სახელმწიფო ინსპექტორის სამსახური
State Inspector's Service

საქართველოს ეროვნული უნივერსიტეტი სეუ
Georgian National University SEU

პერსონალურ მონაცემთა დაცვის აქტუალური პრობლემები და გამოწვევები

სტუდენტურ მოხსენებათა კრებული

თბილისი 2021 Tbilisi

სარედაქციო კომიტეტი

თავმჯდომარეები:

ანა ფირცხალაშვილი - სამართლის დოქტორი, პროფესორი, საქართველოს ეროვნული უნივერსისტეტის სეუს ვიცერექტორი სამეცნიერო კვლევითი მიმართულებით

ლონდა თოლორაია - სახელმწიფო ინსპექტორი

სოფიო ჯიაძე - სახელმწიფო ინსპექტორის მოადგილე

სოფიო ჭარელი - სახელმწიფო ინსპექტორის სამსახურის ადმინისტრაციული დეპარტამენტის უფროსი

ნინო ცხადაძე - სახელმწიფო ინსპექტორის სამსახურის საზოგადოებასთან ურთიერთობის დეპარტამენტის უფროსი

სოფიო შამუგია - სახელმწიფო ინსპექტორის სამსახურის საჯარო სექტორზე ზედამხედველობის დეპარტამენტის უფროსის მოადგილე

ლელა გვიშიანი - სახელმწიფო ინსპექტორის სამსახურის საჯარო სექტორზე ზედამხედველობის დეპარტამენტის იურისტი

თეა ჯუღელი - საქართველოს ეროვნული უნივერსიტეტის სეუ იურიდიული ფაკულტეტის დეკანი

ტექნიკური რედაქტორები:
ანა ცეცხლაძე

ნათია გუგუნაშვილი

Editorial Board

Editor-in-Chief:

Anna Phirtskhalashvili – Doctor, Professor, Vice Rector for Research of Georgian National Univerisity SEU

Londa Toloraia – State Inspector

Sophio Jiadze – Deputy State inspector

Sophio Chareli – Head of Administrative Department of State Inspector's Service

Nino Tskhadadze – Head of Public Relations Department of State Inspector's Service

Sophio Shamugia – Deputy Head of Public Sector Oversight Department of State Inspector's Service

Lela Gvishiani – Lawyer of Public Sector Oversight Department of State Inspector's Service

Tea Jugeli – Dean of Law faculty of Georgian National Univerisity SEU

Technical Editors:

Ana Tsetskhladze

Natia Gugunashvili

საქართველოს ეროვნული უნივერსიტეტი სეუ
Georgian National University SEU

სახელმწიფო ინსპექტორის სამსახური

State Inspector's Service

სარედაქციო კომიტეტის აზრი შეიძლება არ ემთხვეოდეს ავტორისას. სტატიაში მოყვანილი ფაქტებისა და მონაცემების სიზუსტეზე პასუხისმგებელია ავტორი
Editor's position may not coincide with that of authors. Authors are responsible for the facts and data in the article.

წინასიტყვაობა

პერსონალურ მონაცემთა დაცვის საკითხით დაინტერესებული სტუდენტებისთვის, სახელმწიფო ინსპექტორის სამსახურისა და საქართველოს ეროვნული უნივერსიტეტის სეუ მიერ გამოცხადდა ესეების კონკურსი და ჩატარდა ონლაინ კონფერენცია.

ღონისძიების მიზანი იყო, პერსონალური მონაცემების დაცვის თემაზე საზოგადოების ცნობიერების ამაღლება და სტუდენტების განვითარების ხელშეწყობა. პროექტი ადამიანის უფლებათა დაცვის საუნივერსიტეტო კვირეულის ფარგლებში განხორციელდა.

პირველ ეტაპზე კონკურსანტების შეფასება მოხდა შერჩეულ თემაზე მომზადებული აბსტრაქტების მიხედვით. შესაბამისი აბსტრაქტის წარმოდგენის შემდეგ, საკონფერენციო თემების შერჩევა მოხდა თემატიკის რელევანტურობიდან, შინაარსის მნიშვნელობიდან და აქტუალობიდან გამომდინარე.

ესეების შეფასებისა და კონფერენციაზე მათი წარმოდგენის ძირითადი კრიტერიუმები იყო:

- კონკურსის თემასთან/მიზანთან შესაბამისობა;
- მსჯელობა, არგუმენტაცია;
- ესეს სტრუქტურა;
- ინოვაციურობა/შემოქმედებითი მიდგომა;
- ნაშრომის ორიგინალურობა;
- ენობრივი ნორმების და აკადემიური სტანდარტების დაცვა.

ნაშრომები შეაფასეს სახელმწიფო ინსპექტორის სამსახურისა და საქართველოს ეროვნული უნივერსიტეტის წარმომადგენლების მხრიდან დაკომპლექტებულმა ორმხრივმა კომისიამ.

კონკურსის შედეგების შესაბამისად შეირჩა 12 საუკეთესო ესე, რომელთა ავტორების მონაწილეობითაც ჩატარდა ონლაინ კონფერენცია.

პერსონალურ მონაცემთა დაცვის საერთაშორისო დღეს, 28 იანვარს გამოვლინდა 4 საუკეთესო ესეს ავტორი, რომლებიც სახელმწიფო ინსპექტორის სამსახურში 2 თვიან სტაჟირებას გადიან.

აღნიშნული კრებული განკუთვნილია პერსონალური მონაცემების დაცვის საკითხებით დაინტერესებული პირებისათვის.

სარედაქციო კოლეგია

სარჩევი

ნატა სუხაშვილი
დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა 5

თამარ ვარდიაშვილი
COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალური მონაცემების დაცვა 13

მარიამ ჭიკაძე
COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვა 31

თამარ ფაჩულია
არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები 45

ანა ნიჟარაძე
COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალურ მონაცემების დაცვა 59

მარიამ გიორგაძე
COVID-19-ის გავლენა მონაცემთა უსაფრთხოებაზე 70

ელენე სულაბერიძე
COVID- 19 ის გავლენა მონაცემთა უსაფრთხოებაზე 83

ლიკა აბესაძე
დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა 93

მზექალა რომანაძე
COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვა 105

ოთარ მურმანიშვილი
დისტანციური სწავლების დროს სტუდენტების პერსონალური მონაცემების დაცვა 121

სალომე ზეინკლიშვილი
COVID-19-ის პანდემიის პირობებში ონლაინ მომსახურებისას პერსონალური მონაცემების დაცვა 131

ნანა მახარაძე
არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები. 142

დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა

ნატა სუხაშვილი,
საქართველოს ეროვნული უნივერსიტეტი სეუ

აბსტრაქტი

დღევანდელი მოცემულობით, მთელი მსოფლიო მოიცვა ყველასთვის საერთო მტერმა COVID 19-მა. მისმა გლობალურმა ხასიათმა კაცობრიობას მრავალი პრობლემა შეუქმნა და თითქმის ყველა საქმიანობაზე უარყოფითი გავლენა მოახდინა, რაც გამოიხატა იმაში, რომ მისი გავრცელების თავიდან ასაცილებლად ადამიანებს შეეზღუდად არაერთი კონსტიტუციური უფლება, ესენია: გადაადგილების, საკუთრების, შეკრების და სხვა. ყოველივე ამას, მოჰყვა სახელმწიფოების ეკონომიკური ინდექსის ვარდნა, საზოგადოების სოციალური დოვლათის შემცირება, ჯანდაცვის სისტემის გადატვირთულობა და კიდევ მრავალი პრობლემა. მოცემულ ესეში ვისაუბრებ იმაზე, თუ რა საფრთხეს შეიცავს დისტანციური სწავლება სკოლის მოსწავლეებისათვის, ვინაიდან ვიცით, რომ COVID 19-ის ინტესიურობამ, ასევე საფრთხის ქვეშ დააყენა ადამიანების განათლების მიღების შესაძლებლობა, რაც შემდგომში გახდა მიზეზი საგანმანათლებლო სისტემაში ძირეული რეფორმების განხორციელებისა. აღნიშნული რეფორმის შინაარსი გამოიხატა დისტანციური სწავლების დანერგვაში, რომელიც განკუთვნილი იყო ყველა საგანმანათლებლო დაწესებულებებისათვის.

შეიძლება ითქვას, რომ მსგავსი პრევენციული ღონისძიებაც ერთგვარი რისკების შემცველია განსაკუთრებით იმ საზოგადოების ნაწილისთვის, რომლებიც არიან სკოლის მოსწავლეები და მათი ასკიდან გამომდინარე შეიძლება ისე ვერ დაიცვან საკუთარი პერსონალური მონაცემები, როგორც სრულწლოვანმა და ქმედუნარიანმა პირმა. პერსონალურ მონაცემთა დაუცველობა შესაძლოა გამოიწვიოს შემდეგი პრობლემები:

- ბავშვთა გამოსახულების ნებისიერი სახით გავრცელება;
- კიბერბულინგი
- ბავშვთა ღირსების შემლახველი საქმიანობის განხორციელება;

ზემოთხსენებული პრობელემების აღსაკვეთად საჭიროა:

- მშობლების სათანადო ინფორმირება;
- კანონმდებლისგან ქმედითი მექანიზმების შექმნა;

ჩემი თემის მთავარი მიზანია, ყველა ასპექტში გათვალისწინებული და დაცული იყოს ბავშვის საუკეთესო ინტერესი, რომელიც მას მისცემს ჯანსაღ გარემოში ადაფტაციის შესაძლებლობას. გარდა ამისა, გავზარდით ინფორმაციის მიღების შესაძლებლობას მშობლებისათვის, რომელთა მოვალეობაც სწორედ, რომ მათი შვილების ინტერესების დაცვა და მენტალური განვითარების უზრუნველყოფაა. აუცილებელია, ყველა საჭირო ქმედითი მექანიზმების გამოყენება და მათი სათანადო აღსრულება სახელმწიფოს მხრიდან, რომ თითოეულ ბავშს ჰქონდეს გარანტია დაცული იყოს მისი შეხედულებები, ოჯახური გარემო, მათი კეთილდღეობა და სხვა დანარჩენი ფასეულობები, რომელიც შემდგომში შეუქმნის მათ ყველა პირობას მომავალში ცხოვრებისეულ სარბიელზე სრულფასოვნად დაიმკვიდრონ თავი.

