკვე გაუქმებული დირექტივისგან. ზოგადი რეგულაცია აწესებს საკუთარ მასშტაბებს, იგი ვრცელდება მონაცემთა სრულად ან ნახევრად ავტომატიზებულ დამუშავებაზე, იგი არ ვრცელდება ინდივიდის მიერ პერსონალური მონაცემის შეგროვებაზე პირადად, პერსონალური მიზეზის გამო.[27] რეგულაცია ვრცელდება პერსონალურ მონაცემთა მაკონტროლებელ ან გადამამუშავებელ დაწესებულებებზე ევროკავშირის ზონებში, ან ისეთ კომპანიებზე, რომლებიც არ არიან რეგისტრირებულნი ევროკავშირში, მაგრამ სთავაზობენ საკუთარ პროდუქტსა და სერვისებს ევროკავშირის ზონებში და

[27] Long W. RM., Scali G., Blythe F., European Union Overview, The Privacy, Data Protection and Cybersecurity Law Review - Edition 5, III, 2018.

შესაბამისად აქვთ წვდომა მოქალაქეების პერსონალურ მონაცემებთან. აქედან გამომდინარე, მარეგულირებელ ორგანიზაციებს აღარ მოუწევთ იმაზე ფიქრი, აქვთ თუ არა უცხოურ კომპანიებს რაიმე სახის ორგანიზაცია შექმნილი მათ ტერიტორიაზე. რომ გავიხსენოთ, გუგლის შემთხვევა, მონაცემთა დაცვის ზოგადი რეგულაციების თანახმად, გუგლი პირდაპირ იქნება პასუხისმგებელი ქმედებებზე, რადგან ის ამუშავებს ევროკავშირის მოქალაქის მონაცემებს და არა იმიტომ, რომ მისი ერთ-ერთი შვილობილი კომპანია რეგისტრირებულია ესპანეთში.

მონაცემთა დაცვის დირექტივის თანახმად, მხოლოდ მონაცემთა მაკონტროლებელ პირს შეიძლებოდა, რომ დაკისრებოდა პასუხისმგებლობა, თუ დადგებოდა ამის აუცილებლობა. ახალმა რეგულაციამ გაიზიარა ტექნოლოგიური კომპანიების რჩევები, რომ ხშირ შემთხვევაში, მონაცემთა დამუშავებას ახორციელებს სხვა კომპანია, არა მაკონტროლებელი, არამედ პროცესორი კომპანია, შესაბამისად, ჩადენილი ქმედებისთვის პასუხისმგებლობა უნდა დაეკისროს სწორედ იმ პროცესორ კომპანიას, ვისაც ევალებოდა მაკონტროლებლის მონაცემთა დამუშავება.[28]

რაც ძალიან მნიშვნელოვანია და როგორც კვლევის წინა თავშია ნახსენები, ევროკომისიამ შეცვალა პერსონალურ მონაცემთა განმარტება და მისცა მას უფრო ფართო და მრავლის მომცველი როლი ევროკავშირის სამართალში. თუ დირექტივა ითვალისწინებდა მხოლოდ სახელს, ფოტოს, ელექტრონული ფოსტის მისამართს, ფიზიკურ მისამართს, ტელეფონის ნომერსა და პირად ნომერს, მონაცემთა დაცვის ზოგადმა რეგულაციამ დაამატა რამდენიმე მნიშვნელოვანი პუნქტი, კერძოდ: აი-პი მისამართი (ინტერნეტ პროტოკოლის მისამართი), მობილური მოწყობილობის იდენტიფიკატორი, გეო-ლოკაცია, ბიომეტრიული მონაცემები, ამა ყველაფერთან ერთად კი, ფსიქოლოგიური იდენტობა, გენეტიკური იდენტობა, ეკონომიკური სტატუსი, კულტურული იდენტურობა, სოციალური იდენტურობაც მოექცნენ ახალი

[28] SeeUnity, The main differences between the DPD and the GDPR and how to address those moving forward, 3, 2016.

რეგულაციების დაცვის ქვეშ.[29] სწორედ ამ ცვლილებებში აისახება კარგად თანამედროვე ტექნოლოგიების გამოძახილი, როგორ შეცვალეს კომპანიებმა პერსონალურ მონაცემთა შეგროვების მექანიზმები. მონაცემთა დაცვის ზოგადი რეგულაციები განმარტავენ, რომ სპეციალური ნებართვის გარეშე, კომპანიები ვერ შეძლებენ, რომ მიიღონ ინდივიდების ვებ-ბრაუზერის ისტორია, საძიებო სისტემის ისტორია, შეძენის ისტორია და ა.შ.[30]

ევროკავშირის მართლმსაჯულების სასამართლოს მიერ აღიარებული ადამიანის უფლებას - დავიწყების უფლებას, მონაცემთა დაცვის ზოგადმა რეგულაციამ სრული იმპლემენტაცია გაუკეთა საკუთარ ნორმებში. მე-17 მუხლი, წაშლის უფლება (დავიწყების უფლება), საშუალებას აძლევს ადამიანებს, რომ მოსთხოვონ პერსონალურ მონაცემთა მაკონტროლებელ პირს, მონაცემის წაშლა ყველანაირი გადავადების გარეშე, თუ: „პერსონალურ მონაცემებს აღარ აქვს ის საჭიროება, რის გამოც მოხდა მისი შეგროვება თავის დროზე; თუ მონაცემთა სუბიექტი გამოიხმობს მაკონტროლებლისთვის მინიჭებულ უფლებას და სხვა არანაირი მიზეზი არ არსებობს მონაცემის შესანახად; თუ მოხდა მონაცემის უკანონოდ შენახვა და დამუშავება; პერსონალური მონაცემის წაშლის საჭიროება გამომდინარეობს ევროკავშირის ან წევრი ქვეყნის რეგულაციიდან გამომდინარე და მაკონტროლებელი ვალდებულია დაემორჩილოს მას.“[31] აღნიშნულმა მუხლმა მოაგვარა ძველი დირექტივის კიდევ ერთი პრობლემა და განმარტა თუ კონკრეტულად რა შემთხვევაში არ შეიძლება დავიწყების უფლების გამოყენება, მაგალითად: თუ მონაცემის დამუშავება ეხება აზრის გამოხატვის თავისუფლებას; თუ მონაცემის დამუშავებას კანონის ფარგლებში ითხოვს ევროკავშირის ან წევრი სახელმწიფოს რომელიმე რეგულაცია; თუ საჯარო ინტერესების გათვალისწინებით აუცილებელია ეს; თუ

[29] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2016 წლის 24 მაისს), მუხლი 4

[30] იხ. მინიშნება 27, გვერდი 21 ნაშრომში.

[31] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2016 წლის 24 მაისს), მუხლი 17

სასამართლო დავებისთვის არის ეს საჭირო. ამ ნაბიჯებით, ევროკომისიამ აღმოფხვრა „დავიწყების უფლების“ არეალის პრობლემა. ეს საჭირო იყო, რომ აღარ განმეორებულიყო გუგლის მიერ, 2015 წელს, დაშვებული შეცდომა, როდესაც კომპანიამ წაშალა ბმულები, რომლებიც უკავშირდებოდა ექიმის მიერ წარსულში დაშვებულ შეცდომებს.

პასუხისმგებლობის საკითხი GDPR-ის განმარტებით

ტერმინების უფრო დეტალური და კორექტული (ყოველ შემთხვევაში, დღეისთვის) განმარტებების გარდა, GDPR-სა და მონაცემთა დაცვის დირექტივას შორის ძალიან დიდი განსხვავება არის ახლად შემოღებული პასუხისმგებლობის საკითხი და დაცული მონაცემების გატეხვის დროს ქცევის წესები. ამით ევროკავშირმა კიდევ ერთხელ გაუსვა ხაზი იმას, რომ შეიძლება რთულია პერსონალურ მონაცემთა დაცვა ონლაინ სივრცეში, ფიზიკური სამყაროსგან განსხვავებით, მაგრამ ეს მაინც არ არის შეუძლებელი და თუ ახალი კანონმდებლობები ვერ დაარეგულირებენ სათანადოდ, დროთა მანძილზე, ორგანიზაცია მზად იქნება, რომ კვლავ შეიმუშაოს ახალი პროექტი.

ისეთი მგრძნობიარე ინფორმაცია, როგორიცაა პერსონალური მონაცემები, მაქსიმალურად დაცული უნდა იყოს ყველანაირი ზემოქმედებისგან და მესამე პირების უკანონო შეღწევისგან. კორპორაციებს მაქსიმალურად აქვთ გააზრებული პერსონალურ მონაცემთა შენახვისა და დამუშავების რისკები. მონაცემთა უკანონოდ და დაუშვებლად გავრცელებამ, სავალალო შედეგები, არამარტო მონაცემთა სუბიექტისთვის შეიძლება რომ გამოიწვიოს, არამედ მაკონტროლებელი კომპანიისთვისაც შეიძლება, რომ აღმოჩნდეს კატასტროფული. მეგა კორპორაციები, რომლებიც დგანან კიბერ შეტევის ან სხვა სახის საფრთხის წინაშე, იაზრებენ, რომ მონაცემთა დაცვის სისტემის გარღვევა გამოიწვევს ძალიან დიდ ხარჯებს, ჯარიმებს, სასამართლო დავებს და რაც ყველაზე მეტად აწუხებთ მულტი-ნაციონალურ

ტექნოლოგიურ კომპანიებს - რეპუტაციის გაფუჭებას, რაც კიდევ უფრო მეტ ზარალთან არის დაკავშირებული. პატარა კომპანიები კი დგანან მთლიანი გაკოტრების საფრთხის წინაშე.[32] სამწუხაროდ, კომპანიების მონაცემთა ბაზის დაცვის გატეხვა საკმაოდ ხშირი მოვლენაა და ყოველწლიურად, მილიონობით ადამიანის პერსონალური მონაცემები ხვდება არასასურველ ხელში. მაგალითად, 2013 წელს, აშშ-ს ერთ-ერთი ყველაზე დიდი მაღაზიათა ქსელი „Target"-ის მიერ შენახული და დამუშავებული მონაცემთა ბაზა გატეხეს დამნაშავეებმა და მიითვისეს 70 მილიონი მომხმარებლის მონაცემები. ამის შედეგად, კომპანიას ასობით მილიონი დოლარი დაუჯდა ჯარიმები და სასამართლო პროცესები, ხოლო ორი დირექტორი გახდა ვალდებული, რომ გადამდგარიყო. დიდი ბრიტანეთის საინფორმაციო კომისიის ანგარიშის თანახმად, 2016 წლის იანვრიდან მარტამდე, კომისიაში შევიდა 448 განცხადება მონაცემთა ბაზის გატეხვის შესახებ.[33] ივარაუდება, რომ იმ კომპანიების რიცხვი, რომელთა მონაცემთა ბაზებიც გატყდა, მაგრამ არ განაცხადეს კომისიაში, ორჯერ უფრო მაღალია.

რა თქმა უნდა, კანონმდებელთა არცერთ წრეს, არცერთ სახელმწიფოში, არ შეუქმნია ილუზია, რომ მონაცემთა მაკონტროლებლებს (ასევე, პროცესორებს) აქვთ მონაცემთა ბაზების დაცვის აბსოლუტური შესაძლებლობა და შესაბამისად, არც მონაცემთა დაცვის ზოგადი რეგულაცია არ კრძალავს ამ ბაზის დაცვის გატეხვას. ამის მთავარი მიზეზი ისაა, რომ არ არსებობს ტექნოლოგიური შესაძლებლობები, რომლებიც 100% დაცულად ამყოფებენ მონაცემთა ბაზებს. ზოგადი რეგულაცია განმარტავს პერსონალურ მონაცემთა ბაზის გატეხვას: *„დაცვის გატეხვა, რომლის შედეგადაც ხდება დამუშავებულ პერსონალურ მონაცემთა, შემთხვევი, ან არაკანონიერი წაშლა, დაკარგვა, შეცვლა, წვდომა."*[34]

---

[32] IT Governance Privacy Team, Common Data Security Failures, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, 2017, 83

[33] Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2016 Main Report, 2016

[34] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2016 წლის 24 მაისს), მუხლი 4, ნაწილი 12

რეგულაციისთვის არ აქვს მნიშვნელობა, თუ რა ფორმით მოხდა მონაცემთა ბაზის გატეხვა, რადგან ეს გზა შეიძლება იყოს ან ძალიან კომპლექსური, ან ისეთივე მარტივი, როგორიცაა პერსონალური კომპიუტერის მოპარვა ან დაკარგვა ინდივიდის მიერ. ამიტომ, ზოგადი რეგულაცია ყურადღებას ამახვილებს ბაზის გატეხვის შემდეგ საჭირო ნაბიჯებზე, რა უნდა მოიმოქმედონ კომპანიებმა, რომ მაქსიმალურად შეამცირონ მოქალაქეთა ზარალი. GDPR-ს აქვს ერთი წესი, პერსონალურ მონაცემთა მაკონტროლებელი ვალდებულია, რომ ბაზის გატეხვის შესახებ გაგებიდან, 72 საათის განმავლობაში, შეატყობინოს ზედამხედველ ავტორიტეტს (განსხვავებული საჯარო იურიდიული პირები სხვადასხვა სახელმწიფოებში). ასევე, მონაცემთა პროცესორი კომპანიებიც არიან ვალდებულნი, რომ დაუყოვნებლივ შეატყობინონ პრობლემის შესახებ მაკონტროლებელ კომპანიებს. რეგულაციის 33-ე მუხლის თანახმად, შეტყობინება დეტალურ ინფორმაციას უნდა შეიცავდეს არსებული პრობლემის შესახებ.