საკვანძო სიტყვები: კონსტიტუციური უფლება; დისტანციური სწავლება; პერსონალური მონაცემები; ბავშვის საუკეთესო ინტერესი.

Abstract

As of today, COVID 19, a common enemy, has engulfed the entire world. Its global nature has created many problems for mankind and has negatively affected almost all activities, which has manifested itself in the fact that to prevent its spread, people are restricted by a number of constitutional rights, namely: movement, property, assembly and others. All this was followed by the fall of the economic index of the states, the reduction of the social wealth of the society, the overload of the healthcare system and many more problems. In this essay, I will talk about the dangers of distance learning for schoolchildren, as we know that the intensity of COVID 19 has also jeopardized the ability of people to get an education, which has subsequently led to fundamental reforms in the education system. The content of this reform was reflected in the introduction of distance learning, which was intended for all educational institutions.

It can be said that such a preventive measure also carries a kind of risk, especially for the part of the society that is a schoolboy and due to their asceticism may not be able to protect their personal data as an adult and able-bodied person. Insecurity of personal data may cause the following problems:
• Disseminate images of children in any form;
• Cyberbullying
• Carrying out activities that violate the dignity of children;
To prevent the above-mentioned problems, it is necessary to:
• Proper information of parents;
• Creating effective mechanisms from the legislator;
The main goal of my topic is to take into account and protect the best interests of the child in all aspects, to enable they to adapt to a healthy environment. In addition, we have increased access to information for parents whose duty it is precisely to protect the interests of their children and ensure their mental development. It is necessary to use all necessary effective mechanisms and their proper execution by the state, so that each child has a guarantee that his / her views, family environment, their well-being and other values will be protected, which will create all the conditions for them to fully establish themselves in the future.

Key words: Constitutional law; Distance learning; personal information; The best interests of the child

შესავალი

პანდემიის მაშტაბურობამ, რომელიც Covid-19-ის სახით მოგვევლინა, მნიშვნელოვანი გავლენა მოახდინა მსოფლიოს ცხოვრების წესის შეცვლაზე. მისმა მაშტაბურობამ თითოეულ სახელმწიფოს აიძლა განეხორციელებინა ადამიანის ყველა იმ უფლებების შეზღუდვა, რომელიც მისი გავრცლების ხელშემწყობ ფაქტორს წარმოადგენდა. საქართველოში მსგავსი შეზღუდვები გამოიხატა საქართველოს პრეზიდენტის დეკრეტის[1] მიღებაში, სადაც გაიწერა ყველა ის ქმედითი მექანიზმები, რომელიც უზრუნველყოფდა ეპიდოლოგიური სტიუაციის

[1]საქართველოს მთელს ტერიტორიაზე საგანგებო მდგომარეობის გამოცხადებასთან დაკავშირებით გასატარებელ ღონისძიენათა შესახებ პრეზიდენტის დეკრეტი (2020 წლის, 21 მარტი) https://matsne.gov.ge/ka/document/view/4830372?publication=0 [უ.გ 19.02.2021].

კონტროლს და რეგულრებას. არსებულ ეპიდ სიტუაციას უყურადღებოდ განათლების სისტემაც არ დარჩენია და შეიძლება ითქვას, რომ სრულიად ახალი სისტემის დანერგვის აუცილებლობას საჭიროებდა დისტანციური სწავლების კუთხით, ვინაიდან საგანმანათლებლო დაწესებულებებში სასწავლო პროცესის ჩვეულ რეჟიმში გაგრძელება საფრთხის ქვეშ აყენებდა საზოგადოების სიცოცხლესა და ჯანმრთელობას. სწორედ ამიტომ, საქართველოს განათლების, მეცნიერების, კულტურისა და სპროტის მინისტრის ბრძანებით[2] განისაზღვრა დისტანციური სწავლების პროცესის წარმართვის აუცილებლობა. შეიძლება ითქვას, რომ საგანმანათლებლო სფეროში განხორციელებული პრევენციული ღონისძიებები ეფექტურია Covid-19-ის გავრცელების მიზნით, მაგრამ წარმოიშობა ახალი პრობლემა არასრულწლოვნებში პერსონალური მონაცემების დაცვასთან დაკავშირებით. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ მე-2 მუხლის „ვ“ ქვე პუნქტი[3] გვაწვდის ინფორმაციას, რომ ნებისმიერი ფიზიკური პირი არის მონაცემთა სუბიექტი და რა თქმა უნდა, მასში ბავშვებიც უნდა მოვიაზროთ, რომლებიც განეკუთვნებიან მოწყვლად კატეგორიას. დისტანციური სწავლების დროს მეტად საჭიროებს დაცვას მათი პერსონალური მონაცემები, რადგან ალბათობა იმისა, რომ არასწრულწლოვნის პერსონალური მონაცემებზე წვდომა, მანიპულაცია და გამოყენება მეტად მარტივია, ვიდრე ეს სრულწლოვანი პირის შემთხვევაშია.

1. არასწრულწლოვანთა დამოკიდებულება ტექნოლოგიურ საგნებზე.

გასაკვირი არ იქნება, თუ აღვნიშნავთ, რომ 21-ე საუკუნეში კიბერ სივრცის კონტროლი რთულია და ბევრ განვითარებულ სახელმწიფოშიც არ არის ჩამოყალიბებული მისი თავიდან აცილების საშუალებები, მაგრამ ეს არ ნიშნავს იმას, რომ მის შესამცირებლად მაქსიმალური დაცვითი ღონისძიებები არ უნდა გავატაროთ. ყოველივე ამას ისიც ემატება, რომ ამ ბოლო ერთი წლის განმავლობაში ეპიდმოცულობის გამო მეტად გაიზარდა ტექნოლოგიური საკომუნიკაციო საშუალებების გამოყენების აუცილებლობა, რომელის მეშვებითაც ხორციელდება არა მხოლოდ განათლების მიღება, არამედ მრავალი პროფესიული საქმიანობაც. მინდა აღვნიშნო, რომ ამ კუთხით მეტად ყურადსაღებოა არასწრულწლოვანთა დამოკიდებულება საკომუნიკაციო საშუალებებთან, ვინაიდან უმეტეს შემთხვევაში მათ ბოლომდე არ აქვთ გააზრებული საკუთარი შეხედულებები მათი ასაკიდან გამომდინარე, რაც იმას ნიშნავს, რომ შესაძლოა ისინი გახდნენ მსხვეპლნი და მოექცნენ ამ კიბერ სივრცის კონტროლის ქვეშ, რომელიც პირდაპირ ლახავს ადამიანის კონსტიტუციურ უფლებას, კერძოდ კი, პირადი ცხოვრების ხელშეუხლებლობის უფლებას, რომელიც გამტკიცებულია საქართველოს კონსტიტუციის მე-15 მუხლში[4]. არასრულწოვანებიდან გამომდინარე, მათ არ შეუძლიათ საკუთარი უფლებები დაიცვან თავად და სწორედ ეს ამარტივეს მათზე რამე სახის მანიპულაციის განხორციელებას, რომელიც შეიძლება გამოიხატოს მოტყუებაში, არასწორი ინფორმაციის მიწოდებაში, პრობლემის გააზრებაში და სხვა. სწორედ ამიტომ, ბავშვების უფლებების დაცვა, რომელშიც მოიაზრება პერსონალურ მონაცემთა დაცვაც, უნდა

---

[2] საქართველოს ზოგადსაგანმანათლებლო დაწესებულებებში სასწავლო პროცესის დისტანციურად წარმართვისა და მიღებული შედეგების შეფასების წესისა და პირობების დამტკიცების შესახებ მინისტრის ბრძანება, 2020 წლის 9 სექტემბერი
https://matsne.gov.ge/ka/document/view/4988167?publication=0 [უ.გ 3.02.2021].

[3] მუხლი2, ქვეპუნქტი “ვ“ საქართველოს კანონი „ პერსონალურ მონაცემთა დაცვის შესახებ“
https://www.matsne.gov.ge/ka/document/view/1561437?publication=22 [უ.გ 19.02.2021].

[4] მუხლი 15, საქართველოს კონსტიტუცია, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები, საკანონმდებლო მაცნე, 1995 წლის 24 აგვისტო
https://matsne.gov.ge/ka/document/view/30346?publication=36 [უ.გ 19.02.2021].

წარმოადგენდეს მშობლის, სახელმწიფოს და იმ სასკოლო დაწესებულებების მთავარ ამოცანას, რომელთა თითოეული ქმედებაც უნდა გამომდინარეობდეს ბავშვის საუკეთესო ინტერესიდან. ბავშვის საუკეთესო ინტერესში ვგულისხმობთ ყველაფერს იმას, რომელიც მას უქმნის ყველა იმ პირობას, რომელიც აუცილებელია მისი განვითარებისათვის და რა თქმა უნდა, ამას საერთაშორისო „ კონვენცია ბავშვის უფლებების შესახებ“[5] ნათლად განამტკიცებს. იმ შემთხვევაში, თუ არ იქნება შემუშავებული პრევენციული ბერკეტები, სახეზე გვექნება შემდეგი შედეგები, ესენია:

- ბავშვთა გამოსახულების ნებისიერი სახით გავრცელება;
- ბავშვთა ღირსების შემლახველი საქმიანობის განხორციელება;
- კიბერბულინგი

შევეცდები, წარმოვადგინო ჩემი მოსაზრებები ამ საკითხის პრობლემურობასთან დაკავშირებით და გამოვკვეთო ის აუცილებელი დამხმარე საშუალებები, რომელიც დაგვეხმარება მაქსიმალურად დავიცვათ სკოლის მოსაწვლეთა პერსონალური მონაცემები.

1.1 ბავშვთა გამოსახულების ნებისმიერი სახით გავრცელება

როგორც მოგვეხსენება, დინსტანციური სწავლება არის სრულიად ახალი სისტემა, რომლის გამართული სისტემის ჩამოყალიბებაც ბევრ განვითარებულ ქვეყანაშიც პრობლემური იყო, ვინაიდან არსებობს მარავალი ხელშემშლელი ფაქტორი მის ათვისებაში და გამოყენებაში. არაერთი მოსაზრება არსებობს იმასთან დაკავშირებით, რომ ახალი თაობა მეტად კარგად ფლობს ტექონოლოგიებს, თუმცა მას თან სდევს მრავალი რისკი იმისა, რომ იგი მოექცეს მისთვის არასახარბიელო მდგომარეობაში. ამ კუთხით კარგი იქნება, თუ განვიხილავთ ბავშვთა გამოსახულების ნებისმიერი სახით გავრცელებას, მაგალითად როგორიცაა: ფოტო და ვიდეო გადაღებები საგაკვეთილო პროცესში, სადაც გამოჩნდება მისი ფიზიკური მახასიათებლები, მანერები, ჟესტიკულაციები, ოჯახში არსებული ფაქტები და მდგომარეობა და ყველაფერი ის, რომელიც შესაძლოა ციფრული ტექნოლოგიების საშუალებით იქნას გადაღებული და გავრცელებული იმ მიზეზით, რომ შემდგომ იქნას საზოგადოების გარკვეულ ნაწილში განხილვის საგანი ზემოთ ხსენებული ნიშნებით. მსგავსი ფაქტების გავრცელება შესაძლებელია სხვადასხვა სოციალურ ქსელში, დახურულ ჯგუფებში, თუ ღია ჯგუფებში სადაც კი შესაძლებელია რაიმე სახით აღნიშნული ფაქტების საჯაროდ გამოტანა.

1.2 ბავშვთა ღირსების შემლახველი საქმიანობის განხორციელება

ზემოთ აღნიშნული მოქმედება, რომელიც გამოიხატება ბავშვთა გამოსახულების ნებისმიერი სახით გავრცელებაში, ზრდის ალბათობას იმისას, რომ შესაძლოა ბავშვის მსგავსი გავრცელებული მასალები გამოყენებულ იქნას მისი ღირსების შემლახველი საქმიანობისათვის. ეს შეიძლება იყოს რაიმე სახის „საქველმოქმედო“ მიზნებისთვის, სადაც გავრცელებული ბავშვის ფოტო იქნება გამოყენებული, ასევე რაიმე სახის რეკლამა, რომელიც ეწინააღმდეგება ბავშვთა უფლებებეს კერძოდ კი პორნოგრაფიული ნიშნების შემცველი სახის გამოსახულებებს, რომელთა ამ სახით წარმოდგენა შესაძლებელია სხვადასხვა პროგრამების მეშვეობით. ამასთან დაკავშირებით არსებობს ერთი საერთაშორისო პრაქტიკა

[5] კონვენცია ბავშვთა უფლებების შესახებ https://matsne.gov.ge/ka/document/view/1399901?publication=0 მიღებულია 20/11/1989, [უ.გ 19.02.2021].

Regina v Jayson[6] (2002), სადაც რეკლამირებული იყო ბავშვთა ფოტოების გავრცელება ფსევდო სახით, რომელიც პირდაპირ უგულებელყოფდა ადამიანის ღირსებას და ბრიტანეთის სახელმწიფომშესაბამისი ღონისძიებებიც გაატარა.

1.3 კიბერბულინგი

არ იქნება გასაკვირი, თუ ხაზს გასმისთ აღვნიშნავ ზოგადად ბულინგის აქტუალურობას, რომელიც ბოლო წლებში მეტად ინტესიური გახდა. განსაკუთრებით პრობლემური არის სკოლებში, თუმცა დღევანდელი მდგომარეობით გამდოინაცვლა კიბერ სივრცეში. თავდაპირველად, როდესაც საუბარი დავიწყე სკოლის მოსწავლის გამოსახულების გავრცელებაზე, ეს პირდაპირ მასტიმულირებელია ბულინგის არსებობისათვის. დღეს, როდესაც სრულიად უცხო ფაქტების წინაშე ვდგავართ, რაც გულისხმობს იმას, რომ არავინ იყო მომზადებული მსგავსი ყოველდღიური შეზღუდვებისათვის, მათ შორის დისტანციური სწავლების მეთოდების გამოყენბისთვისაც. ეს განსაკუთრებით კვალს ტოვებს ჩვენს არასრულწლოვან მეგობრებზე, რადგან მათ შესაძლოა არ ჰქონდეთ საკუთარი სასწავლო სივრცე გამოყოფილი სახლში, არ ჰქონდეს ისეთი გარემო, როემლიც სხვა ბავშვს აქვს, ადგილი ჰქონდეს ოჯახის წევრების რეპლიკებს ან სხვა რაიმე ფაქტებს, რომელიც ბავშვს დისკომფორტს შეუქმნის და ამის გამო იგი ფსიქოლოგიური წნეხის ქვეშ აღმოჩნდეს და გახდეს ბილინგის მსხვერპლი. სწორედ ამიტომ, აუცილებელია სახელმწიფოს, მშობლების და სკოლის ადმინისტრაციის ერთობლივი მოქმედება, რათა თავიდან იქნას აცილებული მსგავსი ქმედება.

2. მშობლების სათანადო ინფორმირება

იმის გათვალისწინებით, რომ ჩვენ ვსაუბრობთ სკოლის მოსწავლეებზე, მათი ასაკიდან გამომდინარე რთულია თავად დაიცვან საკუთარი პერსონალური მონაცემები და თავი აარიდონ მათთვის არასასურველ მდგომარეობას. ამ შემთხვევაში, უდიდესი როლი აქვს ყველა იმ პირის თუ ორგანოს ჩართულობას, რომელსაც რაიმე სახის პასუხისმგებლობა გააჩნია ბავშვის განვითარებაში. სახელმწიფოს მხრიდან უნდა შემუშავდეს სათანადო პლატფორმა, სადაც მშობლებს სპეციალური ინფორმაციები მიწეოდებათ გარკვეული პერიოდულობით იმასთან დაკავშირებით, თუ რა არის საჭირო მათი შვილებისთვის, რომ დაცული იყოს ბავშვი რაიმე სახის ზემოქმედებისაგან. ამასთანავე, კარგი იქნება, თუ მსგავსი მეთოდით ჩაერთვება ფსიქოლოგის ინტიტუცით, რომლითაც მშობლები ინფრომირებულები იქნებიან თუ როგორ მიაწოდონ თავიანთ შვილებს სწორი ინფრმაცია ამ საკითხთან დაკავშირებით ვფიქორბ, მეტად ეფექტური იქნება.

3. კანონმდებლისგან ქმედითი მექანიზმების შექმნა

იმისათვის, რომ გვქონდეს მყისიერი რეაგირება სკოლის მოსწავლეთა პერსონალურ მონაცემთა დაცვასთან დაკავშირებით, აუცილებელია სპეციალური კანონმდებლობის შექმნა, რომელიც ერთ-ერთი უმთავრესი გასაღებია სათანადო ზომების მისაღებად. დღევანდელმა რეალობამ უფრო მეტად დაგვანახა, რომ კიბერ სივრცე გახდა უფრო მეტად საჭირო და განუყოფელი განათლებისათვის და შესაბამისად მეტად საყურადღებოა სპეციალური კანონმდებლობის შექმნა და სათანადო ზომების მიღება. გარდა ამისა, ეს არის პირდაპირ დაკავშირებული სახელმიწფოს პოზიტიური ვალდებულებების შესრულებასთან, რომელიც

[6] სასამართლო პრააქტიკა „რეჯინა ჯეისონის“ წინააღმდეგ Case: Regina v Jayson https://swarb.co.uk/regina-v-smith-regina-v-jayson-cacd-7-mar-2002/ [უ.გ 19.02.2021].

ავალდებულებს მას შექმნას ეფექტური და სათანადო მექანიზმები, რომელიც საშუალებას მისცემს შესაძლებლობას სკოლის მოსწავლეებს ყოველგვარი დაბრკოლებების გარეშე მიიღონ განათლება და ამასთან ერთად დაიცვან საკუთარი პირადი სივრცე.

დასკვნა

ჩემი მთავარი ამოცანაა, რომ გავაანალიზოთ აღნიშნული პრობლემა, რომელიც საყურადღებოა და საკმაოდ დიდ საფრთხეს უქმნის ბავშვების განათლების სრულფასოვნებას, თვითშეფასებას და განვითარებას. უნდა მოვახდინოთ სწრაფი და ეფექტური რეაგირება, რომელიც უნდა გამოიხატებოდეს სპეციალური პროგრამების და პლატფორმების შექმნაში, რომელიც თავის მხრივ როგორც სკოლის ადმინისტრაციას, ასევე სკოლის მოსწავლეებს და მშობლებს გაუმარტივებს აღნიშნული საშულებებით მიღებული ინფორმაციით ბავშვთა პირადი სივრცის და პერსონალურ მონაცემთა დაცვის შესახებ. გარდა ამისა, ეს უნდა იყოსმუდმივი, რათა მეტად ეფექტური იყოს სასწავლო პროცესი. მიმაჩნია, აქ დიდ როლს თამაშობს კანონდებლისაგან სპეციალური რეგულირების შექმნა არასრულწლოვანთა დინსტანციური სწავლების კუთხით, ასევე ვფიქრობ, იმისათვის, რომ მეტად ეფექტური იყოს სკოოლის მოსწავლეთა უფლებების დაცვა, აუცილებელია კომპლექსური და კომბინირებული მუშაობა, კერძოდ კი მშობლის, სკოლის ადმინისტრაციის და სახელმწიფოს ერთობლივი ნაბიჯები მოგვცემს აღნიშნული პრობლემის მაქსიმალურ შემცირებას და რაც მთავარია, თავად სკოლის მოსწავლეთა მაქსიმალურ ჩართულობას საგანმანათლებლო პროცესში, ვინაიდან განათლების მიღების შესაძლებლობა ეს არის ერთ-ერთი ფუნდამენტური ღირებულება ყველა ადამიანისათვის, რომელიც განმტკიცებულია საქართველო სკონსტიტუციის 27-ე მუხლში[7]. სწორედ ამიტომ, აღნიშნული ღონისძიებების მთავარ ფასეულობას უნდა წარმოადგენდეს იმ გარემოს უზრუნველყოფა, სადაც მოსწავლეს თავისუფლად შეეძლება თავისი თავის რეალიზების შესაძლებლობა ყოველგვარი ხელმშეშლელი ფაქტორებისგან დამოუკიდებლად.