ამის გარდა, ზოგადი რეგულაციის 25-ე მუხლი, ავალდებულებს პერსონალურ მონაცემთა მაკონტროლებელ კომპანიებს, რომ მოახდინონ ისეთი ტექნიკური ზომების იმპლემენტაცია, როგორებიცაა ფსევდონიმიზაცია (Pseudonymisation) და ანონიმიზაცია (Anonymisation). GDPR ავალდებულებს კომპანიებს, რომ მხოლოდ საჭირო მონაცემები შეინახოს და დაამუშაოს, ამასთან ერთად კი დაიცვას, ახლად შექმნილი, პერსონალურ მონაცემთა დაცვის პრინციპები:

- კანონიერების, სამართლიანობისა და გამჭირვალეობის პრინციპი;
- მიზანმიმართული შეზღუდვების პრინციპი;
- მონაცემთა მინიმიზაციის პრინციპი;
- სისწორის პრინციპი;
- ბაზის ვადიანობის პრინციპი;

- კონფიდენციალურობის პრინციპი;[35]

სწორედ ამ პრინციპებისა და კომპანიების ვალდებულებების შესრულებაა ზოგადი რეგულაციის მიზანი. ხოლო, ამის ერთ-ერთ გზას წარმოადგენს ჯარიმა, რომელიც დაეკისრებათ კომპანიებს თუ ისინი არ დაემორჩილებიან ევროკავშირის მიერ მიღებულ რეგულაციას.

მონაცემთა დაცვის დირექტივა, რომელიც გაუქმდა რეგულაციის ძალაში შესვლის შემდეგ, არ ითვალისწინებდა არანაირ ჯარიმას. დირექტივა საშუალებას აძლევდა წევრ ქვეყნებს, რომ შიდა სახელმწიფოებრივი ნორმებით დაერეგულირებინათ პასუხისმგებლობის საკითხები. ასეთი თავისუფლების შედეგი კი იყო დაბალი ჯარიმები და იშვიათი გამოყენება.[36] ამჯერად, ევროკომისიამ აღარ დაუშვა იგივე შეცდომა და ახალი რეგულაციების ქვეშ მოექცა ჯარიმებიც. რეგულაციის გარდა, სახელმწიფოებს შეუძლიათ, რომ შემოიღონ უფრო მკაცრი შიდასახელმწიფოებრივი ნორმები, მაგრამ, ეს არ შეცვლის ზოგადი რეგულაციის მიერ, 83-ე მუხლში, დაწესებულ ადმინისტრაციულ ჯარიმებს. კომპანიის მხრიდან, რეგულაციის მძიმე დარღვევის შემთხვევაში, ის შეიძლება, რომ დაჯარიმდეს წლიური ბრუნვის არაუმეტეს 4%-ით, არანაკლებ 20 000 000 ევროთი. მძიმე დარღვევად ჩაითვლება უფლების გარეშე პერსონალურ მონაცემთა დამუშავება, ან დაცვის არასრული იმპლემენტაცია ბაზაში. ამის გარდა, უფრო პატარა დარღვევებისთვის, მაგალითად, როგორიცაა მონაცემთა ბაზის გატეხვის არ შეტყობინება, კომპანია დაჯარიმდება წლიური ბრუნვის არაუმეტეს 2%-ით, არანაკლებ 10 000 000 ევროთი.

ერთი შეხედვით, შეიძლება ჯარიმების ოდენობა ძალიან მაღალი ჩანს, მაგრამ ასეთი თანხა მწყობრში ამყოფებს პატარა კომპანიებს, რომლებთა საქმიანობაც ვრცელდება ევროკავშირში, მაგრამ, წლიური ბრუნვა არ არის იმდენად მაღალი, რომ

[35] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2016 წლის 24 მაისს), მუხლი 5

[36] SeeUnity, The main differences between the DPD and the GDPR and how to address those moving forward, 4, 2016.

სერიოზული ზარალის გარეშე შეძლონ მათი გადახდა. ხოლო, მულტინაციონალური მეგაკორპორაციები კი სამაგალითოდ დაისჯებიან რეგულაციის არ დამორჩილებისთვის. 2019 წლის 21 იანვარს, საფრანგეთის ინფორმატიკისა და თავისუფლების ნაციონალური კომისია გახდა პირველი ორგანო, რომელმაც დააჯარიმა ტექნოლოგიური კომპანია, გუგლი, 50 000 000 ევროთი. ამის მიზეზი კი იყო, გუგლის მხრიდან ორი პრინციპის დარღვევა: გამჭვირვალეობის პრინციპის არ შესრულება, რადგან ადამიანებმა არ იცოდნენ რაზე თანხმდებოდნენ, უკანონოდ და უნებართვოთ რეკლამების კონკრეტულ ინდივიდზე მორგება.[37] ეს იყო GDPR-ის პირველი რეალური გამოყენება და გუგლის სახით შეიქმნა პრეცედენტი, რომ ევროკავშირის მიერ დადგენილ ზოგად რეგულაციებს ვერავინ ვერ აუვლის გვერდს. შეიძლება საფრანგეთის კომისიის მიერ დაკისრებული ჯარიმა დიდ თანახად გეჩვენებოდეთ, მაგრამ გასათვალისწინებელია, რომ გუგლის წლიური ბრუნვის 4% უკავშირდება მილიარდებს, შესაბამისად, 50 000 000 ევროს უფრო სამაგალითო დასჯის სახე ქონდა.

3.3. თანამედროვე პრობლემები და გამოწვევები ევროკავშირისთვის

თამამად შეიძლება ითქვას, რომ GDPR არის უმნიშვნელოვანესი ნაბიჯი 1995 წლის შემდეგ. გამოსწორებულია ბევრი არსებული ხარვეზი და არის კანონთა ჰარმონიზაციის ერთგვარი მცდელობა. ევროკავშირის თანამედროვე მიდგომა და სამომავლო გეგმები, სამართლებრივ და ეკონომიკურ სფეროში, ბრუნავს ჰარმონიზაციის გარშემო. თუმცა, ჰარმონიზაციისთვის საჭიროა, რომ კანონის გარდა, სახელმწიფოები იყვნენ ერთ აზრზე და მოქმედებდნენ ერთი სისტემის ქვეშ. ზოგადმა რეგულაციამ ეს გააკეთა, როდესაც შეუმცირა ხელმომწერ სახელმწიფოებს დისკრეციის უფლებამოსილება გარკვეულ საკითხებში და აქცია ისინი ახალი

[37] Deliberation of the Restricted Committee SAN-2019-001, pronouncing a financial sanction against GOOGLE LLC, 28, 2019

რეგულაციის ნაწილად. მაგრამ, ზოგადი რეგულაციები მაინც მოიკოჭლებენ გაკრვეულ სიტუაციებში და ევროკავშირს პრობლემა ექმნება, როდესაც საქმე ეხება მონაცემთა ქვეყანათაშორისო გადატანას. მიუხედავად იმისა, რომ ევროკომისიამ შეამცირა ხელმომწერი სახელმწიფოების დისკრეციული უფლებამოსილებები, მათ მაინც დაუტოვა გარკვეული შესაძლებლობები. ამას დაემატა ისიც, რომ სახელმწიფოების უფლებების შესახებ არსებული მუხლი, არ არის სათანადოდ განმარტებული და არ განსაზღვრავს დეტალურად, თუ როდის შეიძლება, რომ ქვეყანამ შეიმუშაოს დამატებითი შიდა კანონმდებლობა. მაგალითად, თუ გერმანიის რეზიდენტი პირი გამოიყენებს დაივწყების უფლებას გერმანიაში, მაგრამ პერსონალურ მონაცემები მუშავდება ბელგიაში და ბელგიური კომპანია იყენებს განსხვავებულ კანონმდებლობას, რომლითაც შესაძლებელია პერსონალური მონაცემის დამუშავების უფლების შენარჩუნება, როგორ გადაჭრის საკითხს ზოგადი რეგულაციები.[38] ამის გარდა, რეგულაცია იყენებს მრავალ ტერმინს, რომელსაც არ განმარტავს თავისით, რაც საშუალებას აძლევს, როგორც კომპანიებს, ასევე სახელმწიფოებსაც, რომ საკუთარი მოსაზრება მოარგონ ყველაფერს. რადგან არ არსებობს კონკრეტული და ნათელი განმარტება, საჭიროა, რომ დავუცადოთ სასამართლოების მიერ ჩამოყალიბებულ პრეცედენტებს, რასაც შეიძლება რამდენიმე წელი მაინც დასჭირდეს, რა დროსაც, თავისუფლად შესაძლებელია, რომ GDPR, მისი წინამორბედის მსგავსად, გამოუსადეგარი გახდეს.

ზოგადმა რეგულაციამ ბევრი ახალი ვალდებულება შემოიღო კომპანიებისთვის. მიუხედავად იმისა, რომ 2012 წელს მოხდა პირველი ვერსიის წარდგენა, რეალურად იგი 2016 წელს შევიდა ძალაში და კომპანიებს არ ქონიათ მისი კარგად შესწავლისა და საკუთარი შიდა რეგულაციების დალაგების დრო. საკმაოდ რთულია ტრანზიცია ერთი კანონმდებლობიდან მეორეში და ამის ნათელი მაგალითია გუგლის დაჯარიმება 2019 წლის დასაწყისში. არ იქნება მართებული იმ არგუმენტის

[38] Dode A., the challenges of implementing General Data Protection Law (GDPR), 14th International Conference in "Standardization, Protypes and Quality: A Means of Balkan Countries' Collaboration, 2, Albania, 2018.

მოყვანა, რომ გუგლს გაანალიზებული ქონდა საკუთარი ქმედების დანაშაული და მზად იყო რისკებისთვის. ისეთი კომპანიისთვისაც კი, როგორიცაა გუგლი, რთული აღმოჩნდა ახალი რეგულაციების იმპლემენტაცია და 2018 25 მაისს, გახდა თუ არა ახალი ზოგადი რეგულაციები სავალდებულო ხელმომწერი ქვეყნებისთვის, კომპანიის წინააღმდეგ შევიდა საჩივრები რამდენიმე ათასობით ადამიანისგან.

ევროკავშირის სურვილი, საკანონმდებლო ბაზისა და ფუძეების ჰარმონიზაცია, შეუძლებელი იქნება იქამდე, სანამ ევროპულ გაერთიანებას ჭირდება სხვა სახელმწიფოებთან მჭიდრო კავშირის არსებობა. ეს საჭიროება კი, აშკარაა, რომ კიდევ დიდი ხანი არ გაქრება. სანამ გადავალთ უშუალოდ აშშ-ევროკავშირის ურთიერთობის გარჩევაზე, აუცილებელია სხვა სახელმწიფოებთან დაკავშირებული პრობლემები.

21-ე საუკუნის ტექნოლოგიურ სამყაროში, მონაცემთა ბაზების კონტროლი შეიძლება, რომ ხდებოდეს სხვა ქვეყანაში. ძველი დირექტივა მოიხსენიებდა მათ, როგორც „მესამე სახელმწიფოებს“, ნებისმიერი ქვეყანა, რომელიც არ არის ევროკავშირის და/ან ევროპის ეკონომიკური ტერიტორიის წევრი. მესამე სახელმწიფოების ცნება არ შეცვლილა მონაცემთა დაცვის ზოგადი რეგულაციებით. ამავე რეგულაციაში დაემატა საერთაშორისო ორგანიზაციის განმარტება: ნებისმიერი კომპანია ან ორგანიზაცია, რომელიც ექვემდებარება საერთაშორისო საჯარო სამართალს ან შექმნილია ორი ან მეტი სახელმწიფოს შეთანხმების შედეგად. ასევე, საერთაშორისო ორგანიზაციად ჩაითვლება იურიდიული პირი, რომელიც შექმნილია ევროკავშირის ქვეყანაში მუშაობს ქვეყნის ტერიტორიაზე და ასევე აქვს გარკვეული ოპერაციები ე.წ. მესამე სახელმწიფოში.[39]

ევროკავშირი ძალიან მკაცრად უყურებს საკუთარი მოქალაქეების პერსონალურ მონაცემთა დაცვას, ამიტომ ნებისმიერმა კერძო თუ საჯარო იურიდიულმა პირმა, რომელსაც სურს, რომ აწარმოოს საქმიანობა ევროკავშირის ფარგლებში და არ არის

[39] IT Governance Privacy Team, Managing Personal Data Internationally, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, 250, დიდი ბრიტანეთი, 2017.

დარეგისტრირებული არცერთ წევრ სახელმწიფოში, მაინც ვალდებულია, რომ დაიცვას მონაცემთა დაცვის ზოგადი რეგულაციები. ხოლო მესამე სახელმწიფოები კი ვალდებულნი ხდებიან, რომ დაემორჩილონ ევროკავშირის მოთხოვნებს და თუ მათ ტერიტორიაზე ხდება ევროკავშირის მოქალაქეების პერსონალურ მონაცემთა გადატანა და დამუშავება, მაქსიმალურად მსგავსი დაცვის სტანდარტები დააწესონ.[40]

მონაცემთა დაცვის ზოგადი რეგულაციის მეხუთე თავი, დიდად არ განსხვავდება ძალადაკარგული დირექტივის მიერ დაწესებული პრინციპებისგან: პერსონალურ მონაცემთა ტრანსფერი მესამე ქვეყნებში, არის დაუშვებელი, რამდენიმე წინაპირობის გარეშე: თუ არსებობს სპეციალური Safe Guards ან ევროკომისიამ დაადგინა, რომ კონკრეტულ მესამე ქვეყანაში შეიძლება მონაცემთა მიმოცვლა.[41] მესამე სახელმწიფოს უნდა გააჩნდეს „მონაცემთა დაცვის ადექვატური ზომები“.[42] საბოლოო გადაწყვეტილება, თითოეულ სახელმწიფოზე, უნდა მიიღოს ევროკავშირის სპეციალურმა კომისიამ და მესამე სახელმწიფოს უნდა გააჩნდეს შემდეგი: კანონის უზენაესობა, სამართლიანი სასამართლო, ფუნდამენტური თავისუფლებები და ადამიანის უფლებები, რელევანტური კანონმდებლობა დაკავშირებული საჯარო დაცვას, საჯარო წესრიგთან, სისხლის სამართალთან.[43] ზოგადი კანონმდებლობის არსებობის გარდა, GDPR-მა შექმნა სპეციალური რეგულაციები, კონკრეტულად პერსონალურ მონაცემთა დაცვასთან დაკავშირებით, რომელსაც უნდა იზიარებდეს მესამე სახელმწიფო. ე.წ. Safeguards (დაცვის მექანიზმები), რომელთაც სავალდებულოს ხდის ზოგადი რეგულაციების 45-ე მუხლი, მესამე სახელმწიფოსგან მოითხოვს: საკანონმდებლო აქტებს საჯარო იურიდიული პირებისთვის, კორპორატიული სამართალი, მონაცემთა დაცვის სტანდარტული მუხლები, რომელიც შეიმუშავა

[40] Dode A., The challenges of implementing General Data Protection Law (GDPR), 14th International Conference in “Standardization, Protypes and Quality: A Means of Balkan Countries’ Collaboration, 5, Albania, 2018.
[41] Vrbljanac D., Personal Data Transfer to Third Countries – Disrupting the Even flow?, Athens Journal Law – Volume 4, Issue 4, 2018.
[42] General Data Protection Regulation (მიღებულია 2016 წლის 14 აპრილს, ძალაში შევიდა 2016 წლის 24 მაისს), მუხლი 44.
[43] იქვე, მუხლი 45.

კომისიამ, ქცევის წესები მაკონტროლებელი/პროცესორი კომპანიებისთვის, რომლებიც დაარსებულები არიან მესამე ქვეყნებში, სერტიფიცირების გარკვეული მექანიზმები მაკონტროლებელი/პროცესორი კომპანიებისთვის და კიდევ რამდენიმე დეტალი, რომლებიც უნდა იყოს დამოწმებული და ნებადართული, კომისიის მიერ.

ევროკავშირის მიზანი ნათელია, მაქსიმალურად დაიცვას საკუთარი მოქალაქეების პერსონალური მონაცემები და ხელი შეუწყოს კანონის ჰარმონიზაციას. მაგრამ, შედეგის მიღწევა არც ისეთი იოლია, როგორც ფურცელზე წერია. კომპანიები აღარ არიან შეზღუდულნი ერთი ქვეყნის ტერიტორიით და მონაცემთა ბაზების გაცვლა, დამუშავება, აღარ წარმოადგენს რთულ და ხანგრძლივ პროცესს. GDPR ცდილობს, რომ გაუმკლავდეს არსებულ პრობლემებს და დაავალდებულოს ე.წ. მესამე სახელმწიფოები, რომ მეტი გააკეთონ პერსონალურ მონაცემთა დაცვისთვის. კომპანიებისთვის და სახელმწიფოებისთვის საკმაოდ დიდი ხარჯების გარდა, ევროკავშირმა დააწესა ორმაგი სტანდარტები, ერთის მხრივ ისინი მკაცრად ექცევიან მესამე სახელმწიფოების საკმაოდ დიდ ნაწილს, მაგრამ მაქსიმალურად ცდილობენ, რომ მოერგონ აშშ-ში არსებულ სიტუაციას პერსონალურ მონაცემთა დაცვის შესახებ და არ შეუქმნან დიდი პრობლემები მეგა კორპორაციებს, რომლებიც სწორედ ამერიკის ტერიტორიაზე ამუშავებენ მონაცემებს.

იურისდიქციის პრობლემის მოგვარება უფრო და უფრო რთული ხდება, ტექნოლოგიის განვითარებასთან ერთად. მაგრამ, თუ ევროკავშირმა შეძლო GDPR-ის იმპლემენტაცია საკუთარი ქვეყნების გარეთ, თანამშრომლობის და ეკონომიკური ურთიერთობების გამყარების საფუძველზე, მაშინ პერსონალურ მონაცემთა დაცვის სფეროში, იურისდიქციის მნიშვნელოვანი პრობლემა უკან გადაიწევს. ამის იდეალური საწყისი წერტილი იქნება აშშ-ს კანონმდებლობასთან ურთიერთობის დარეგულირება. დღეს, ამერიკასა და ევროკავშირს შორის, ძალიან ვიწრო ძაფია (პერსონალურ მონაცემთა მიმართებით), რომელიც ისევე შეიძლება გაწყდეს, როგორც გამყარდეს. აშშ-ს გარდა არსებობს უამრავი სახელმწიფო, რომელსაც სურს

ევროკავშირთან მჭიდრო ურთიერთობის დამყარება, მათ შორის, შეგვიძლია, რომ საქართველოც მივიჩნიოთ.

ევროკავშირის მკაცრი რეგულაცია კარგია, მაგრამ, მთავარია, რომ სახელმწიფოების ერთი ქოლგის ქვეშ მოქცევა, ოცნებად არ დარჩეს. ამისთვის კი, მხოლოდ ცალმხრივი ურთიერთობა პოტენციური „მესამე ქვეყნებიდან“ ვერ იქნება საკმარისი. მნიშვნელოვანია, უშუალოდ ორგანიზაციის ჩართულობაც, აღნიშნული პრობლემის მოგვარებაში. ევროკავშირის მიდგომა ცხადია, „მონაცემთა დაცვის ევროპული საბჭო“-მ, რომელიც აფასებს ორგანიზაციის გარეთ არსებული სახელმწიფოების მდგომარეობას, მაქსიმალურად დეტალურად და მკაცრად უნდა განსაჯოს ისინი. მაგრამ „არჩევითი“ მიდგომა, რაც მდგომარეობს მხოლოდ ისეთ სახელმწიფოებთან ურთიერთობა, რომელიც ჭირდება ან აწყობს ევროკავშირს. მნიშვნელოვანია იმის გააზრება, რომ პერსონალური მონაცემები არის ინფორმაციული სამყაროს განუყოფელი ნაწილი, ხოლო ევროკავშირის მოქალაქეები კი წარმოადგენენ მონაცემთა ძალიან დიდ ბაზას და მისი გამოყენება, თუნდაც ვაჭრობაში ან სხვა რაიმე აქტივობაში, ხშირ შემთხვევაში, საჭიროა სხვადასხვა ქვეყნებისა და კომპანიებისთვის. ამიტომაც არ არის მიზანშეწონილი, რომ მესამე ქვეყნებისადმი დამოკიდებულება იყოს მკაცრი და ფაქტობრივად საშუალება არ ეძლეოდეთ პატარა სახელმწიფოებს, რომ შეუერთდნენ ევროკავშირს მოქალაქეთა პერსონალურ მონაცემთა გაცვლის საქმიანობაში.

4. აშშ-ს დამოკიდებულება პერსონალურ მონაცემთა დაცვაზე და პარტნიორობა ევროკავშირთან

ამერიკის შეერთებულ შტატებში პერსონალურ მონაცემთა დაცვა ძალიან ზოგადად და მშრალად არის გაწერილი კონსტიტუციაში.[44] ჯერ კიდევ 1928 წელს, ოლმსტედი აშშ-ს წინააღმდეგ საქმეში, მოსამართლე ბატლერმა, განსახვავებულ მოსაზრებაში იმსჯელა, რომ ადამიანის უფლება დაცულია კონსტიტუციის მეოთხე შესწორებაში: „ადამიანის უფლება იყოს დაცული საკუთარ სახლში, პიროვნებაში და დოკუმენტებში, არაზომიერი ჩხრეკისა და ძებნისგან.“[45] ოლმსტედის შემდეგ, მხოლოდ 1967 წელს, კატზი ამერიკის შეერთებული შტატების წინააღმდეგ საქმეში, სასამრთლომ დაადგინა, რომ ინდივიდის სუბიექტური მოლოდინი მონაცემთა დაცვაზე, დაცულია იქამდე, სანამ საზოგადოება თვლის, რომ ეს არის სამართლიანი და გონივრული.[46]

მაგრამ, აშშ-ს არ აქვს შემუშავებული ერთი ზოგადი კანონი, პერსონალურ მონაცემთა დაცვისთვის საჭირო მინიმალური მოთხოვნები, რომელიც გავრცელდებოდა ყველა შტატზე. ხშირად, ამერიკის ლეგისლატურას, მონაცემთა დაცვის შესახებ, უწოდებენ ფედერალური და საშტატო კანონების ჩანაკერებს (Patchwork).[47] შესაბამისად, აშშ-ს მიდგომა საფუძვლიანად განსხვავდება ევროკავშირისგან და სწორედ აქ იქმნება პრობლემა. ევროკავშირმა GDPR-ით, ერთი ქოლგის ქვეშ მოაქცია მონაცემთა დაცვის ძირითადი, თანამედროვე ელემენტები, 2000 წელს მიანიჭა მას ადამიანის ფუნდამენტური უფლების სტატუსი და ევროკავშირის ეკონომიკური ზონის წევრი ქვეყნების გარდა, მესამე ქვეყნების სტატუსის მსურველებს აიძულებს, რომ იმოქმედონ მის მიერ დაწესებული სტანდარტებით. აშშ-ში პერსონალურ მონაცემთა დაცვის რეგულაციები დაყოფილია კატეგორიებად და

[44] Weiss M.A., Archick K., U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, 2016, 3.
[45] Olmstead v. United States, მოსამართლე ბატლერის განსხვავებული აზრი, 277 U.S. 438 (1928).
[46] Katz v. United States, მოსამართლე ჰარლანის თანმხვედრი აზრი, 389 U.S 347 (1967).
[47] იხ. მინიშნება 43, ამავე გვერდზე.

დამოკიდებულია იმ სექტორზე, სადაც მიმდინარეობს მონაცემთა მოპოვება და დამუშავება.[48] მაგალითად, თუ საქმე ეხება ჯანმრთელობის სექტორს ან საკრედიტო ბარათების სექტორს, ფედერალური კანონმდებლობა სხვაგვარად არეგულირებს კონკრეტულად ამ სექტორში არსებული მონაცემების დაცვისთვის განკუთვნილ ნორმებს, შესაბამისად ამ ორ სფეროში წარმოქმნილია განსხვავებული უფლებები და ვალდებულებები. ერთის მხრივ, შეგვიძლია მივიჩნიოთ, რომ ეს საშუალებას აძლევს კანონმდებელს, მონაცემთა დაცვისთვის საჭირო რეგულაციები უფრო კონკრეტულად მოარგოს ამა თუ იმ სფეროს და მაქსიმალურად დაიცვას ის. მეორეს მხრივ, სწორედ ასეთმა მიდგომამ გამოიწვია ის, რომ სახელმწიფოში არ არსებობს მონაცემთა გამოყენების ზოგადი წესები, რაც პოტენციურად ტოვებს მონაცემთა გამოყენებისა და დამუშავების დაურეგულირებელ არეალებს. მაგალითად, დღევანდელი მდგომარეობით არ არსებობს რეგულაციები, რომლებიც დაიცავს და გააკონტროლებს პერსონალურ მონაცემთა დაცვის წესს ისეთი ონლაინ გამყიდვლების ხელში, როგორიცაა ამაზონი. ასევე, დიდი ხარვეზებია ფიესბუქისა და გუგლის მონაცემთა მოპოვების სხვადასხვა საშუალებებზე.[49]

რეალურად, აშშ-ს კანონმდებლობების წყობა და მონაცემთა დაცვა კომერციულ სექტორში, ერთ-ერთი ყველაზე ძველია და მისი ჩანაფიქრების მოძებნა შესაძლებელია მე-20 საუკუნის დასაწყისში.[50] მაგრამ, პრობლემები იქმნება, როდესაც ყველა შტატს აქვს საკუთარი კანონის შექმნის საშუალება. შესაბამისად, ვერც ასეთი სექტორული კანონები ვერ ხდება ისეთი ზოგადი და მრავლის მომცველი, როგორიც შეიძლება, რომ იყოს. დღევანდელი მდგომარეობით, ამერიკის კანონები, პერსონალურ მონაცემთა დაცვის შესახებ, რამდენიმე კატეგორიად იყოფა:

[48] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, Washington, DC, May 2014, 18.
[49] Solove D.J., Hartzog W., The FTC and the new common law of privacy, Columbia Law Review Vol. 114, 2014, 587.
[50] Raul A. C., Faircloth E. F., Moham K V., United States, The Privacy, Data Protection and Cybersecurity Law Review - Edition 5, III, 2017, 364.

- ფინანსური, სადაზღვევო და სამედიცინო ინფორმაცია;
- ინფორმაცია ბავშვებსა და სტუდენტებზე;
- ტელეფონი, ინტერნეტი და სხვა ელექტრონული კომუნიკაციის საშუალებები და მათი ჩაწერა;
- კრედიტი და საკრედიტო ინფორმაცია, მათი გამოძიება ფედერალურ დონეზე;
- სხვა კატეგორიები, რომლებიც დამოკიდებულია შტატებზე.[51]

ამ დანაწევრებასთან ერთად, სახელმწიფოს არ გააჩნია ერთი, ყველაფერის მომცველი მარეგულირებელი ორგანო, როგორც ევროპის ქვეყნებს. ძირითად ვალდებულებებს კისრულობს აშშ-ს ფედერალური ვაჭრობის კომისია (Federal Trade Commission – FTC) და ითვლება, რომ მას აქვს იურისდიქცია კომერციული კომპანიების მიერ მომხმარებელთა მონაცემთა დაცვაზე.[52] მაგრამ კომისიას აქვს ლიმიტირებული წვდომა ბანკებზე, სადაზღვევო კომპანიებზე, ზოგიერთ ინტერნეტ სერვის პროვაიდერებზე და არაკომერციულ ორგანიზაციებზე.[53] შესაბამისად, მხოლოდ კომისიის ნება, რომ იყოს მთავარი მარეგულირებელი, ვერ იქნება გადამწყვეტი, როდესაც კანონები ერთმანეთთან წინააღმდეგობაში მოდის და არც დიდ კომპანიებს არ უყვართ სახელმწიფო ზედამხედველი, მითუმეტეს, თუ კანონი არ ავალდებულებს ამას.

ასეთი მიდგომა საკმაოდ ართულებს სახელმწიფოს მხრიდან მოქალაქეთა პერსონალური მონაცემების დაცვის შესაძლებლობას და პერსონალურ მონაცემთა მფლობელებსაც, ე.წ. მონაცემთა სუბიექტებსაც უკარგავს ნდობას, როგორც კომპანიებისადმი, ასევე სახელმწიფოსადმიც. აშშ-ში არსებული სიტუაცია, კიდევ უფრო დაამძიმა 2017 და 2018 წლის მოვლენებმა, როდესაც ამერიკული კომპანია Equifax-ის მონაცემთა ბაზა გატყდა და გავრცელდა 143 მილიონი მოქალაქის

[51] Raul A. C., Faircloth E. F., Moham K V., United States, The Privacy, Data Protection and Cybersecurity Law Review - Edition 5, III, 2017, 368.