[7]მუხლი 27, საქართველოს კონტიტუცია, საკანონმდებლო მაცნე https://matsne.gov.ge/document/view/30346?publication=36 [უ.გ 19.02.2021].

ბიბლიოგრაფია

1. საქართველოს მთელს ტერიტორიაზე საგანგებო მდგომარეობის გამოცხადებასთან დაკავშირებით გასატარებელ ღონისძიებათა შესახებ პრეზიდენტის დეკრეტი 2020 წლის, 21 მარტი https://matsne.gov.ge/ka/document/view/4830372?publication=0 [უკანასკნელად გადამოწმდა 19.02.2021];
2. საქართველოს ზოგადსაგანმანათლებლო დაწესებულებებში სასწავლო პროცესის დისტანციურად წარმართვისა და მიღებული შედეგების შეფასების წესისა და პირობების დამტკიცების შესახებ მინისტრის ბრძანება, 2020 წლის 9 სექტემბერი, https://matsne.gov.ge/ka/document/view/4988167?publication=0[უკანასკნელად გადამოწმდა 19.02.2021];
3. მუხლი 2 ქვეპუნქტი „ვ'' საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ" გამოქვეყნდა:27/03/2017https://www.matsne.gov.ge/ka/document/view/1561437?publication=22 [უკანასკნელად გადამოწმდა19.02.2021];
4. მუხლი 15 საქართველოს კონსტიტუცია, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები, საკანონმდებლო მაცნე, 1995 წლის 24 აგვისტო, https://matsne.gov.ge/ka/document/view/30346?publication=36 [უკანასკნელად გადამოწმდა 19.02.2021];
5. სასამართლო პრაქტიცა „რეჯინა ჟეისონის" წინააღმდეგ Case: Regina v Jayson https://www.lawteacher.net/free-law-essays/criminal-law/indecent-images-law-uk.php [უკანასკნელად გადამოწმდა19.02.2021] ;
6. კონვენცია ბავშვთა უფლებების შესახებ, მიღებულია 20/11/1989, https://matsne.gov.ge/ka/document/view/1399901?publication=0 [უკანასკნელად გადამოწმდა 19.02.2021];
7. მუხლი 27, საქართველოს კონტიტუცია, საკანონმდებლო მაცნე 1994 წლის 24 აგვისტო https://matsne.gov.ge/document/view/30346?publication=36 [უკანასკნელად გადამოწმდა 19.02.2021].

Bibliography

1. Decree of the President on the measures to be taken in connection with the declaration of a state of emergency throughout the territory of Georgia 2020, March 21 https://matsne.gov.ge/ka/document/view/4830372?publication=0 [Last seen19.02.2021];
2. Order of the Minister on the approval of the rules and conditions for the remote management of the educational process in the general education institutions of Georgia and the evaluation of the obtained results, September 9, 2020; https://matsne.gov.ge/ka/document/view/4988167?publication=0 [Last seen19.02.2021];
3. Article 2, sub-paragraph "ვ", Law of Georgia on Personal Data Protection Published: 27/03/2017, https://www.matsne.gov.ge/ka/document/view/1561437?publication=22 [Last seen19.02.2021];
4. Legislative Herald, Article 15 of the Constitution of Georgia, rights to privacy and family life, personal space and inviolability of communication, August 24, 1995, https://matsne.gov.ge/ka/document/view/30346?publication=36 [Last seen19.02.2021];
5. Judicial case against Regina Jason Case: Regina v Jayson https://www.lawteacher.net/free-law-essays/criminal-law/indecent-images-law-uk.php [Last seen19.02.2021];

6. Convention on the Rights of the Child, Retrieved 20/11/1989 https://matsne.gov.ge/ka/document/view/1399901?publication=0 [Last seen19.02.2021];
7. Article 27 of the Constitution of Georgia, Legislative Herald, August 24, 1994 https://matsne.gov.ge/document/view/30346?publication=36 [Last seen 19.02.2021].

COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალური მონაცემების დაცვა

თამარ ვარდიაშვილი,
თბილისის სახელმწიფო უნივერსიტეტი

აბსტრაქტი

პერსონალურ მონაცემთა დაცვა თანამედროვე სამართლებრივ სისტემაში სრულიად სამართლიანადაა მიჩნეული ერთ-ერთ ყველაზე აქტუალურ საკითხად. პერსონალურ მონაცემთა დაცვის ზოგადი სფეროდან კი, თავის მხრივ შესაძლებელია გამოვყოთ პირის ჯანმრთელობის შესახებ ინფორმაცია, რომელიც განსაკუთრებული კატეგორიის მონაცემად მიიჩნევა. როგორც საერთაშორისო, ისე ეროვნული კანონმდებლობის თანახმად, მასზე დაცვის უფრო მაღალი სტანდარტი მოქმედებს.

2020 წლის 11 მარტს, მსოფლიო ჯანდაცვის ორგანიზაციამ (WHO) ვირუსის გავრცელების მასშტაბებისა და სიმწვავის მიზეზით COVID-19 პანდემიად გამოაცხადა. მსოფლიო პანდემიის არსებობამ კი ჯანმრთელობის შესახებ ინფორმაციის დაცვის საკითხი მნიშვნელოვან გამოწვევად აქცია მთელი მსოფლიოსათვის.

კითხვის ნიშნებს არ ბადებს ის საკითხი,რომ სამედიცინო დაწესებულებისთვის მიმართვისას აუცილებელია პირს ჰქონდეს განცდა და ლეგიტიმური მოლოდინი მისი ინფორმაციის კონფიდენციალურობის დაცულობისა, თუმცა მნიშვნელოვანია იმის დადგენა კორონავირუსის პირობებში სახეზე ხომ არ არის პერსონალური მონაცემების დამუშავებასთან დაკავშირებული გამონაკლისები, როდესაც პირის ჯანმრთელობის მდგომარეობის გასაჯაროება დასაშვები ხდება სხვადასხვა გარემოებების - მათ შორის, საჯარო ინტერესისა და დაავადების პრევენციის მიზეზით.

ნაშრომის მიზანია, განიხილოს ჯანმრთელობის შესახებ ინფორმაციის დაცვის საერთაშორისო სამართლებრივი ფარგლები და საქართველოს კანონმდებლობის შესაბამისობა მასთან, დაადგინოს აღნიშნულ საკითხთან დაკავშირებით არსებული ძირითადი გამოწვევები და გამოკვეთოს მათი გადაჭრის ოპტიმალური გზები, გამოარკვიოს ვის აქვს უფლება მიიღოს ინფორმაცია ინფიცირებულთა შესახებ, შეიძლება თუ არა ამ ტიპის ინფორმაციის გასაჯაროება და რა თანმდევი შედეგები მოყვება მას თან. მნიშვნელოვანია, შესაბამისი საერთაშორისო და ადგილობრივი პრაქტიკის ანალიზის საფუძველზე, იმის გამორკვევა, იზღუდება თუ არა საგანგებო მდგომარეობის პირობებში პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის უფლება.

დღეისათვის,მსოფლიოში COVID-19 -ით ინფიცირების შემთხვევათა რიცხვი 109 მილიონს აჭარბებს. აღნიშნული ინფორმაცია კიდევ ერთხელ ჰფენს ნათელს ინფიცირებულთა ინფორმაციის დაცვის განსაკუთრებულ მნიშვნელობასა და აღნიშნული საკითხის საკვანძო თემათა შესახებ კერძო და საჯარო ინტერესთა შეპირისპირსების საფუძველზე დამყარებული სამართლებრივი ანალიზის საჭიროებას.

საკვანძო სიტყვები: COVID-19, პერსონალური მონაცემების დაცვა, ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემები, საერთაშორისო სამართალი, შიდასახელმწიფოებრივი სამართალი

Abstract

Protection of personal data is one of the most important current issues of contemporary jurisprudence. From the general field of data protection, health data is peculiarly interesting since it is considered sensitive data and is subject to particularly strict rules according to national as well as international legislations.

The World Health Organization (WHO) on March 11, 2020, declared COVID-19 a pandemic pointing to the alarming levels of spread and severity. The presence of a world pandemic challenged the protection of health data all over the world more than ever.

It is beyond a shadow of a doubt that when people go to any health facility they must have the legitimate, reasonable expectation that their privacy is granted, their health data is protected. However, it is important to ruminate whether there is an exception to the general rule of protecting health data in the times of Covid-19 due to the public interest and prevention of the infectious disease caused by a newly discovered coronavirus.

The main purpose of the article is to examine the protection of health data in International law and the compliance of Georgian laws to the international legal framework, to state the main challenges and their solving options, to ascertain who has access to information about covid-infected patients If it is legal to make such information public and judicial results of it.