[52] Data Protection Laws of the World, United States <https://www.dlapiperdataprotection.com/index.html?t=law&c=US> [28.01.2019]

[53] O'Connor N., Reforming the U.S. Approach to data protection and privacy, <https://www.cfr.org/report/reforming-us-approach-data-protection> [30.01.2018]

პერსონალური ინფორმაცია, პოპულარულმა საძიებო სისტემამ Yahoo აღიარა, რომ მილიარდამდე ადამიანის ელექტრონული ფოსტა გატყდა, კიდევ ერთმა ამერიკულმა კომპანიამ Deep Root-მა ვერ დაიცვა სათანადოდ მონაცემთა ბაზა და დაახლოებით 200 მილიონი ამერიკელის პერსონალური მონაცემები მოიპარეს, ტაქსის კომპანია Uber-ს ქონდა იმის დამალვის მცდელობა, რომ ჰაკერებმა მოიპარეს 57 მილიონი მომხმარებლის ინფორმაცია და ბოლოს, 2018 წელს, გახმაურდა და სკანდალი გამოიწვია Facebook - Cambridge Analytica-ს საქმემ, სადაც ამ უკანასკნელმა მიითვისა 87 მილიონი მომხმარებლის პერსონალური მონაცემები და ინფორმაცია, მათ შორის 71 მილიონამდე იყვნენ ამერიკელები. მოვლენების ასეთმა განვითარებამ, მოქალაქეებს აჩვენა, რომ მათი მონაცემები არ არის სათანადოდ დაცული და ვერც სავაჭრო კომისია ვერ უზრუნველყოფს მონაცემთა სუბიექტების დაცვას სავალალო შედეგებისგან.

ერთ-ერთი ყველაზე დიდი პრობლემა, რაც გამოიკვეთა ბოლო ორ წლის გახმარებული საქმეებისგან, იყო ის, რომ კომპანიები, პირველ რიგში, ცდილობდნენ მონაცემთა ბაზის გატეხვის ინფორმაციის დამალვას, რათა შემდეგ უფრო მშვიდ გარემოში, საკუთარი მოსაზრებებითა და უკვე ჩამოყალიბებული სამომავლო გეგმებით გაეკეთებინათ განცხადება და გაესაჯაროვებინათ ბაზის გატეხვა. 2003 წელს, კალიფორნიის შტატი იყო პირველი, რომელმაც გადადგა მნიშნველოვანი ნაბიჯი კიბერ სივრცეში პერსონალურ მონაცემთა დაცვასთან დაკავშირებით და შეიმუშავა კანონი „დაცვის გატეხვის შეტყობინების“ შესახებ.[54] კანონის თანახმად, თუ კომპანიამ იზარალა საკუთარი მონაცემთა ბაზის გატეხვა, ის ვალდებულია, რომ უახლოეს შესაძლებელ მომავალში, შეატყობინოს მონაცემთა სუბიექტს, პირს, რომლის მონაცემის უკანონოდ გამოყენების შესაძლებლობაა. დროთა მანძილზე სხვა შტატებმა და ცალკეულმა სააგენტოებმა აითვისეს აღნიშნული ნორმა და 2018 წელს სამხრეთ დაკოტისა და ალაბამას შტატები გახდნენ ბოლო ტერიტორიები, რომლებმაც მიიღეს ასეთი ტიპის კანონი.

[54] California Security Breach Information Act (SB-1386) (ძალაში შევიდა 2003 წლის 1 ივლისს).

ევროკავშირის მონაცემთა დაცვის რეგულაციამ ერთი ნორმით დაარეგულირა შეტყობინების ვალდებულება და მის ეკონომიკურ ტერიტორიაზე მოღვაწე კომპანიები ვალდებული გახდა, რომ მონაცემთა ბაზის ნებისმიერი სახის დარღვევა უნდა გახდეს ცნობილი კონკრეტული სახელმწიფოს ორგანოსთვის, მაქსიმალურად სწრაფად, რაც ნიშნავს, რომ მონაცემთა სუბიექტებმაც ძალიან მალე უნდა შეიტყონ საკუთარი მონაცემების საფრთხის ქვეშ დაყენების შესახებ. ხოლო, იმის გამო, რომ აშშ-ს არ გააჩნია მსგავსი, საერთოდ კანონმდებლობა, სახელმწიფოს დასჭირდა 15 წელი, რომ სრულად, მთელი ტერიტორიის მასშტაბით დაევალდებულებინა კომპანიებისთვის ინფორმაციის შეტყობინება.

საკმაოდ დაულაგებელი და ხარვეზიანი კანონმდებლობის მიუხედავად, ამერიკის ფედერალური სავაჭრო კომისია და მეგა კორპორაციები გარკვეულწილად ახერხებენ თანაარსებობას. ის კომპანიები, რომელთაც არ ეხებათ აშშ-ს კანონები, ერთგვარი რეპუტაციის ამაღლების მიზნით, ცდილობენ, რომ ამერიკის მოქალაქეებისთვის შექმნათ სპეციალური წესები და შინაგანაწესები, ისინი, რეალურად, საკუთარი თავის დარეგულირებას ცდილობენ. ხოლო, სავაჭრო კომისია არის მთავარი ორგანო ამერიკაში, რომელსაც აქვს, კომპანიის მიერ შექმნილი, წესების დავალდებულების უფლება ამავე კომპანიებისთვის და თუ დარღვევა მნიშვნელოვანია, მაშინ სხვადასხვა სახის ჯარიმის დაკისრებაც შეუძლია.[55] კომისიას სწორედ ეს სურდა, ინტერნეტის სწრაფად განვითარების მიზნით, კომპანიები რაც შეიძლება ნაკლებად უნდა შეზღუდულიყვნენ, კომისია კი მხოლოდ კომპანიების მიერ დაწესებულ ლიმიტებს მიხედავდა. წლების მანძილზე, ამას დაემატა სხვადასხვა ფედერალური კანონები ბავშვთა დაცვისა და ჯანმრთელობის შესახებ, რომლებმაც მარეგულირებელ ორგანოდ სწორედ სავაჭრო კომისია დააყენეს. საბოლოოდ კი, სავაჭრო კომისია გახდა მონაცემთა დაცვის დე ფაქტო ფედერალური ავტორიტეტი.[56]

[55] Solove D.J., Hartzog W., The FTC and the new common law of privacy, Columbia Law Review Vol. 114, 2014, 588.

[56] Hetcher შ, The De Facto Federal Privacy Commission, The John Marshall journal of information technology & privacy law vol. 19, 2000, 19.

ამავე პერიოდში, ევროკავშირმაც ამერიკის სავაჭრო კომისიას მისცა უფლება, რომ გაეწია ზედამხედველობა აშშ-სა და ევროკავშირს შორის დადებული „უსაფრთხო ტერიტორიის შეთანხმება“ (Safe Harbor Agreement).[57]

მაგრამ, რამდენად სწორია, როდესაც ტექნოლოგიურ კომპანიებს, რომლებიც დღეს მართავენ, კიბერ სივრცეში, პერსონალურ მონაცემთა გრანდიოზულ ბაზებს და მუშაობენ, როგორც მონაცემთა მაკონტროლებლები, მიეცეთ უფლება, საკუთარი ნების საფუძველზე, როგორც თითონ მიაჩნიათ სწორად, ისე დაარეგულირონ მონაცემთა დამუშავებისა და გამოყენების წესები. ხოლო იმ ქვეყნის მთავარი მარეგულირებელი კომისია, სადაც მუშაობს ასეთი კომპანიების დიდი ნაწილი, მხოლოდ ამ შეზღუდვებზე მოქმედებდეს და სხვა არანაირი ბერკეტი არ არსებობდეს მოქალაქის პერსონალურ მონაცემთა დასაცავად.

ჯერ კიდევ, ბოლო სამი წლის სკანდალურ მოვლენებამდე, კვლევები აჩვენებდა, რომ აშშ-ს მოქალაქეები ძალიან ზრუნავდნენ პერსონალურ მონაცემთა დაცვაზე და ფიქრობდნენ ამ საკითხზე. მაგრამ, ასევე გამოჩნდა, რომ მათ არ იცოდნენ კომპანიების მიერ ინფორმაციის მოპოვების საშუალებები და კანონები, რომლებიც არეგულირებდნენ ამ ყველაფერს.[58]

4.1. კალიფორნიის მომხმარებელთა კონფიდენციალურობის კანონი (CCPA)

გამომდინარე იქიდან, რომ ინტერნეტის შექმნის შემდეგ ტექნოლოგიური კომპანიების ძალიან დიდი ნაწილი კალიფორნიის შტატშია რეგისტრირებული და

[57] საბჭოს 2000 წლის 26 ივლისის გადაწყვეტილება 2000/520/EC, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2002], O.J. L215/7.
[58] Turow J., Hoofnagle C., Mulligan D., Good N., Grossklags J., The Federal Trade Commission and consumer privacy in the coming decade, I/S: A Journal of Law and Policy for the Information Society, Vol.3:3, 2008, 744. იხ. ციტირება: Turow, Americans and Online Privacy, 4.

სწორედ მისი ტერიტორიიდან მოღვაწეობს, აშშ-ს ამ ნაწილის კანონმდებლებს დასჭირდათ, რომ უფრო სწრაფად განევითარებინათ სფეროს დარეგულირება, ვიდრე სხვა შტატებს. ამან გამოიწვია ის, რომ კალიფორნია გახდა მონაცემთა დაცვის გზამკვლევი და პირველი იყო 2003 წელს, რომელმაც მიიღო კანონი შეტყობინების ვალდებულების შესახებ, მართალია, დანარჩენმა შტატებმა 2018 წლამდე ვერ მოხერხეს ამის გაკეთება, მაგრამ ეს არ უკარგავს კალიფორნიას წინსვლისა და განვითარების მცდელობას.

თანამედროვე რეგულაციებიდან და შესაბამისი რეპუტაციიდან გამომდინარე, კალიფორნიის კანონმდებლობა ითვლება ლიდერად აშშ-ს ტერიტორიაზე და ხშირ შემთხვევაში, მის მიერ დაწესებული უფლებები და ვალდებულებები მიჩნეულია, როგოც დე ფაქტო, აშშ-ში მოღვაწე კომპანიებისთვის.[59]

ამერიკის კანონმდებლები დიდი ხანია დაობენ GDPR-ის მსგავსი რეგულაციის აუცილებლობაზე აშშ-ში. შეიძლება ბევრი ემხრობა, მაგრამ ასევე მოწინააღმდეგეც ძალიან ბევრი ყავს. ამის ნათელი მაგალითი შეიძლება ვიპოვოთ აშშ-ს ლობირების კანონმდებლობასა და მის გამოყენებაში. ლობირება საკმაოდ მგრძნობიარე თემაა ამერიკელებისთვის. ერთის მხრივ, ითვლება, რომ ლობირების აქტი დაცულია კონსტიტუციის პირველი შესწორებით: „უფლება, რომ მოითხოვო სახელმწიფოს დახმარება ისე, რომ არ ინერვიულო დასჯაზე.“[60] და ასევე, ის ითვლება, მეორე ძალიან მგრძნობიარე უფლების, თავისუფალი სიტყვის, ნაწილად. მეორეს მხრივ კი, კვლევები ადასტურებს, რომ ლობირების ინსტიტუტი ნეგატიურად გამოიყურება ამერიკელების თვალში და ის იწვევს ნდობის დაკარგვას, როგორც კომპანიაში, ასევე სახელმწიფოში.[61] ამასთან ერთად, 2018 წელს, აშშ-ს მოქალაქეებისა და სახელმწიფოს მხრიდან,

[59] Raul A. C., Faircloth E. F., Moham K V., United States, The Privacy, Data Protection and Cybersecurity Law Review - Edition 5, III, 2017, 383.

[60] ამერიკის შეერთებული შტატების კონსტიტუცია, პირველი შესწორება (ძალაში შევიდა 1791 წლის 15 დეკემბერს).

[61] Saad L., Americans Decry Power of Lobbyists, Corporations, Banks, Feds, Gallup. < https://news.gallup.com/poll/147026/Americans-Decry-Power-Lobbyists-Corporations-Banks-Feds.aspx> [11.04.2011]

პერსონალურ მონაცემთა დაცვაზე, სერიოზული ზეწოლის პერიოდში, გაირკვა, რომ ტექნოლოგიურმა გიგანტებმა: Facebook, Google, Microsoft, Apple და Twitter, მთლიან ჯამში, გამოყვეს 64 მილიონი აშშ დოლარი ლობირებისთვის. Facebook-ის სკანდალმა გააღვივა მოთხოვნა პერსონალურ მონაცემთა მეტი დაცვისთვის, მაგრამ არა იმდენად, რომ სახელმწიფოს გადაედგა საჭირო ნაბიჯები და უარი ეთქვა კომპანიების ფინანსებისთვის.

ზემოთ აღნიშნული პრობლემები, საკმაოდ ართულებს ერთი, საერთო კანონის მიღების შესაძლებლობას. ჯერ-ჯერობით, აშშ-სთვის ისევ ლოგიკურად რჩება ცალკეული კანონების მიღება შტატებისთვის და ზოგადი კანონების მიღება სპეციფიკური სფეროებისთვის, ფედერალურ დონეზე. როგორც ლიდერი სფეროში, ისევ კალიფორნიის შტატმა გადადგა პირველი ნაბიჯი კანონმდებლობის გაერთიანებისკენ და 2018 წელს ძალაში მიიღო კალიფორნიის მომხმარებელთა კონფიდენციალურობის კანონი.[62]

ახალი კანონი, რომელიც ვრცელდება მხოლოდ კალიფორნიის შტატზე, საკმაოდ გავს და ასევე, ბევრი განსხვავებაც აქვს ევროპაში, ამავე პერიოდში მიღებულ მონაცემთა დაცვის ზოგად რეგულაციას. კალიფორნიის მიერ გადადგმული ნაბიჯი ძალიან სერიოზულია, იმის გათვალისწინებით, დღეს, შტატს აქვს მეხუთე ყველაზე დიდი ეკონომიკა მსოფლიოში (დამოუკიდებელი ქვეყანა რომ იყოს)[63] და შარშან ჩამოიტოვა დიდი ბრიტანეთი ამ რეიტინგში. მიიჩნევა, რომ ახალ კანონს, რომელიც ამოქმედდება 2020 წელს, დიდი გავლენა ექნება მსოფლიო დონეზე.