It is essential, within the analyzing international and local case law, to ascertain if the Right to respect for private and family life (which includes the protection of personal data) can be derogated in case of declaration of the state of emergency throughout the whole territory of Georgia.

At the present time, the overall number of global coronavirus cases has surpassed the 109 million mark. It once again underlines the importance of protection of health data and the need for judicial analysis of contradiction between private and public interests in the face of the world pandemic.

Key words: COVID-19, personal data, health data, data protection, international law, municipal law

შესავალი

2019 წლის 31 დეკემბერს ჩინეთის რეგიონის, ვუჰანის მუნიციპალურმა ჯანმრთელობის კომისიამ სოციალურ ქსელში გაავრცელა ინფორმაცია პნევმონიის შემთხვევების ვირუსულ გავრცელებასთან დაკავშირებით. 2020 წლის 9 იანვარს კი მსოფლიო ჯანდაცვის ორგანიზაციამ (WHO) გააკეთა ოფიციალური განცხადება პნევმონიის გავრცელების მიზეზის შესახებ, დადგინდა რომ სახეზე იყო ახალი კორონავირუსი, რომელიც სწრაფი გავრცელების

სიხშირიდან გამომდინარე მალევე მსოფლიო პანდემიად გამოცხადდა და იქცა მსოფლიოს მთავარ, უპრეცედენტო გამოწვევად.[1]

მას შემდგომ რაც ვირუსი მსოფლიო მასშტაბით გავრცელდა, თუმცა თითოეულ ქვეყანაში ჯერ კიდევ ერთეულობით შემთხვევას ითვლიდნენ, შეშინებული მოქალაქეები ტელევიზიებს მოუწოდებდნენ გაევრცელებინათ ინფიცირებულთა მაიდენტიფიცირებელი ინფორმაცია, მათივე თქმით ვირუსის პრევენციის მიზნით, რათა იმ შემთხვევაში თუ ინფიცირებულები მათი მეზობლები აღმოჩნდებოდნენ ან სხვა გზით შემთხვევითი კონტაქტის შანსი იარსებებდა მეტი სიფრთხილე გამოეჩინათ.

აქედან გამომდინარე, ნათელი ხდება, რომ ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა დაცვის საკითხი განსაკუთრებულად დადგა დღის წესრიგში COVID-19-ის პირობებში.

დღეისათვის მსოფლიოს თითქმის ყველა ტელევიზია, მრავალი ვებ-გვერდი, სახელმწიფოთა მთავრობების ოფიციალური გვერდები... ყოველდღიურად აახლებენ და გვაწვდიან ინფორმაციას ინფიცირებულთა საერთო ოდენობის, ახალი შემთხვევების, კარანტინში თუ თვითიზოლაციაში მყოფი პირების რაოდენობასთან დაკავშირებით, თუმცა აღნიშნულნი, არასდროს შეიცავენ პირის მაიდენტიფიცირებელ ინფორმაციას, მაშინაც კი თუ მხოლოდ ერთეულ პირებზეა საუბარი. უმნიშვნელოვანესია იმის დადგენა რა გავლენა შეიძლება ჰქონდეს საჯარო ინტერესსა და პანდემიის პრევენციის მიზანს პერსონალური მონაცემების დამუშავების ზოგად სტანდარტებზე, შეიძლება თუ არა ჩამოყალიბდეს ან/და უკვე ხომ არ ჩამოყალიბდა განსხვავებული მიდგომა - გამონაკლისი COVID-19 -ის ვითარებასთან დაკავშირებით.

აღნიშნული სტატია, მიზნად ისახავს გამოარკვიოს ჯანმრთელობის შესახებ ინფორმაციის დაცვის საერთაშორისო სამართლებრივი ფარგლები და საქართველოს კანონმდებლობის შესაბამისობა მასთან, დაადგინოს ძირითადი გამოწვევები პერსონალურ მონაცემთა დაცვასთან დაკავშირებით, პანდემიის პირობებში.

დაადგინოს ვის აქვს უფლება მიიღოს ინფორმაცია ინფიცირებულთა შესახებ. მნიშვნელოვანია, შესაბამისი საერთაშორისო და ადგილობრივი პრაქტიკის ანალიზის საფუძველზე, იმის გამორკვევა, იზღუდება თუ არა საგანგებო მდგომარეობის პირობებში პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის უფლება.

1. პერსონალური მონაცემები ჯანმრთელობის შესახებ

პერსონალური მონაცემების დაცვა სრულიად სამართლიანად უნდა მივიჩნიოთ ადამიანის პირადი და ოჯახური ცხოვრების ხელშეუხებლობის უფლების შემადგენელ, განუყოფელ ნაწილად, რომელიც განმარტებული და დაცულია მრავალი სამართლებრივი დოკუმენტით, როგორც საერთაშორისო, ისე რეგიონალურ და ეროვნულ დონეზე

[1] Listings of WHO's response to COVID-19; WHO; 29 June 2020 https://www.who.int/news/item/29-06-2020-covidtimeline [უ. გ. 05.01.2021].

ჯანმრთელობის შესახებ პერსონალური მონაცემები მიემართება ყველა იმ პერსონალურ მონაცემს, რომელიც ეხება პირის ჯანმრთელობას. ევროპის საბჭოს მინისტრთა კომიტეტის 1997 წლის 13 თებერვლის რეკომენდაცია #R (97) 5 სამედიცინო მონაცემთა დაცვის შესახებ პირველ მუხლში[2] ხოლო აღნიშნული რეკომენდაციის განმაახლებელი 2019 წლის მინისტრთა კომიტეტის რეკომენდაცია ჯანმრთელობასთან დაკავშირებული მონაცემების დაცვის შესახებ[3] მე-3 მუხლში განმარტავს, რომ ჯანმრთელობასთან დაკავშირებული მონაცემები არის ფიზიკური პირის ფიზიკურ ან ფსიქიკურ ჯანმრთელობასთან, მათ შორის, სამედიცინო მომსახურების გაწევასთან დაკავშირებული მონაცემები, რომლითაც შესაძლებელია პირის ამჟამინდელ, წარსულში არსებულ ან სამომავლო ჯანმრთელობის მდგომარეობასთან დაკავშირებით ინფორმაციის მიღება. ამგვარ მონაცემს განეკუთვნება ასევე ინფორმაცია, რომ პირი არის ჯანმრთელი ან/და პირის მიერ სამედიცინო დაწესებულებისათვის მიმართვის შესახებ.

ჯანმრთელობის მდგომარეობის შესახებ არსებული პერსონალური ინფორმაცია თავისი ხასიათით სპეციფიკური და სენსიტიურია, ამიტომ ის ექცევა განსაკუთრებული დაცვის სფეროში, როგორც საერთაშორისო სამართლებრივ დოკუმენტებში, ისე ევროკავშირის სამართლის ფარგლებში და ჩვენთვის, როგორც ევროპის საბჭოს წევრი ქვეყნისთვის განსაკუთრებულად მნიშნელოვან ევროპის საბჭოს სამართლებრივ დოკუმენტებში. აღსანიშნავია, ნახსენები რეკომენდაციების, როგორც რბილი სამართლის როლი, მონაცემთა დაცვის საკითხში, რამდენადაც სწორედ მათზე დაყრდნობით, საქართველოში, ისევე როგორც ევროპის საბჭოს თითქმის ყველა წევრ სახელმწიფოში, ჩამოყალიბებულია ერთგვაროვანი, საკმაოდ ფრთხილი და პირადი ცხოვრების უფლების დაცვაზე მაქსიმალურად ორიენტირებული პოლიტიკა.

ადამიანის უფლებათა ევროპული სასამართლოს დამკვიდრებული პრაქტიკის მიხედვით პერსონალური მონაცემები ჯანმრთელობის მდგომარეობის შესახებ ექვემდებარება ბევრად უფრო მკაცრ ინფორმაციის დამუშავების სამართლებრივ რეჟიმს, ვიდრე სხვა ნებისმიერი სახის არასპეციალური/არასენსიტიური პერსონალური მონაცემი.[4]

კონვენცია პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, სხვაგვარად წოდებული, როგორც კონვენცია 108+, ასევე აქცევს მისი მე-6 მუხლის ფარგლებში ჯანმრთელობის შესახებ ინფორმაციას, მონაცემთა სპეციალურ კატეგორიაში.[5]

2. სამართლებრივი რეგულირების ჩარჩო და შესაბამისი პრაქტიკა

ჯანმრთელობასთან დაკავშირებული ყოველი პერსონალური მონაცემის დამუშავება უნდა შეესაბამებოდეს იმ ძირითადად დადგენილებებსა და პრინციპებს, რომელიც

[2] Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997). http://hrlibrary.umn.edu/instree/coerecr97-5.html [უ. გ. 05.01.2021].

[3] Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e [უ.გ.05.01.2021].

[4] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე Z v. Finland; no. 22009/93; 1997 წლის 25 თებერვალი; პარაგრაფები 94-112.

[5] მუხლი 6 კონვენცია 108+, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [უ.გ.05.01.2021].

წარმოდგენილია, როგორც ევროკავშირის შემთხვევაში ძირითად პერსონალურ მონაცემთა დაცვის რეგულაციებით (GDPR)[6], ევროპის საბჭოს შემთხვევაში კი კონვენცია 108+ -ით[7]. აღნიშნული სახის მონაცემების დამუშავებისას სახეზე აუცილებლად უნდა იყოს შესაბამისობა 7 ძირითად პრინციპთან - 1. კანონიერება, გამჭირვალობა და მიუკერძოებლობა 2. მიზნობრივი შეზღუდვა 3. მონაცემთა მინიმიზაცია 3. სიზუსტე 5. ზღვრული აკუმულირება 6. უსაფრთხოების გარანტია და 7. პასუხისმგებლიანობა.