კალიფორნია, ამერიკის დანარჩენ ნაწილთან ერთად, ცნობილია როგორც თავისუფალი ბაზრისა და კაპიტალიზმის მხარდამჭერად, ამიტომ საჭირო იყო სიფრთხილე ახალი კანონის მიღების დროს. მაგალითად, GDPR-გან განსხვავებით, კომპანია მხოლოდ იმ შემთხვევაში ემორჩილება კანონს, თუ ის ამუშავებს 50 000-ზე

[62] California Consumer Privacy Act (SB-1121) (ძალაში შევიდა 2018 წლის 28 ივნისს).

[63] ეკონომიკური ანალიზის ბიურო, მთლიანი შიდა პროდუქტი შტატების მიხედვით: 2018 წლის მეორე კვარტალი. [14.11.2018]

მეტი მომხმარებლის მონაცემებს კალიფორნიის შტატში, ან აქვს 25 მილიონ აშშ დოლარზე მეტი მთლიანი შემოსავალი, ან მთლიანი შემოსავლის 50%-ზე მეტი მოდის პერსონალურ მონაცემთა დამუშავებისგან. ამით ის საშუალებას აძლევს პატარა ბიზნესებს, რომ არ დაიმატონ ზედმეტი, საკმაოდ ხარჯიანი ვალდებულებები და მშვიდ გარემოში განვითარდნენ.

ახალი კანონი აღარ განასხვავებს ბიზნესის სპეციფიკურ სფეროებს და ერთი კანონმდებლობის ქვეშ აერთიანებს ყველას, ვისაც შეხება აქვს კალიფორნიასთან ან მის მოქალაქეებთან. კანონი მომხმარებლებს ანიჭებს რამდენიმე მნიშვნელოვან უფლებას: ცოდნის უფლება, თუ რა ინფორმაცია ინახება მასზე; უარის თქმის უფლება, რომ შეიზღუდოს მისი მონაცემის დამუშავება და გაყიდვა; დაცულად შენახვის უფლება, რომ შეამოწმოს რამდენად კარგად არის დაცული ინფორმაცია; დავიწყების უფლება, რომ მთლიანად წაიშალოს მასზე შეგროვებული მონაცემები.[64] ზოგადი უფლებები, პატარა ტექნიკური განსხვავების გარდა, არის ევროპული GDPR-ის ასლი.

ევროკავშირისა და კალიფორნიის კანონების მთავარი განსხვავებები თავს იჩენს ტერმინოლოგიის განმარტებებში. კალიფორნიის კანონი პერსონალურ მონაცემებს უფრო ფართო განმარტებას ანიჭებს და არ შემოიფარგლება მხოლოდ ინდივიდის მაიდენტიფიცირებელი მონაცემებით. პერსონალურ მონაცემად ჩაითვლება ინფორმაცია, რომელიც უკავშირდება ელექტრონულ მოწყობილობას ან სახლს. ამასთან ერთად, კალიფორნიის კანონი არ ეხება არაკომერციულ ორგანიზაციას და პატარა ბიზნესების მსგავსად, საშუალებას აძლევს მათ შეუზღუდავად ამუშაონ პირთა პერსონალური მონაცემები.[65] GDPR მორგებულია თანამედროვე ავტომატიზირებულ სისტემებზე, რომლებიც ადამიანების ჩარევის გარეშე ინახავენ და ამუშავებენ ინფორმაციას და კანონის მიერ დადგენილი შეზღუდვები ეხება ასეთ სისტემებს, ევროკავშირის რეგულაციები ხელს უშლის ამ პროცესს და საშუალებას აძლევს

[64] Bartley P. The California Consumer Privacy Act: not just 'America's GDPR', 451 Research, 2019, 4.
[65] California Consumer Privacy Act (SB-1121) (ძალაში შევიდა 2018 წლის 28 ივნისს), სექცია 1798.140 (c).

მოქალაქეებს, რომ დაიცვან საკუთარი ინფორმაცია ამისგან. კალიფორნიის კანონმა არჩია, რომ არ ეხსენებინა ასეთი ტექნიკური საკითხები იმის შიშით, რომ არ შეეშალა ხელი შტატში მოღვაწე ტექნოლოგიური კომპანიებისთვის და მიეცა მათთვის ინოვაციების საშუალება.[66]

ლოგიკურიც არის, რომ კალიფორნიის კანონი გამოსვლისთანავე გახდა განხილვის საგანი და ბოლო ერთი წლის განმავლობაში გამოქვეყნებული კვლევების დიდი ნაწილი ადარებს მას ევროკავშირის რეგულაციებს. გარკვეული განსხვავებების გარდა, ფუნდამენტი ორივე კანონს ერთი აქვს: საკუთარი მოქალაქეები პერსონალურ მონაცემთა დაცვა და კომპანიების გაკონტროლების მინიმალური საშუალებები, ნებისმიერ სფეროში, გარე რეგულაციებისა და დამატებითი მესამე პირების გარეშე. ორივე კანონმდებლობა ითხოვს ორგანიზაციებისგან ტექნოლოგიური ინფორმაციული წყაროების დაცვას.

კალიფორნია არამარტო ძალიან მაღალი მთლიანი შიდა პროდუქტის მქონეა, ის, ასევე, აშშ-ს ყველაზე დიდი შტატია მოსახლეობის მიხედვით, დაახლოებით 12%. შესაბამისად, კალიფორნია დარწმუნებულია, რომ აქვს სერიოზული ძალა გააკონტროლოს ტექნოლოგიური კომპანიები, რომ ამ უკანასკნელებმა, წინ დააყენონ ახალი კანონი და არა სხვა შტატის მიერ მიღებული რომელიმე რეგულაცია. მართალია, GDPR-თან ერთად, კალიფორნიის კანონის დამორჩილება უფრო დიდ ხარჯებთან იქნება დაკავშირებული დიდი კომპანიებისთვის, მაგრამ ახალი კანონი ხელს შეუწყობს პერსონალურ მონაცემთა დაცვის რეგულაციების ჰარმონიზაციას. კალიფორნია იყენებს საკუთარ პოზიციას სახელმწიფოს ეკონომიკაში და ცდილობს, რომ მოახდინოს გლობალური გავლენა. გამოუვა თუ არა ეს, ამას ვიხილავთ 2020 წლის შემდეგ.

[66] იხ. შენიშვნა 62, გვერდი 42 ნაშრომში.

4.2. აშშ-სა და ევროკავშირის სავალდებულო ურთიერთობა

მსოფლიოს ორი ძალიან დიდი ძალა, მჭიდრო კავშირშია ერთმანეთთან. ბოლოს და ბოლოს, აშშ და ევროკავშირის ერთმანეთის უმსხვილესი ეკონომიკური და სავაჭრო პარტნიორები არიან. შესაბამისად, საწინააღმდეგო სურვილის მიუხედავად, ორივეს უწევს გარკვეულ დათმობებზე წასვლა და მეორე მხარის გათვალისწინება კონკრეტულ საკითხებში.

არც პერსონალურ მონაცემთა დაცვის სფერო არ არის განსხვავებული. ინტერნეტის განვითარებასთან ერთად, აშშ-სა და ევროკავშირის ურთიერთობაც საგრძნობლად შეიცვალა. ევროკავშირს, 1995 წელს გამოშვებული დირექტივიდან მოყოლებული, სურს, რომ მაქსიმალურად გააერთიანოს სხვადასხვა სახელმწიფოს რეგულაციები და აიძულოს მათ მსგავს კანონმდებლობაზე ყოფნა. არც ამერიკასთან მიმართებაში არ განსხვავდება ევროკავშირი, ყოველ შემთხვევაში, ცდილობს მაინც, რომ არ იყოს განსხვავებული. მაგრამ, აშშ-ს პოზიცია მსოფლიო პოლიტიკასა და ეკონომიკაში, საკმაოდ ართულებს ამ საქმეს.

ნაშრომის მესამე თავში განხილულია 1995 წლის დირექტივის მიერ ჩამოყალიბებული და 2018 წლის რეგულაციის მიერ განვრცობილი მესამე ქვეყნების ინსტიტუტი. ნებისმიერო სახელმწიფო, რომელიც არ შედის ევროკავშირისა და ევროკავშირის ეკონომიკური ტერიტორიის ნაწილში, ითვლება მესამე ქვეყნად და ვალდებულია, რომ გაიაროს ევროკავშირის საბჭოს მიერ შემუშავებული, სპეციალური შემოწმების ფაზა, რომლის გავლაც საკმაოდ რთულია.[67] ამ შემოწმებების გავლისა და სახელმწიფოს მიერ სერიოზული რეგულაციების შემუშავების მიუხედავად, სრულებით შესაძლებელია, რომ უარი მიიღოს მესამე ქვეყნის სტატუსის მოპოვებაზე, რადგან საბოლოოდ, ეს ევროკავშირის საბჭოს დისკრეციული უფლებამოსილებაა და

[67] IT Governance Privacy Team, Managing Personal Data Internationally, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, დიდი ბრიტანეთი, 2017, 251.

არანაირი ვალდებულება არ არსებობს, რომ კონკრეტულ სახელმწიფოს აუცილებლად უნდა მიენიჭოს სტატუსი.[68]

მესამე სახელმწიფოს სტატუსს ოფიციალურად ვერ მიიღებს ამერიკის შეერთებული შტატები, რადგან ქვეყანას არ გააჩნია ზოგადი, ყველაფრის მომცველი კანონმდებლობა და შტატები მხოლოდ და მხოლოდ ცალკეულად ცდილობენ არეულობის მოგვარებას. ეს ძალიან დიდი პრობლემას ქმნის ეკონომიკურ და სამართლებრივ სფეროში. ევროკავშირი კრძალავს ევროპის მოქალაქეების პერსონალურ მონაცემთა გაცვლას და გატანას მისი ქვეყნების გარეთ, თუ მას არ გააჩნია მესამე ქვეყნის სტატუსი, ხოლო ამერიკა კი, ბოლო 30 წლის მანძილზე, იქცა ყველაზე მსხვილი ტექნოლოგიური კომპანიების სახლი, რომლებიც საკუთარი ოპერაციების დიდ ნაწილს, სწორედ აშშ-ს ტერიტორიაზე ახდენენ.

იმ მიზნით, რომ საფრთხე არ შექმნოდა აშშ-ევროკავშირის სავაჭრო ურთიერთობას, 1995 წლის დირექტივის გამოცემასთან ერთად, აშშ-ს ვაჭრობის დეპარტამენტმა შეიმუშავა ე.წ. „მონაცემთა დაცვის უსაფრთხო ნავსაყუდელის პრინციპები“ (Safe Harbor Privacy Principles), რომელიც აღიარა ევროპის ორგანიზაციამ 2000 წელს[69], რითაც საშუალება მისცა კომპანიებს, რომ გარკვეული უსაფრთხოების წესების დაცვით, გადაეტანათ მოქალაქეთა პერსონალური მონაცემები აშშ-ს ტერიტორიაზე.[70]

“უსაფრთხო ნავსაყუდელის“ პრინციპი არ არის ახალი სამართლებრივ სფეროში. მისი მიზანია, რომ შექმნას სპეციალური სამოქმედო გეგმა, რის შემდეგაც პირი დაცული იქნება კანონის დარღვევისგან. პერსონალურ მონაცემთა დაცვის შემთხვევაში, აშშ და ევროკავშირი შეთანხმდნენ, რომ თუ კომპანია ასრულებდა

[68] იქვე, 252.
[69] კომისიის 2000 წლის 26 ივლისის გადაწყვეტილება 2000/520/EC, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce. [2000]
[70] Weiss M.A., Archick K., U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, 2016, 5.

მინიმალურ მოთხოვნებს, მაშინ ის აღარ ჩაითვლებოდა 1995 წლის დირექტივის დამრღვევად. ამით აშშ ვერ იღებდა მესამე ქვეყნის სტატუსს, მაგრამ კომპანიები უფრო მშვიდად და უსაფრთხოდ ასრულებდნენ მნიშნველოვან საქმიანობას პერსონალურ მონაცემთა დაკავშირებით.

პრინციპების მიხედვით, კომპანიას უნდა შეესრულებინა შვიდი აუცილებელი მოთხოვნა: პირის შეტყობინება თუ რატომ აგროვებს მის პერსონალურ ინფორმაციას; პერსონალურ მონაცემთა შეგროვებაზე უარის თქმის შესაძლებლობა; მესამე პირებთან პერსონალური მონაცემების გაცვლის შემთხვევაში, იმ მესამე პირის შემოწმება, თუ აკმაყოფილებს მოთხოვნებს; მონაცემთა ბაზების დაცვის საჭირო სტანდარტების შედგენა; მხოლოდ საჭირო მონაცემთა შეგროვება; პირის უფლება, რომ იცოდეს რა ინფორმაცია ინახება და შეძლოს მისი შეცვლა ან წაშლა; ამ ნორმების შესრულების იძულება, ანუ არსებობდეს ისეთი საფეხურები, რომელიც უზრუნველყოფს კომპანიის მხრიდან, ზემოთ ხსენებული მოთხოვნების იძულებას.

2000 წლის გადაწყვეტილების მიხედვით, ზემოთ ხსენებული მოთხოვნები უნდა დაეცვა და გაეკონტროლებინა ფედერალურ სავაჭრო კომისიას და ნებისმიერ კომპანიას შეეძლო დარეგისტრირება. სისტემატიური დარღვევების შემთხვევაში, კომპანია ავტომატურად წაიშლებოდა უსაფრთხო ნავსაყუდელის სიიდან და ვეღარ შეძლებდა ევროკავშირის ქვეყნების მოქალაქეების მონაცემთა შეგროვებასა და დამუშავებას.

2000 წლის გადაწყვეტილება საჭირო იყო ევროკავშირისა და აშშ-ს მშვიდი ეკონომიკური კურსის გასაგრძელებლად. ამით, ორივე მხარემ დაიზღვია თავი საქმიანობის შესაძლო გართულებისგან, რადგან აშშ ავტომატურად ვერ ჯდებოდა ევროკავშირის მესამე ქვეყნების მოთხოვნილებებში და როგორც ყველაზე დიდი პარტნიორი, საჭირო იყო გამოსავლის მოძებნა. მიღებული მნიშვნელოვანია იმის გააზრება, რომ 1995 წლის დირექტივა და 2000 წლის გადაწყვეტილება, შედგა იმ ეპოქაში, როდესაც ინტერნეტი და პირადული მონაცემები იყო ახალი მცნება, როგორც

კანონმდებლებისთვის, ასევე მომხმარებლებისთვისაც. შესაბამისად, ლოგიკურია, რომ არ იყო განჭვრეტილი შემდეგი ათწლეულის ტექნოლოგიური მოვლენები. საბოლოოდ, ეს ყველაფერი აისახა აშშ-ს „უსაფრთხო ნავსაყუდლების“ კანონიერების დაკარგვაში[71], როდესაც მაქსიმილიან შრემსმა გაასაჩივრა „ფეისბუქის“ აქტივობები ირლანდიის მონაცემთა დაცვის კომისართან.

Maximillian Schrems v. Data Protection Commissioner (შრემსი „უსაფრთხო ნავსაყუდლების“ წინააღმდეგ)

2013 წელს, ედვარდ სნოუდენის გახმაურებული სკანდალის შემდეგ, ავსტრიის მოქალაქე მაქსიმილიან შრემსმა საჩივარი შეიტანა ფეისბუქის წინააღმდეგ, ირლანდიის მონაცემთა დაცვის კომისართან. საჩივრის თანახმად, ევროკავშირის მოქალაქეები ხელშეკრულებას აფორმებდნენ ფეისბუქის ირლანდიურ კომპანიასთან, ხოლო შემდეგ ეს კომპანია, უსაფრთხო ნავსაყუდლების დაყრდნობით, გადასცემდა შეგროვებულ ინფორმაციას აშშ-ში რეგისტრირებულ ფეისბუქს. მოსარჩელე ითხოვდა ირლანდიის კომისარისგან, რომ შეწყვეტილიყო მისი პერსონალური ინფორმაციის გადატანა აშშ-ს კომპანიაში. მიზეზი კი იყო უნდობლობა აშშ-დმი, რადგან ეს უკანასკნელი ვერ ახდენდა მონაცემთა სათანადო დაცვის უზრუნველყოფას, ეს კი ცნობილი გახდა ედვარდ სნოუდენის მიერ გავრცელებული მასალებისგან, რომ ნაციონალური დაცვის სააგენტო, ტექნოლოგიური კომპანიების დახმარებით აგროვებდა გარკვეულ ინფორმაციებს. კომისიამ იმსჯელა წარდგენილ საჩივარზე და განმარტა, რომ ამერიკის შეერთებულ შტატებს აქვს პერსონალურ მონაცემთა დაცვის ადექვატური დონე და არ არსებობდა არანაირი სამხილი, რომ ნაციონალურ დაცვის სააგენტოს ქონდა მოსარჩელის ინფორმაცია.[72]

[71]საქმე C-312/14, Maximillian Schrems v Data Protection Commissioner [2015].
[72] იქვე, 28-30.

აღნიშნული გადაწყვეტილება, მოსარჩელემ გაასაჩივრა ირლანდიის სასამართლო, ხოლო ამ უკანასკნელმა საქმე განსახილველად გადასაცა ევროკავშირის მართლმსაჯულების სასამართლოს, რადგან აშკარა იყო აშშ-ს სახელმწიფო სააგენტოების მხრიდან დარღვევები. სასამართლომ დეტალურად განიხილა, კომისიის მიერ აღიარებული „მონაცემთა დაცვის უსაფრთხო ნავსაყუდელის პრინციპები“ და დაადგინა, რომ არ არსებობდა იმის დამადასტურებელი ფაქტი, რომ ეს Safe Harbor-ები ადექვატურად იცავდა ევროკავშირის მოქალაქეთა პერსონალურ მონაცემებს აშშ-ს ტერიტორიაზე. მთავარი პრობლემა იყო ის, რომ მისი მუხლები მოდიოდა 1995 წლის დირექტივის ნორმებთან წინააღმდეგობაში. სასამართლოს განმარტებით, არ არის აუცილებელი, რომ მესამე სახელმწიფოს გააჩნდეს ზუსტად იგივე მექანიზმები, მაგრამ მნიშვნელოვანია, რომ ის გავდეს მონაცემთა დაცვის დირექტივას.[73] სახელმწიფოს უნდა გააჩნდეს ფუნდამენტური უფლებების დაცვის ძალიან მაღალი დონე და ამაზე წინ არ უნდა დგებოდეს სახელმწიფო უსაფრთხოება, საჯარო ინტერესი ან რომელიმე სამართალდამცავი ორგანო. ამასთან ერთად, დირექტივასთან მსგავსება უნდა მოწმდებოდეს პერიოდულად.

სასამართლომ პრობლემატურად ცნო პრინციპების კიდევ ერთი მუხლი, რომლითაც სახელწმიფო ავტორიტეტებს არ ქონდათ უფლება, რომ შეემოწმებინათ ინდივიდების განცხადებები და მოთხოვნები. ეს პირდაპირ წინააღმდეგობაში მოდიოდა დირექტივასთან.[74]

მართლმსაჯულების სასამართლოს გადაწყვეტილებამ, რომელიც გამოცემისთანავე შევიდა ძალაში, არასამართლებრივი გახადა 2000 წელს, კომისიის გადაწყვეტილება, რომლითაც საფუძველი ჩაედო „უსაფრთხო ნავსაყუდლების“ შექმნას პერსონალურ მონაცემთა დაცვის სფეროში. ამერიკის მხრიდან დიდი დამწუხრების მიუხედავად, სამომავლო გეგმები ორივე მხარისთვის ნათელი იყო: რაც

[73] იქვე, 61-65.
[74] საქმე C-312/14, Maximillian Schrems v Data Protection Commissioner [2015], 100-106.

შეიძლება მალე, უნდა შექმნილიყო ახალი დოკუმენტი, რომელიც აღმოფხვრიდა უკვე ძალა დაკარგული პრინციპების პრობლემებს და შეეცდებოდა ევროკავშირის პოზიციასთან, პერსონალურ მონაცემთა დაცვის შესახებ, დაახლოებას. შეიძლება ძველმა დოკუმენტმა ძალა დაკარგა, მაგრამ ის ფაქტი ძალაში დარჩა, რომ ნებისმიერი კომპანიის მხრიდან, მონაცემთა იმ ქვეყანაში გადაგზავნა, რომელსაც არ აღიარებს ევროკავშირი, იყო სამართალდარღვევა.[75]

2013 წლიდან მოყოლებული, 3 წლიანი მუშაობის შემდეგ, 2016 წლის თებერვალში, აშშ-სა და ევროკავშირის ოფიციალურმა წარმომადგენლებმა საჯარო გახადეს ახალი დოკუმენტი, ხოლო ამავე წლის 12 ივლისს კომისიის გადაწყვეტილებით, სრული ძალა მიიღო US – EU Privacy Shield-მა (აშშ - ევროკავშირის კონფიდენციალურობის ფარი).[76]

ახალმა დოკუმენტმა მაქსიმალურად აღმოფხვრა სასამართლოს მიერ წარმოდგენილი პრობლემები და გააძლიერა მოთხოვნის ის სტანდარტები, რომლებიც იყვნენ „უსაფრთხო ნავსაყუდელის“ პრინციპებში. მაგრამ, საინტერესო პრობლემა ის არის, რომ 2016 წელს ჯერ კიდევ არ იყო ძალაში შესული ევროკავშირის GDPR და მოქმედებდა 1995 წლის დირექტივა. ამასთან ერთად, ევროკავშირის მონაცემთა დაცვის სამუშაო ორგანომ სამუშაო ვადა დაუწესა აშშ-სა და ევროკავშირს,[77] შესაბამისად, ოფიციალური მხარეები ვეღარ დაუცდიდნენ ახალი რეგულაციების ძალაში შესვლას და ვალდებულები იყვნენ, რომ კონფიდენციალურობის ფარი მოერგოთ მონაცემთა დაცვის დირექტივაზე. აქედან გამომდინარე, ახალი რეგულაციები მაქსიმალურად მორგებულია, აწ უკვე ძალადაკარგულ დირექტივაზე და მხოლოდ ზოგადად იცავს GDPR-ის მოთხოვნებს.

[75] IT Governance Privacy Team, Managing Personal Data Internationally, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, 257, დიდი ბრიტანეთი, 2017.
[76] კომისიის გადაწყვეტილება 2016/1250, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016].
[77] Weiss M.A., Archick K., U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, 2016, 9.

აღნიშნული პრობლემა წინ წამოწია მონაცემთა დაცვის სამუშაო ორგანომ და GDPR-ის გარდა განაცხადა, რომ ახალ ფარს ჭირდებოდა კიდევ უფრო მეტი დახვეწა, რადგან მას ქონდა რამდენიმე ფუნდამენტური პრობლემა: აშშ-ს კომპანიების არ გააჩნიათ მონაცემთა წაშლის ვალდებულება, როდესაც ის აღარ ჭირდებათ; აშშ-დან მესამე ქვეყანაში მონაცემთა გადაცემა არ არის სათანადოდ დაცული; ანაზღაურების მექანიზმები არის არასაჭიროდ კომპლექსური; დოკუმენტი არ უკრძალავს აშშ-ს სახელმწიფო ორგანოებს, რომ შეაგროვონ პერსონალურ მონაცემები (რის გამოც დაიწყო ყველაფერი).[78]

დღეს, აშშ და ევროკავშირი ისევ კონფიდენციალურობის ფარის დოკუმენტის თანახმად მოქმედებენ, რომელიც არ განახლებულა 2016 წლის შემდეგ და მხოლოდ ზოგადად ექვემდებარება ევროკავშირის მიერ მიღებულ ახალ რეგულაციებს. ეს ვითარება საკმაოდ უცნაურ მდგომარეობაში აყენებს ევროკავშირსა და მის მიერ შექმნილ - პერსონალურ მონაცემთა დაცვის საბჭოს, რომელმაც უნდა განიხილოს და შეაფასოს მესამე ქვეყნების საქმიანობები. აშშ დღემდე რჩება ყველაზე მჭიდრო ეკონომიკურ პარტნიორად ორგანიზაციისთვის და ნებისმიერი არასწორად გადადგმული ნაბიჯი, გამოიწვევს ორივე მხარის დაზარალებას. ამას ემატება აშშ-ში მოღვაწე ტექნოლოგიური კომპანიების უფრო და უფრო მზარდი როლი მსოფლიოში, რომლებიც ასევე არიან მონაცემთა ყველაზე დიდი მაკონტროლებლები. ურთიერთობა ძალიან ფრთხილი და დელიკატურია. როდესაც მონაცემთა დაცვის სამუშაო ორგანომ წარადგინა არსებული პრობლემები, აშშ-ს კომერციის დეპარტამენტის დირექტორმა განაცხადა, რომ ეს კომენტარები იყო მნიშვნელოვანი, მაგრამ რთული იქნებოდა დოკუმენტის კიდევ ერთხელ გადახედვა.[79] ეს აშკარა უარი იყო, რომ მინიმუმ რამდენიმე წელი, დოკუმენტში ჩარევა არ განხორციელდება არცერთი მხარის მიერ.

[78] Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 2016, 57.

[79] Fioretti J., U.S. reluctant to change data pact after EU watchdogs' concerns, Reuters, 2016.

ევროკავშირს ძალიან მკაცრი დამოკიდებულება აქვს მესამე ქვეყნების მიმართ. მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვის დირექტივა 1995 წლიდან არსებობს და მის ქვეშ მიღებული მესამე ქვეყნის სტატუსი მოქმედებს GDPR-ის ქვეშაც, მხოლოდ და მხოლოდ 11-მა ქვეყანამ მოახერხა ამის გაკეთება.[80] ამ სიაში აშშ საერთოდ არ შედის, რადგან ის ვერ განიხილება მესამე ქვეყნად, რადგან ერთი საერთო კანონიც კი არ არსებობს სახელმწიფოში, პერსონალურ მონაცემთა დაცვის შესახებ. აშშ, ფაქტობრივად, საკუთარი პოლიტიკური და ეკონომიკური სტატუსის გამო ახერხებს, რომ გარკვეულწილად უგულებელყოს ევროკავშირის მოთხოვნები და მაქსიმალურად ცადოს საკუთარი წესებით თამაში.

არავინ არ იცის რა მოხდება 2020 წლიდან, როდესაც ძალაში შევა კალიფორნიის შტატის კანონი მომხმარებელთა კონფიდენციალურობის დაცვის შესახებ. თუ მისი დამორჩილება მოუწევს აშშ-ში მყოფ ყველა დიდ კომპანიას, რადგან ისინი საქმიანობას აწარმოებენ სწორედ კალიფორნიაში, მაშინ არ არის გამორიცხული, რომ კანონის ათვისება მოხდეს სხვადასხვა შტატებისგანაც. თუ მსოფლიო იხილავს მოვლენების ასეთ იდეალურ განვითარებას, მაშინ აშშ შეძლებს, რომ ზედმეტი რეგულაციებისა და დამატებითი დოკუმენტების გარეშე, მიიღოს მესამე ქვეყნის სტატუსი, ევროკავშირის პერსონალურ მონაცემთა დაცვის საბჭოსგან. ეს საშუალებას მისცემს ორივე მხარეს, რომ ნებისმიერი „უხერხულობისა“ და ზედმეტი თვალის დახუჭვის გარეშე, აწარმოონ ეკონომიკური საქმიანობა ერთმანეთთან და კომპანიებსაც მიეცემათ საშუალება, რომ საკუთარი რეგულაციები და წესები მოაქციონ ერთი ქოლგის ქვეშ.

[80] IT Governance Privacy Team, Managing Personal Data Internationally, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, 253, დიდი ბრიტანეთი, 2017.