რამდენადაც პერსონალურ მონაცემთა დაცვა, როგორც პირადი და ოჯახური ცხოვრების პატივისცემის უფლების შემადგენელი ნაწილი არ შედის აბსოლუტურ უფლებათა კატეგორიაში, ადამიანის უფლებათა ევროპული კონვენციის მიხედვით დასაშვებია მასში ჩარევა და მისგან გადახვევა, თუმცა ამისათვის ,,აუცილებელია, რომ ჩარევა ხორციელდებოდეს კანონის შესაბამისად და აუცილებელი იყოს დემოკრატიულ საზოგადოებაში ეროვნული უშიშროების, საზოგადოებრივი უსაფრთხოების ან ქვეყნის ეკონომიკური კეთილდღეობის ინტერესებისათვის, უწესრიგობის ან დანაშაულის თავიდან ასაცილებლად, ჯანმრთელობის ან მორალისა თუ სხვა უფლებათა და თავისუფლებათა დასაცავად. ‘’[8]

აღნიშნულ უფლებაში ჩასარევად საჭიროა არა მხოლოდ საჯარო ინტერესის, არამედ განსაკუთრებული საჯარო ინტერესის არსებობა. ამის მაგალითად შეგვიძლია მოვიყვანოთ ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა. საქმეში Avlikina and Others v. Russia[9] აპლიკანტებს წარმოადგენდნენ იეჰოვას მოწმეები, რომლებიც ამტკიცებდნენ რომ მათი სამედიცინო დოკუმენტების რუსეთის საგამომძიებო ორგანოებისათვის მიწოდება, რაც მოჰყვა აპლიკანტების მიერ სისხლის გადასხმაზე უარის თქმას, არღვევდა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლს. სასამართლომ, მართლაც დაადგინა, რომ სახეზე იყო მე-8 მუხლის დარღვევა, რამდენადაც აღნიშნული საქმის ფაქტობრივ გარემოებებში არ იკვეთებოდა დემოკრატიულ საზოგადოებაში ჩასარევად საჭირო სტანდარტი, განსაკუთრებული საჭიროება ჯანმრთელობის შესახებ პირადი მონაცემების გავრცელებისა. მოცემული პრეცედენტული გადაწყვეტილებით კიდევ ერთხელ დადასტურდა, რომ იმისათვის, რომ აღნიშნულ უფლებაში ჩარევა განხორციელდეს მართლზომიერად, აუცილებელია სახეზე იყოს განსაკუთრებული საჭიროება, რაც შეიძლება გამოიხატებოდეს განსაკუთრებულ საჯარო ინტერესსში.

Covid-19-ის პირობებში, მსოფლიოს მრავალ კუთხეში საჯარო ინტერესის საფუძვლით, არაერთხელ გასაჯაროვდა პერსონალური მონაცემები პირის ჯანმრთელობის შესახებ.

ინდოეთში, მთავრობის მიერ ინტერნეტში აიტვირთა PDF ფაილები, სადაც იყო კარანტინში გადაყვანილ პირთა სახელი, გვარი, მისამართი და მოგზაურობის ისტორია.[10]

---

[6] General Data Protection Regulation GDPR; 23.5.2018; https://gdpr-info.eu/ . [უ.გ.05.01.2021.

[7] Convention 108 +; Convention for the protection of individuals with regard to the processing of personal data.

[8]მუხლი 8(2),1950 წლის 4 ნოემბრის ადამიანის უფლებათა ევროპული კონვენცია.

[9]ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე ,,ავლიკინა და სხვები რუსეთის წინააღმდეგ’’; (Application no. 1585/09) 2013 წლის 7 ოქტომბერი; პარაგრაფები 60-63.

[10] Bangalore Mirror. Government publishes details of 19,240 home-quarantined people to keep a check, 2020. https://bangaloremirror.indiatimes.com/bangalore/others/government-publishes-details-of-19240-home-quarantined-people-to-keep-a-check/articleshow/74807807.cms [უ.გ.08.01.2021].

პერუს ჯანდაცვის ეროვნულ ინსტიტუტში, შექმნილი იყო პლატფორმა, რომელიც აწვდიდა ინფორმაციას იმ პირთა შესახებ, რომელთაც კორონავირუსის ტესტი ჰქონდათ გაკეთებული, პირველ ეტაპზე, საჭირო იყო პირადი მონაცემების შეყვანა, შემდგომ კი რამდენიმე დღე მონაცემები საჯაროდ იყო ხელმისაწვდომი.[11]

მონაცემების დაცვის მნიშნელობას ნათლად ცხადყოფს ასევე შემდეგი შემთხვევა - ა.შ.შ-ს მოქალაქე ფრენკ ქინგი სამოგზაუროდ იმყოფებოდა კამბოჯაში, როდესაც ის შეცდომით იქნა იდენტიფიცირებული, როგორც COVID-19-ის მატარებელი, მიუხედავად ტესტის შედეგის შესწორებისა, მას შემდეგ რაც ქინგი ა.შ.შ-ში დაბრუნდა ის რამდენიმე კვირის განმავლობაში იყო სასიკვდილო მუქარებისა და პირადი თავდასხმების ობიექტი, როგორც სოციალურ ქსელში, ისე პირადად. [12] აქედან გამომდინარე, აშკარაა, რომ პირის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გავრცელებამ არამარტო შეიძლება შელახოს პირადი ინტერესი მონაცემის კონფიდენციალურობის შესახებ, არამედ გამოიწვიოს დისკრიმინაციული დამოკიდებულებები, გახდეს სხვადასხვაგვარი ძალადობისა თუ სისხლისამართლებრივი დანაშაულის ჩადენის საფუძველი.

რაც შეეხება უშუალოდ საქართველოს, პირის ჯანმრთელობასთან დაკავშირებული ინფორმაციის დაცვის უფლება განსაზღვრულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, ,,პაციენტის უფლებების შესახებ'' საქართველოს კანონით და სხვა კანონქვემდებარე აქტებით, აღნიშნულ მონაცემებთან დაკავშირებით, თავის მხრივ მოქმედებს მკაცრი კონფიდენციალურობის პრინციპი.

რამდენადაც არსებობს ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაციის დაცვის გონივრული მოლოდინი, საქართველოს ყველა შესაბამისი საკანონმდებლო აქტი ევროპულ სტანდარტებზე დაყრდნობით, მათ არამართლზომიერ დამუშავებას უხეშ დარღვევად მიიჩნევს და საკმაოდ ფრთხილ პოლიტიკას ატარებს აღნიშნულ საკითხთან დაკავშირებით.

განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დაუშვებელია, თუმცა რა შემთხვევაში შეიძლება აღნიშნულ აკრძალვაში შეჭრა?

ჯანმრთელობის დაცვის სისტემის გამართული ფუნქციონირებისთვის მნიშვნელოვანია პაციენტის შესახებ ინფორმაციის გაზიარებაც. სწორედ ამიტომ, არსებობს სამართლებრივი გამონაკლისები,რადგან ისეთი განსაკუთრებული შემთხვევებისა და გარემოებების დროს, როგორიც მათ შორის,არის ამჟამად არსებული მსოფლიო პანდემია - COVID-19, სახელმწიფო არ აღმოჩნდეს საკანონმდებლო ჩიხში.

ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავება დასაშვებია, როდესაც :

1. სახეზეა მონაცემების სუბიექტის წერილობითი თანხმობა
2. მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არა აქვს, მონაცემთა დამუშავებაზე თანხმობა განაცხადოს;

[11] Perú. Instituto Nacional de Salud. https://ins.gob.pe/resultado_coronavirus/.[უ.გ.08.01.2021].
[12] The New York Times. What It's Like to Come Home to the Stigma of Coronavirus, 2020. https://www.nytimes.com/2020/03/04/us/stigma-coronavirus.html. [უ.გ.08.01.2021].

3. მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის. [13]

მონაცემთა მიმართ განხორციელებული ნებისმიერი სახის აქტივობისთვის აუცილებელია არსებობდეს ინდივიდუალური სამართლებრივი საფუძველი. მაგალითად, პაციენტის ჯანმრთელობასთან დაკავშირებული მონაცემების შეგროვების საფუძველი შეიძლება იყოს საზოგადოებრივი ჯანმრთელობის დაცვის მიზნით მონაცემთა დამუშავების აუცილებლობა, თუმცა, ამ ინფორმაციის მესამე პირებისთვის გადაცემის საფუძველი - მონაცემთა სუბიექტის წერილობითი თანხმობა.[14]

პანდემიის არსებობა, როგორც მოცემულობა, ეჭვგარეშეა რომ გვაძლევს იმის საფუძველს, სახელმწიფო წარმომადგენლებმა და ასევე დამსაქმებელმა(როდესაც საქმე ეხება უსაფრთხო სამუშაო გარემოს შენარჩუნებას) მოსთხოვონ პირს ისეთი სახის ინფორმაციის მიწოდება, რომელიც მიზეზ-შედეგობრივ კავშირშია პანდემიის პრევენციასთან, მათ შორის უკანასკნელი პერიოდის მოგზაურობის ისტორია, მუშაობის დაწყების წინ სხეულის ტემპერატურის გაზომვა და ა.შ[15] განვითარებული მსჯელობიდან ნათელი გახდა იმის გარდაუვალი საჭიროება, რომ პანდემიის პირობებში ინტენსიურად დამუშავდეს მონაცემები ჯანმრთელობის მდგომარეობის შესახებ. მათ შორის, განსაკუთრებულად გამოვყოფდი ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემის დამუშავებას იმ შემთხვევაში, როდესაც პირის სიცოცხლეს და ჯანმრთელობას საფრთხე ემუქრება, ე.ი თუკი აღმოჩნდება, რომ ვირუსით ინფიცირებულ პირთან ჰქონდა მეორე პირს კონტაქტი, თავისთავად მეორე პირის სიცოცხლისა და ჯანმრთელობისთვის შექმნილი საფრთხიდან გამომდინარე მას აქვს უფლება მიიღოს ინფორმაცია მოსალოდნელი საფრთხის შესახებ, რაც უკავშირდება პირის ჯანმრთელობის შესახებ პერსონალური მონაცემის დამუშავებას. თუმცა, ვფიქრობ, რომ რამდენადაც COVID-19-თან დაკავშირებით, ფაქტობრივად ხორციელდება ფორს-მაჟორული, საგამონაკლისო მიდგომა, ვირუსიის პრევენციისათვის, კვლევითი მიზნებისათვის აუცილებელია აღნიშნული თემატიკის მონაცემები მოექცეს, არა მხოლოდ სეპარირებულად, ინდივიდუალურ პირთა სამედიცინო ისტორიაში, არამედ ერთიან სივრცეში, რათა გამარტივდეს სტატისტიკაზე დაყრდნობით სიმპტომების, რისკ-ჯგუფებისა და სხვა სახის გადამწყვეტი ინფორმაციის დეტალური შესწავლა.