5. საქართველო და პერსონალურ მონაცემთა დაცვა

მე-20 საუკუნის 70-იან წლებში, როდესაც მსოფლიო იწყებდა ზრუნვას პერსონალურ მონაცემთა დაცვის შესახებ რეგულაციებზე, საბჭოთა კავშირსა და შესაბამისად, საქართველოში, ეს სფერო ნამდვილად არ მიიჩნეოდა პრობლემატურად. ასეთი კანონი, იმ დროინდელი წყობისთვის, არანაირ საჭიროებას არ წარმოადგენდა. ამის აშკარა მიზეზებზე საუბრის მაგივრად, უფრო ლოგიკური იქნება, რომ მხოლოდ საქართველოს უახლესი წარსული გავაანალიზოთ და დავინახოთ, თუ რა ნაბიჯები გადადგა საქართველომ, როგორც დამოუკიდებელმა სახელმწიფომ.

90-იანი წლების განმავლობაში, როდესაც ევროკავშირმა მიიღო პერსონალურ მონაცემთა შესახებ დირექტივა და ამერიკამ დაიწყო სექტორული დარეგულირება, საქართველოში აღარ იყო საბჭოთა კავშირი, მაგრამ იყო სამოქალაქო ომი. ხოლო მეორე ნახევარში, პერსონალურ მონაცემთა დაცვის შესახებ რეგულაციების შემუშავებაზე მნიშვნელოვანი იყო სამოქალაქო კოდექსის, სისხლის სამართლის კოდექსისა და სხვა კანონების მიღება, რომლებიც ძირითად საკანონმდებლო ბაზას შექმნიდნენ დამოუკიდებელი საქართველოსთვის.

მრავალწლიანმა ინფორმაციულმა ვაკუუმმა, გამოიწვია პერსონალურ მონაცემთა დაცვის შესახებ კანონის უგულებელყოფა. მხოლოდ 2011 წლის ბოლოს მიიღო პარლამენტმა კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ და ის ამოქმედდა მომდევნო წელს.[81] ხოლო, 2013 წლის 1 ივლისს შეიქმნა პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, როგორც სახელმწიფოს საზედამხედველო ორგანო. მიუხედავად იმისა, რომ საქართველოში კიბერ სივრცე, მათ შორის ელექტრონული კომუნიკაციები მოგვიანებით განვითარდა, ის მაინც ძალიან სწრაფად აითვისა როგორც საჯარო სექტორმა, ასევე კერძო სექტორმაც და საქართველოს მოქალაქეებმა აქტიურად დაიწყეს თანამედროვე ინფორმაციული ტექნოლოგიების

[81] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011

შესწავლა. ეს ყველაფერი, გარკვეულწილად, 2011 წლის პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონშიც აისახა, მაგალითად, მისი მეორე მუხლი, გამოყოფს მონაცემთა სამი სახის დამუშავებას: ავტომატური, ნახევრად ავტომატური, არაავტომატური.[82] ნებისმიერი ინფორმაცია, რომელიც მუშავდება ელექტრონული საშუალებით, იგულისხმება, რომ მუშავდება ავტომატურად. საქართველოს კანონი ამას არ ამბობს ცხადად, მაგრამ, როგორც „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის“ შესახებ ევროპული კონვენციის ხელმომწერი სახელმწიფო, იზიარებს კონვენციის მიერ დადგენილ ავტომატურ საშუალებებს, რადგან ეს უკანასკნელი დეტალურად განმარტავს, თუ რას ნიშნავს პერსონალურ მონაცემთა ავტომატური დამუშავება.[83] განმარტების გარდა, მონაცემთა ავტომატურ დამუშავებაზე საქართველოს კანონი არ ამახვილებს განსაკუთრებულ ყურადღებას. ის იგივე სტანდარტების ქვეშ ექცევა, როგორც ნახევრად ავტომატური და არაავტომატური დამუშავება.

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

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

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

[82] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011, მუხლი 2 (დ).

[83] არჩუაძე თ., პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016, 26. იხ. ციტატა: ,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენცია, CETS No.108, (მიღებულია 1981 წლის 28 იანვარს, ძალაში შევიდა 1985 წლის 1 ოქტომბერს), მე-3 მუხლის 1-ლი ნაწილი.

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.“[84]

აღსანიშნავია, რომ აღნიშნული პრინციპები და ზოგადად კანონი, აძლევს მონაცემთა სუბიექტს საშუალებას, რომ მოითხოვოს საკუთარი ინფორმაციის წაშლა,[85] საქართველოს კანონი, გარკვეულწილად, აღიარებს „დავიწყების უფლების“ პრინციპს. ასევე, კანონი არ საუბრობს კიბერ სამყაროს გამოწვევებზე და არ ჩადის ისეთ ტექნიკურ სიღრმეებში, როგორც GDPR ან კალიფორნიის კანონი.

პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატისთვის, ორი რამ არის უაღრესად მნიშვნელოვანი, მკაცრად აკონტროლოს საჯარო და კერძო პირების მიერ რა ინფორმაცია მუშავდება, როგორ მუშავდება და თუ სათანადო ვალდებულებებს არ იღებს პირი, მაშინ დააჯარიმოს ის. კანონში ნაკლებად არის საუბარი მონაცემთა სუბიექტებზე, მათ უფლებებსა და შესაძლებლობებზე. მთავარი ფოკუსი კეთდება იურიდიული პირების ქმედებებზე. ნებისმიერი ბიზნესი, რომელიც საქართველოს ტერიტორიაზე ამუშავებს ე.წ. „ფაილურ კატალოგს“, ვალდებულია, რომ შეავსოს სპეციალური ფორმა პერსონალურ მონაცემთა დაცვის ინსპექტორის საიტზე და თუ მიუთითებს მონაცემთა შენახვის ვადასა, მიზეზს და დაცვის ზოგად წესებს,

[84] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011, მუხლი 4.

[85] იქვე, მუხლი 15 (დ).

პრობლემების გარეშე შეუძლია საქმიანობის გაგრძელება. ვალდებულება აკისრია ნებისმიერ ბიზნესს, რომელიც რეგისტრირებულია საქართველოში და ამუშავებს მონაცემებს (კანონის მესამე მუხლით, არ კონკრეტდება საქართველოს მოქალაქე) ან არ არის რეგისტრირებული საქართველოში, მაგრამ იყენებს საქართველოს ტერიტორიაზე არსებულ ტექნიკურ საშუალებებს, ინფორმაციის დამუშავებისთვის.[86]

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი კარგი დასაწყისია იმ სახელმწიფოსთვის, რომელსაც არანაირი გამოცდილება არ აქვს სფეროში, მაგრამ ის ზედმეტად მარტივი და ზოგადია იმისთვის, რომ სერიოზული გავლენა იქონიოს ბიზნესებზე, მისი მოქმედების გავრცელების სფერო არის საკმაოდ ვიწრო და კანონი თავს არიდებს კომპლექსურ და ტექნიკურ დეტალებს, რაც ავტომატურად საშუალებას აძლევს ბიზნესებს, რომ საკუთარი დისკრეციული უფლებამოსილებით იმოქმედონ და არ დაემორჩილონ მონაცემთა ბაზების დაცვის არანაირ მინიმუმს.

საქართველოს კანონი მკაცრად ერგება ტერიტორიას და არა ამ ტერიტორიაში მცხოვრებ პირებს. ის უგულებელყოფს თანამედროვე ტექნოლოგიურ შესაძლებლობებს და არც დირექტივას და არც ახალ რეგულაციებს არ იზიარებს. მთავარი არის, რომ მონაცემები მუშავდებოდეს საქართველოს ტერიტორიაზე. ეს დათქმა უცნაურ მდგომარეობაში აგდებს, როგორც კერძო ბიზნესებს, ასევე საჯარო იურიდიულ პირებსაც. რა მოხდება, თუ რომელიმე სამინისტრო, რომელიც დიდი მოცულობით პერსონალურ ინფორმაციას ამუშავებს, გადაწყვეტს, რომ გამოიყენოს უცხოეთში არსებული კომპანია, როგორც მონაცემთა პროცესორი. ამასთან ერთად, გამოიყენოს ისეთი ქვეყანა, რომელსაც არანაირი კანონი არ გააჩნია მონაცემთა დაცვის შესახებ. ამ ორი წინაპირობით, საქართველოში რეგისტრირებულ ნებისმიერ კომპანიას და ნებისმიერ საჯარო იურიდიულ პირს, შეუძლია, რომ აარიდოს საქართველოს კანონს თავი და ყველანაირი შეზღუდვის გარეშე მიიღოს, დაამუშაოს და გამოიყენოს

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

(თუნდაც გაყიდოს) მათ მიერ მიღებული პერსონალური ინფორმაციები. ამ შემთხვევაში, პერსონალურ მონაცემთა დაცვის ინსპექტორი და საქართველოს მოქალაქეთა პერსონალური მონაცემების უსაფრთხოება, დამოკიდებული ხდება კომპანიის კეთილ ნებაზე. საქართველოს კანონი ითვალისწინებს მონაცემთა დამმუშავებელ მესამე პირს, მაგრამ მისი რეგულირების სფერო ვრცელდება მხოლოდ და მხოლოდ საქართველოში არსებულ დამმუშავებელ პირებზე.[87]

ტერიტორიაზე ორიენტირებული კანონის მეორე პრობლემა იკვეთება, როდესაც საქმე ეხება საერთაშორისო, მულტი-ნაციონალურ კომპანიებს, რომლებიც მართავენ და ამუშავებენ მილიარდობით ადამიანის პერსონალურ მონაცემებს, მათ შორის საქართველოს მოქალაქეებისასაც. მაგალითად, თუ ავიღებთ ბოლო ორი წლის ყველაზე საკამათო და საქართველოში ყველაზე აქტიურ სოციალურ ქსელს - ფეისბუქს. საქართველოს არ იცავს ევროკავშირის რეგულაციები და მითუმეტეს არ დაიცავს კალიფორნიის კანონი. შესაბამისად, სახელმწიფოს მხოლოდ და მხოლოდ საკუთარი კანონი იცავს. დღევანდელი კანონმდებლობის თანახმად, როდესაც ფეისბუქი აგროვებს პერსონალურ მონაცემებს საქართველოდან, თუ კომპანია არ ამუშავებს მონაცემებს საქართველოს ტერიტორიაზე, მაშინ მას შეუძლია, რომ შეუზღუდავად, შეაგროვოს ყველაფერი რაც უნდა. ამ შემთხვევაში, კომპანიის ერთადერთი მარეგულირებელი საკუთარი თავია, ვებსაიტზე განთავსებული კონფიდენციალურობის წესებით.

ამით ნათელი ხდება, რომ საქართველოს კანონი საერთოდ არ არის მორგებული საერთაშორისო დონეზე. მისი მთავარი მიზანია, რომ გააკონტროლოს ურთიერთობა, საქართველოს მასშტაბით, დამსაქმებელსა და დასაქმებულს შორის. მისცეს საშუალება დამსაქმებელს, რომ იცოდეს, თუ რა სახის პირადი ინფორმაცია ინახება კომპანიასთან და ამუშავებს, თუ არა კონკრეტული კომპანია ამ ინფორმაციას სათანადოდ. ამასთან ერთად, დამსაქმებელი ვალდებული ხდება კანონით, რომ შეატყობინოს მონაცემთა

[87] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, N5669-რს, საქართველოს საკანონმდებლო მაცნე, 28.12.2011, მუხლი 16.

სუბიექტს ინფორმაციის დამუშავების მიზანი, დამმუშავებლის ვინაობა, სუბიექტის უფლებები.[88]

საქართველოს მოსახლეობა ჯერ ვერ იაზრებს, თუ რამდენად მნიშვნელოვანია პერსონალურ მონაცემთა დაცვა. დიდი ნაწილისთვის, არ აქვს მნიშვნელობა, თუ რას ეთანხმება, როდესაც რეგისტრირდება სხვადასხვა საიტებზე, არ აქვს გააზრებული, თუ როგორ და რისთვის შეუძლიათ დიდ კომპანიებს, რომ გამოიყენონ ადამიანთა პერსონალური მონაცემები ან რა საშიშროება არსებობს, თუ მათ შესახებ ინფორმაცია ჩავარდა არასასურველ პირებთან.

ზოგადად, ყოველთვის რთულია იმაზე საუბარი, თუ როგორ უნდა მოხდეს კონკრეტული კანონის იმპლემენტაცია საგრძნობლად განვითარებული სახელმწიფოებისგან. მნიშვნელოვანია იმის გააზრება, რომ პერსონალურ მონაცემთა დაცვა განსხვავდება რეგულირების სხვა სფეროებისგან. პირის ცხოვრების კონფიდენციალურობა და პირად მონაცემთა დაცვა ევროკავშირმა მიიჩნია, როგორც ადამიანის ფუნდამენტური უფლება. საქართველო, საკუთარ კონსტიტუციაში, ცალკე არ გამოყოფს დათქმას პერსონალური მონაცემის შესახებ, მაგრამ გათვალისწინებულია „ყოველი ადამიანის პირადი ცხოვრების ხელშეუხებლობის უფლება“[89], ეს ძალიან წააგავს აშშ-ს კონსტიტუციის პირველ შესწორებაში არსებულ უფლებას და თეორიულად, შეგვიძლია მივიჩნიოთ, რომ აქ შედის პირად მონაცემთა კონფიდენციალურობაც.

აუცილებელია, რომ შეიქმნას დაცვის ადექვატური მეთოდები კომპანიებისთვის. ეს საჭიროა, რომ დაიხვეწოს კომპანიებისა და საჯარო იურიდიული პირების ქცევის წესები და მათ მიიღონ კონკრეტული სახელმძღვანელო. ასევე, სასიხარულოა, რომ არსებობს პერსონალურ მონაცემთა დაცვის ინსპექტორი და მისი აპარატი, როგორც მაკონტროლებელი ორგანო.

[88] იქვე, მუხლი 15.
[89] საქართველოს კონსტიტუციის მე-15 მუხლი.

ამასთანავე, საქართველო არის ევროსაბჭოს წევრი. 1981 წელს ევროსაბჭომ მიიღო კონვენცია“ ინდივიდების დაცვა პერსონალური მონაცემების ავტომატური დამუშავებისგან“. 1999 წლიდან, როდესაც სახელმწიფო გახდა ევროსაბჭოს წევრი, მისთვის სავალდებულო გახდა, რომ კონვენციით დადგენილი ვალდებულებები დაეცვა და შეესრულებინა. 2018 წელს, 7 წლიანი მუშაობის შემდეგ, ევროსაბჭომ მიიღო კონვენციის განახლებული ვერსია, რომელიც შეიცავს თანამედროვე ინფორმაციულ ტექნოლოგიებთან დაკავშირებულ პრობლემებს. საქართველოში მიღებული კანონი პერსონალურ მონაცემთა დაცვის შესახებ პასუხობს როგორც 1981 წლის კონვენციას, ასევე 1995 წლის დირექტივას. მაგრამ, კანონი არ შეესაბამება GDPR-ისა და ევროსაბჭოს განახლებული კონვენციით გათვალისწინებულ სტანდარტებს. მნიშვნელოვანია, ევროსაბჭოს უახლესი მიდგომების ასახვა საქართველოს კანონმდებლობაში. ასევე, განსაკუთრებული ყურადღებაა გასამახვილებელი GDPR-ის მაღალ სტანდარტებზე. მით უფრო, რომ საქართველოს მიზანია ევროკავშირის კანონმდებლობასთან საქართველოს კანონმდებლობის მიახლოება და მომავალში აღნიშნულ ორგანიზაციაში წევრობა.

მნიშვნელოვანია იმის გააზრება, რომ საქართველო არ არის მსხვილი მოთამაშე მსოფლიო ეკონომიკაში, თუ სახელმწიფო შეეცდება, რომ შეზღუდოს უცხოური დიდი კომპანიები და აუკრძალოს მათ გარკვეული ქმედებები, შეიქმნება საშიშროება, რომ სრულებით გავიდნენ კომპანიები ბაზრიდან. საბჭოთა კავშირის დაშლის შემდეგ, მიუხედავად სხვადასხვა ტიპის გამოწვევისა, დამოუკიდებელმა საქართველომ შეძლო პროდასავლური პოლიტიკის განხორციელება. მნიშვნელოვანმა მუშაობამ და მჭიდრო თანამშრომლობამ საბოლოო შედეგი გამოიღო 2014 წლის 27 ივნისს, როდესაც, ერთის მხრივ, საქართველოსა და, მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის ხელი მოეწერა

ასოცირების შესახებ შეთანხმებას.[90] საქართველოს საგარეო პოლიტიკის პრიორიტეტია ქვეყნის ევროკავშირში წევრობა. შესაბამისად, საქართველო წლებია ცდილობს თავისი კანონმდებლობა მიუახლოვოს ევროკავშირის კანონმდებლობას. მაგალითად, 2011 წლის პერსონალურ მონაცემთა დაცვის შესახებ კანონი იყო მცდელობა 1995 წლის დირექტივის სტანდარტებთან შესაბამისობის.

საქართველოს კანონი პერსონალურ მონაცემთა შესახებ ზედმეტად ვიწროა და წააგავს მხოლოდ კონკრეტულ სექტორზე გათვლილ რეგულაციას. კანონის დახვეწის ერთადერთი რეალური გზა არის ევროკავშირის სტანდარტებთან მიახლოება, რაც საქართველოს მისცემს შესაძლებლობას სათანადოდ დაიცვას საკუთარი მოქალაქეების პირადი მონაცემები უცხო კომპანიების ქმედებებისგან.

[90] 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.

6. დასკვნა

საქართველოს კანონმდებლობა პერსონალურ მონაცემთა დაცვის შესახებ დახვეწას საჭიროებს, განსაკუთრებით ინტერნეტის მეშვეობით მოპოვებული ინფორმაციის თვალსაზრისით. მაგრამ აშშ-სა და ევროკავშირის მაგალითების მიმოხილვით ნათლად გამოჩნდა, რომ არც სხვა ქვეყნები არ არიან ბოლომდე ჩამოყალიბებულნი. ევროკავშირმა მხოლოდ შარშან აამოქმედა თანამედროვე საინფორმაციო ტექნოლოგიებზე მორგებული რეგულაციები და ჯერ კიდევ რთულია იმაზე საუბარი, თუ რა შედეგს მოიტანს ის. ჯერ მხოლოდ ერთი დიდი საქმე განიხილა საფრანგეთმა GDPR-ის ფარგლებში და შესაბამისად დააჯარიმა გუგლი. კომპანიებს უჭირთ საკუთარი დამკვიდრებული პრაქტიკის შეცვლა პერსონალურ მონაცემთა შეგროვებასთან დაკავშირებით, მაგრამ გუგლისთვის 50 000 000 ევროს დაკისრება იმდენად ხმამაღალი განცხადებაა, რომ რთული არ არის სამომავლო შედეგების გარკვეულწილად განჭვრეტა. ამ ყველაფრის მისაღწევად ევროკავშირს დასჭირდა 20 წელზე მეტი. 1995 წლის დირექტივა რამდენიმე წელიწადში სრულებით გამოუსადეგარი გახდა. შესაბამისად, რთულია იმის თქმა, რა ბედი ეწევა GDPR-ს და შეძლებს, თუ არა ის დროის ინოვაციებს გაუძლოს. ჯერ-ჯერობით კი ნათელია, რომ კომპანიები ძალიან უკმაყოფილოები არიან ახალი რეგულაციით, ეს კი შეგვიძლია მივიჩნიოთ, როგორც პოზიტიური შედეგი. ევროკავშირი ცდილობს, რომ თავი გაართვას 2000 წელს აღებულ ვალდებულებას და დაიცვას პერსონალური მონაცემების კონფიდენციალურობა, როგორც ადამიანის ფუნდამენტური უფლება.

მეორეს მხრივ, აშშ-მ ძალიან განსხვავებული მიდგომა აირჩია და სხვანაირად შეხედა პერსონალურ მონაცემთა რეგულირების სფეროს. ბოლო წლებმა ნათლად აჩვენეს, რომ რეგულაციების სექტორული დაყოფა იმდენად ბევრ და დიდ ხარვეზებს ქმნის, რომ განვითარებული, გიგანტური ტექნოლოგიური კომპანიები საერთოდ არ ექცეოდნენ აშშ-ს რეგულაციის ფარგლებში, ანუ კომპანიასა და აშშ-ს მოქალაქის პერსონალურ მონაცემთა დიდი რაოდენობით შენახვა-შეგროვებას შორის, მხოლოდ

საკუთარი თავის შეზღუდვა იდგა. ამის თავიდან აცილების მცდელობა იყო 2000 წლის "უსაფრთხო ნავსაყუდელის" პრინციპები, რომლებიც იმდენად წარუმატებელი გამოდგა, რომ ევროკავშირის მართლმსაჯულების სასამართლომ პირველივე საქმეზე ძალადაკარგულად ცნო ის. აშშ-ს დასაწყისი ძალიან ტურბულენტური იყო, მაგრამ ბოლო წლების მანძილზე მანაც გადადგა მნიშვნელოვანი ნაბიჯები. 2016 წელს მიღებული US –EU Privacy Shield ითვლება, რომ არის საკმაოდ მრავლის მომცველი და სათანადო დოკუმენტი, მცირედი პრობლემებით. ამასთან ერთად, კალიფორნიამ შეიმუშავა კონფიდენციალურობის კანონი, რომელიც ამოქმედდება 2020 წელს და შტატის სტატუსის გამო, დიდი ალბათობით ყველა კომპანიასა და სხვა ტერიტორიებსაც მოუწევთ მისი გათვალისწინება.

პერსონალურ მონაცემთა დაცვის მექანიზმების შემუშავება სახელმწიფოს მხრიდან არ ნიშნავს, რომ ეს სახელმწიფო ავიწროებს კომპანიას და ცდილობს, რომ დაახშოს მათი ინოვაციები ან სიტყვის თავისუფლება. კონფიდენციალურობის უფლება არის ყველა ადამიანისთვის ისევე მნიშვნელოვანი, როგორც სიცოცხლის უფლება და როგორც ადამიანები უნდა იაზრებდნენ, თუ რას აძლევენ კომპანიებს, ასევე კომპანიებიც უნდა იყვნენ იმაში შეზღუდულები, თუ რას იღებენ ადამიანებისგან.

საინფორმაციო ტექნოლოგიების სწრაფი განვითარების ფონზე მონაცემთა დაცვის მიზნით ევროკავშირმა შეძლო უახლესი საერთაშორისო სტანდარტების შემუშავება. ამდენად, მნიშვნელოვანია, მომავალში პერსონალური მონაცემების შესახებ საქართველოს კანონმდებლობის დახვეწა ევროკავშირის მიერ შემუშავებული სტანდარტების გათვალისწინებით. მით უფრო, როდესაც ქვეყნის მიზანია ევროკავშირში წევრობა.

ბიბლიოგრაფია

გამოყენებული სტატიები

- Katrin N.M., The Right to Privacy as a Human Right and Everyday Technologies, Legal Aspects of Privacy Law and Data Protection
- Weiss M.A., Archick K., U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, 2016
- Tassanakunlapan T., Verdugo M.A., Protection of Personal Data in Cyberspace: The EU-US E-Market Regime, ASEAN Journal of Legal Studies, Vol. 1, 2018
- Long W. RM., Scali G., Blythe F., European Union Overview, The Privacy, Data Protection and Cybersecurity Law Review - Edition 5, III, 2017
- Raul A. C., Faircloth E. F., Moham K V., United States, The Privacy, Data Protection and Cybersecurity Law Review - Edition 5, III, 2017
- IT Governance Privacy Team, Common Data Security Failures, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, 2017
- Vrbljanac D., Personal Data Transfer to Third Countries – Disrupting the Even flow?, Athens Journal Law – Volume 4, Issue 4, 2018
- Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, Washington, DC, May 2014, 18
- Solove D.J., Hartzog W., The FTC and the new common law of privacy, Columbia Law Review Vol. 114, 2014, 587
- Hetcher ȣ, The De Facto Federal Privacy Commission, The John Marshall journal of information technology & privacy law vol. 19, 2000
- Walker R., The Right to be Forgotten, Hashtings Law Journal, Vol 64, 2012
- Turow J., Hoofnagle C., Mulligan D., Good N., Grossklags J., The Federal Trade Commission and consumer privacy in the coming decade, I/S: A Journal of Law and Policy for the Information Society, Vol.3:3, 2008
- Bartley P. The California Consumer Privacy Act: not just 'America's GDPR', 451 Research, 2019

- IT Governance Privacy Team, Managing Personal Data Internationally, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide – Second edition, დიდი ბრიტანეთი, 2017
- Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 2016
- Fioretti J., U.S. reluctant to change data pact after EU watchdogs' concerns, Reuters, 2016
- არჩუაძე თ., პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016

ანალიზები და პრეზენტაციები:

- Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2016 Main Report, 2016
- SeeUnity, The main differences between the DPD and the GDPR and how to address those moving forward, 3, 2016.
- An introduction to Data Protection, Edited by EDRi and Digital Courage, Germany, 2012
- Dode A., the challenges of implementing General Data Protection Law (GDPR), 14th International Conference in "Standardization, Porotypes and Quality: A Means of Balkan Countries' Collaboration, Albania, 2018
- ეკონომიკური ანალიზის ბიურო, მთლიანი შიდა პროდუქტი შტატების მიხედვით: 2018 წლის მეორე კვარტალი. [14.11.2018]

ელექტრონული:

- National Institute of Standards and Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), იხ. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>
- M. Guiness, France Maintains Long Tradition of Data Protection, იხ <https://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711>
- Special Eurobarometer 431, Data Protection Report, 03.2015; იხ. <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf> [05.2015]

- Google Transparency Report, Search removals under European privacy law; იხ.: <https://transparencyreport.google.com/eu-privacy/overview> [03.2015]
- Data Protection Laws of the World, United States <https://www.dlapiperdataprotection.com/index.html?t=law&c=US> [28.01.2019]
- O'Connor N., Reforming the U.S. Approach to data protection and privacy, <https://www.cfr.org/report/reforming-us-approach-data-protection> [30.01.2018]
- Saad L., Americans Decry Power of Lobbyists, Corporations, Banks, Feds, Gallup. < https://news.gallup.com/poll/147026/Americans-Decry-Power-Lobbyists-Corporations-Banks-Feds.aspx> [11.04.2011]

გამოყენებული საქმეები

- საქმე C-131/12 Google Spain vs AEPD and Mario Costeja Gonsalez [2014]
- ადამიანის უფლებათა ევროპული სასამართლოს 2018 წლის 28 ივნისის განჩინება საქმეზე, Wolfgang Werle and Manfred Lauber v. Wikipedia
- Deliberation of the Restricted Committee SAN-2019-001, pronouncing a financial sanction against GOOGLE LLC, 28, 2019
- Olmstead v. United States, მოსამართლე ბატლერის განსხვავებული აზრი, 277 U.S. 438 (1928)
- Katz v. United States, მოსამართლე ჰარლანის თანმხვედრი აზრი, 389 U.S 347 (1967)
- საქმე C-312/14, Maximillian Schrems v Data Protection Commissioner [2015]

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)
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

- 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)
- ქარტია ევროპის კავშირის ფუნდამენტური უფლებების შესახებ, (მიღებულია 2000 წლის 2 ოქტომბერს, ძალაში შევიდა 2000 წლის 7 დეკემბერს)
- საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, ინდივიდების დაცვა პერსონალურ მონაცემთა დამუშავებასა და ამ მონაცემების თავისუფლად მიმოსვლასთან დაკავშირებით [1995]
- California Security Breach Information Act (SB-1386) (ძალაში შევიდა 2003 წლის 1 ივლისს)
- საბჭოს 2000 წლის 26 ივლისის გადაწყვეტილება 2000/520/EC, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2002], O.J. L215/7
- ამერიკის შეერთებული შტატების კონსტიტუცია, პირველი შესწორება (ძალაში შევიდა 1791 წლის 15 დეკემბერს)
- California Consumer Privacy Act (SB-1121) (ძალაში შევიდა 2018 წლის 28 ივნისს)
- კომისიის გადაწყვეტილება 2016/1250, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016]
- 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
- საქართველოს კონსტიტუცია