ჯანდაცვის სფეროში მომუშავე პირებს, სამედიცინო პერსონალს,იმ დაწესებულებებს, რომელთაც უშუალო პასუხისმგებლობა გააჩნიათ საზოგადოებრივი ჯანმრთელობისა და წესრიგის დაცვაზე, მათ შორის - ჯანდაცვის სამინისტროსა თუ სხვა სამედიცინო დაწესებულებეს, ასევე უშუალოდ COVID-19-ის პირობებში, საკარანტინო რეჟიმების აღსრულებაზე პასუხისმგებლობის მქონე პირებსა თუ დაწესებულებებს, თავის მხრივ მიუწვდებათ ხელი ჯანმრთელობასთან დაკავშირებულ მონაცემებზე. რაც მარტივად აიხსნება

[13] მუხლი 6 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.
[14] „რეკომენდაცია ჯანმრთელობის დაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ”.UNDP პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი გვ 17.
[15] Suder S. Processing employees' personal data during the Covid-19 pandemic. European Labour Law Journal. December 2020.

იმ ფაქტორით, რომ აღნიშნული, აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისა და ფუნქციონირებისთვის.

გარდა მოცემული შემთხვევებისა, ძირითადად ჯანმრთელობის მდგომარეობასთან დაკავშირებულ მონაცემებზე წვდომის მოპოვება შესაძლებელია, მხოლოდ მონაცემის სუბიექტის დამოუკიდებელი და ნათლად გამოხატული ნების მეშვეობით.

აქვე, შეგვიძლია განვიხილოთ, მედიაში, სამინისტროებისა თუ COVID-19-თან დაკავშირებულ ვებ-გვერდებზე გავრცელებული სტატისტიკური მონაცემები, ინფიცირების შემთხვევათა, კარანტინსა თუ თვითიზოლაციაში განთავსებულ პირთა შესახებ. ამ შემთხვევაში, რამდენადაც სახეზე არ გვაქვს პირთა მაიდენტიფიცირებელი მონაცემები და ის ორგანოები, რომელთაც აქვთ მონაცემთა დამუშავების ლეგიტიმური უფლებამოსილება, მხოლოდ კონკრეტულ რიცხვით მონაცემს ავრცელებენ, სახეზე არაა პერსონალურ მონაცემთა დაცვის საკითხი, რამდენადაც არ ვრცელდება მაიდენტიფიცირებელი ინფორმაცია და მედია იღებს და ავრცელებს მხოლოდ სტატისტიკურ მონაცემს, აღნიშნული ქმედება აბსოლუტურად მართლზომიერია.

პირის ინფიცირების შესახებ ინფორმაციის გავრცელება,კი თითქმის ვერცერთ შემთხვევაში ვერ შეესაბამება, როგორც ევროპული კანონმდებლობით დადგენილ სტანდარტს, ისე შესაბამის ეროვნულ კანონმდებლობას. ამ შემთხვევაში, ვფიქრობ საჯარო ინტერესი ვერანაირად ვერ გადაწონის პირის უფლებას ჯანმრთელობის მდგომარეობის დაცვის შესახებ, თუკი აღნიშნული ინფორმაციის დამუშავების აკრძალვით საფრთხე არ ექმნებათ სხვა პირებს, ისეთი სენსიტიური პერსონალური მონაცემის დამუშავების დაუშვებლობა, როგორიცაა ჯანმრთელობასთან დაკავშირებული ინფორმაცია, უნდა გავიგოთ როგორც იმპერატიული დანაწესი. მაღალი საჯარო ინტერესი არ შეიძლება გახდეს მონაცემთა დამუშავების ლეგიტიმური საფუძველი, მაგალითად თანამდებობის პირების ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია(არის თუ არა პირი კოვიდ-ინფიცირებული) აბსოლუტურად მიზანშეუწონელია, რომ დამუშავდეს ავტომატურად, სუბიექტის ნებართვის გარეშე, ვინაიდან არ არსებობს პროპორციულობა საჯარო ინტერესთან მიმართებაში, თავის მხრივ არ იკვეთება აუცილებლობაც. ასეთი სახის ინფორმაციის მიღება, ვფიქრობ, იმპერატიულად უნდა აღვიქვათ, რომ შეიძლება მხოლოდ იმ შემთხვევაში, თუ თანამდებობის პირები, სამოქალაქო პასუხისმგებლობის ფარგლებში, სურვილისამებრ გაავრცელებენ პერსონალურ მონაცემებს მათი ინფიცირების შესახებ.

3. „დიდი ძმის" სილუეტი მსოფლიო ჯანდაცვის კრიზისში

COVID-19 პანდემიის წინააღმდეგ საბრძოლველად და ზიანის მაქსიმალურად შესამცირებლად სახელმწიფოებმა ყველა შესაძლო გზას მიმართეს. სხვადასხვა მეთოდებს შორის, მსოფლიოს თითქმის ყველა ქვეყანაში განსაკუთრებული აქტუალობით სარგებლობდა მობილური აპლიკაციები, რომლებიც ფიზიკურ პირებს, ინდივიდუალურად ატყობინებდათ ჰქონდათ თუ არა კონტაქტი კოვიდ-ინფიცირებულთან.[16] აპლიკაციებმა მალევე მოიპოვეს პოპულარობა, თუმცა მრავალი იურისტის მიერ გაჟღერდა მოსაზრება, რომ აღნიშნული აპლიკაციები წინააღმდეგობაში მოდის სახელმწიფოთა კონსტიტუციებთან, რადგან მიზანშეუწონლად ამუშავებს პირად მონაცემებს, მათ შორის პირთა ჯანმრთელობის

[16]Apple and Google partner on COVID-19 contact tracing technology". https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing Apple. 2020-04-10. Retrieved [უ.გ.2020.04.10].

მდგომარეობის შესახებ.[17] აპლიკაციების გამოყენების მასშტაბიდან გამომდინარე აღნიშნული საკითხის გამორკვევა მეტად პრობლემური და ამასთანავე ძალიან მნიშვნელოვანია პერსონალურ მონაცემთა დაცვის კუთხით. საინტერესოა ირღვევა თუ არა ერთი შეხედვით სახელმწიფოს პრევენციული ღონისძიებით პირთა ფუნდამენტური უფლებები, რომლებიც დაცულია როგორც ადამიანის უფლებათა საყოველთაო დეკლარაციითა და სამოქალაქო და პოლიტიკურ უფლებათა შესახებ საერთაშორისო პაქტით, ასევე სახელმწიფოთა კონსტიტუციებით.

მრავალ სახელმწიფოში, მათ შორის საქართველოში, ამგვარი აპლიკაციის ჩამოტვირთვა და გამოყენება მოქალაქეთა სურვილზე იყო დამოკიდებული, ჯანდაცვის სამინისტრო კი აქტიურად უწევდა რეკომენდაციას აპლიკაციას და მის პოტენციურ სარგებელს. ზოგიერთ სახელმწიფოში, მათ შორის ჩინეთში, ირანსა და თურქეთში აპლიკაციის ჩამოტვირთვა სავალდებულო ხასიათს ატარებდა. [18]

აღნიშნული აპლიკაციის მეშვეობით, მრავალი ქვეყნის სამთავრობო დაწესებულებები ამუშავებდნენ პირის პერსონალურ მონაცემებს, რამდენადაც აპლიკაციის ჩამოტვირთვა რამდენიმე ქვეყანაში იყო სავალდებულო, ფიზიკურ პირებს მასში შეჰყავდათ პირადი მონაცემები, მათ შორის ინფორმაცია ინფიცირების შესახებ, ამის შემდგომ კი აპლიკაციით მიწვდილ მონაცემებზე დაყრდნობით(რომელიც ინიშნავს პირის გადაადგილების მარშრუტს) სამხრეთ კორეაში დაიწყო ისეთი მონაცემების გასაჯაროვება, როგორიც იყო კოვიდ-ინფიცირებულებისა და მათთან კონტაქტში მყოფი პირების გადაადგილების ისტორია, ასევე ისეთი ინფორმაცია, რა დროს დატოვეს ამ ადამიანებმა სამუშაო ადგილი, ეკეთათ თუ არა პირბადე საზოგადოებრივ ტრანსპორტში(რამდენადაც იდენტიფირება ხდებოდა გამოსახულებითაც), კლინიკები რომლებშიც ისინი იმყოფებოდნენ ტესტის გასაკეთებლად(რაც თავის მხრივ შედის ჯანმრთელობის შესახებ პირად მონაცემებში) და შემდგომ მიღებული ტესტის პასუხი. [19]

ასევე, ზოგიერთ შემთხვევაში, მაგალითად სინგაპურში გავრცელდა მონაცემები, რომელიც არ შეიცავდა უშუალოდ სახელს და გვარს, თუმცა რეალურად შეიცავდა იდენტიფიცირებისათვის საკმარის მონაცემებს, მაგალითად, იყო შემთხვევები, როდესაც გავრცელდა ინფორმაცია - ,,219-ე შემთხვევა დაუფიქსირდა 30 წლის მამაკაცს, რომელიც მუშაობდა სენგკანგის სახანძრო სადგურში, ამჟამად იმყოფება სენკანგის მთავარ ჰოსპიტალში, ის ასევე არის 236-ე ინფიცირებულის ოჯახის წევრი''[20] მიუხედავად იმისა, რომ არცერთ ამ ტიპის აპლიკაციაში უშუალოდ არ ზიარდება ფიზიკურ პირებს შორის იდენტიფიცირებადი ინფორმაცია ჯანმრთელობის მდგომარეობის შესახებ, აპლიკაციის მეშეობით მიღებული ინფორმაცია

[17] Cho, Hyunghoon, Daphne Ippolito, and Yun William Yu. "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs." arXiv preprint arXiv:2003.11511 (2020).

[18] https://theconversation.com/health-data-collected-during-the-coronavirus-pandemic-needs-to-be-managed-responsibly-141978 [უ. გ. 08.01.2021].

[19] The New York Times. What It's Like to Come Home to the Stigma of Coronavirus, 2020. https://www.nytimes.com/2020/03/04/us/stigma-coronavirus.html [უ. გ. 08.01.2021].

[20] Kuguyo, Oppah, Andre Pascal Kengne, and Collet Dandara. "Singapore COVID-19 pandemic response as a successful model framework for low-resource health care settings in Africa?" OMICS: A Journal of Integrative Biology 24.8 (2020): 470-478.

საავადმყოფოში ვიზიტისა თუ სხვა ფაქტების შესახებ, მრავალი სახლმწიფოს მიერ მაინც საჯაროვდებოდა.

აღსანიშნავია ის ფაქტორი, რომ რეალურად აპლიკაციის ჩამოტვირთვის მოხალისეობრივი ხასიათი მის მოქმედებას მნიშვნელოვნად ასუსტებს, ვინაიდან როგორც ოქსფორდის პერსონალურ მონაცემთა ინსტიტუტმა დაადასტურა, იმისათვის რომ აპლიკაციას ჰქონდეს ეფექტი საჭიროა რომ ის ჩამოტვირთული იყოს მოსახლეთა 80%-ის მიერ, სურვილისამებრი ჩამოტვირთვის პირობებში კი ამის მიღწევის ალბათობა მნიშვნელოვნად იკლებს.[21] მიუხედავად აპლიკაციების პოპულარობისა სინგაპურსა და ისლანდიაში აპლიკაციათა ჩამოტვირთვის ინტენსივობა, მხოლოდ 29%-ს სინგაპურში, 38%-ს კი ისლანდიაში წარმოადგენდა.[22] აღნიშნული გარემოებებიდან გამომდინარე ფაქტობრივად შეგვიძლია ვთქვათ, რომ სურვილისამებრი ჩამოტვირთვის შემთხვევაში აღნიშნული აპლიკაციები არაეფექტიანია. საინტერესოა რამდენად გადაწონის მსოფლიო ჯანდაცვის კრიზისი ისეთ ფუნდამენტურ უფლებებს, რაც აპლიკაციის სავალდებულო ჩამოტვირთვის შემთხვევაში ირღვევა. თუმცა, რამდენადაც აპლიკაციები გლობალურ გამოყენებას ექვემდებარება, თუნდაც სურვილისამებრი ჩამოტვირთვის შემთხვევაში ხაზგასასმელია რამდენად ხდება პირის ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვის უზრუნველყოფა. აპლიკაცია იდენტური დანიშნულებით შეიქმნა, ინდივიდუალურად თითოეული სახელმწიფოს მიერ, ამდენად სახელმწიფოთა პოლიტიკაც პერსონალურ მონაცემთა დაცვის კუთხით განსხვავდებულად ჩამოყალიბდა. მაშინ, როცა ჩინეთში არსებული აპლიკაცია მოითხოვს რეგისტრაციასა და პირადი მონაცემების შეყვანას[23] ფაქტობრივად სრულად ამუშავებს პერსონალურ მონაცემებს ჯანმრთელობის მდგომარეობის შესახებ, საქართველოში არსებული აპლიკაცია Stop Covid სრულებით არ მოითხოვს რეგისტრაციას და მის გამოსაყენებლად პერსონალური მონაცემების მითითება აბსოლუტურად არ არის საჭირო. საქართველოში აპლიკაციის ჩამოტვირთვა ნებაყოფლობითია. მომხმარებელი კი თავად წყვეტს რა ტიპის ინფორმაცია გააზიაროს, როდის მისცეს სისტემას წვდომა და როდის შეწყვიტოს ის. COVID 19-ის დადასტურების შემთხვევაში პირს შეუძლია, თავად გადაწყვიტოს გააზიარებს თუ არა ინფორმაციას ინფიცირების შესახებ, ასევე იმ ლოკაციების შესახებ, სადაც ბოლო პერიოდში იმყოფებოდა.

Stop Covid აპლიკაცია გადმოწერისას ანიჭებს პირს უნიკალურ ID-ს, რისი მეშვეობითაც სრულიად ანონიმურად განისაზღვრება სოციალური კონტაქტები აპლიკაციის მომხმარებლებს შორის. ინფიცირების შესახებ ინფორმაციის გაზიარებისას კი მის კონტაქტებს მისდით გაფრთხილება, რომ კონტაქტი ქონდათ ინფიცირებულ პირთან, თუმცა აღნიშნული პირის მონაცემები ცნობილი არ ხდება აპლიკაციის სხვა მომხმარებლებისთვის.[24]

[21] https://www.bdi.ox.ac.uk/news/controlling-coronavirus-transmission-using-a-mobile-app-to-trace-close-proximity-contacts [უ.გ. 05.01.2021].

[22] „Tracking Apps are Unlikely to Help Stop COVID-19" ACLU, 6 August 2020.

[23] Liang, Fan. "COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China." Social Media + Society, July 2020.

[24] https://www.moh.gov.ge/ka/news/5060/STOP-COVID-aplikacia---xSirad-dasmuli-kiTxvebi [უ.გ.05.01.2021].

ამ ყველაფრიდან გამომდინარე აშკარაა, რომ საქართველოში არსებული აპლიკაციის პირობებში ფაქტობრივად არ ხდება პერსონალურ მონაცემთა დაცვის სფეროში ჩარევა, რადგან არცერთი სახით არ საჯაროვდება პირთა ჯანმრთელობასთან დაკავშირებული მონაცემი, მაშინ როდესაც თუნდაც ჩინეთის მაგალითზე სახეზე გვაქვს მათი დამუშავება. ამ შემთხვევაში უნდა შევაპირისპიროთ, პერსონალურ მონაცემთა დაცვა და საჯარო ინტერესი. დღევანდელ რეალობაში, ყველაზე ოპტიმალურ ვარიანტად რჩება აპლიკაციის ნებაყოფლობითი ჩამოტვირთვა პირის ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემების დაცვის შენარჩუნებით, ვინაიდან, მიუხედავად პანდემიის, როგორც ფორს-მაჟორული გარემოების არსებობისა დაუშვებელია მოქალაქეთა პერსონალური მონაცემების დამუშავება მოხდეს არალეგიტიმურად, უფლებაში უხეში შეჭრით მაშინ როდესაც მრავალი ქვეყნის პრაქტიკით იკვეთება, რომ უფლებაში უხეში ჩარევის გარეშე შესაძლებელია ანალოგიური სისტემის ამუშავება. პირთა ჯანმრთელობის შესახებ პერსონალური მონაცემების დამუშავების შემთხვევაში თუკი ის გადაწონილი იქნებოდა საჯარო ინტერესით, აპლიკაცია მაინც ვერ შეძლებს მაქსიმალური ეფექტის გამოვლენას, რამდენადაც აუცილებელია ის ჩამოტვირთული ჰქონდეს მოსახლეობის ძირითად ნაწილს, ამ პირობის შესრულება კი საკმაოდ რთულია, იმის გათვალისწინებითაც, რომ რისკ ჯგუფში შემავალი ასაკოვანი ადამიანების მიერ აპლიკაციით სარგებლობის უზრუნველყოფაც ცალკეულ სირთულეს წარმოადგენს. ამიტომაც, ვფიქრობ, მიუხედავად მსოფლიო პანდემიისა, სახეზე არ გვაქვს საკმარისი საფუძველი პირთა უფლებებში იმ ხარისხით შეჭრისა რაც პანდემიის პრევენციის მიზნით, მათი ჯანმრთელობის შესახებ პერსონალურ მონაცემების დამუშავებას გულისხმობს სავალდებულოდ ჩამოსატვირთი აპლიკაციის მეშვეობით. რაც შეეხება, აპლიკაციის ისეთ ვერსიებს, რომლებიც ითვალისწინებენ, ნებაყოფლობით, რეგისტრაციის გარეშე მისით სარგებლობას, აღნიშნული ვერსიები თავის მხრივ, სრულიად მისასალმებელია და მიუხედავად სავარაუდო ნაკლები ეფექტისა, ისინი სრულად შეესაბამებიან საერთაშორისო სტანდარტებს.

4. ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დაცვა საგანგებო მდგომარეობის მოქმედების პირობებში

,,საგანგებო მდგომარეობა არის დროებითი ღონისძიება, რომელიც საქართველოს კანონმდებლობის შესაბამისად ცხადდება საქართველოს მოქალაქეთა უსაფრთხოების უზრუნველყოფის ინტერესებისათვის, მასობრივი არეულობის, ქვეყნის ტერიტორიული მთლიანობის ხელყოფის, … ბუნებრივი ან ტექნოგენური კატასტროფის ან ეპიდემიის დროს ან სხვა შემთხვევაში, როდესაც სახელმწიფო ხელისუფლების ორგანოები მოკლებული არიან კონსტიტუციურ უფლებამოსილებათა ნორმალური განხორციელების შესაძლებლობას.''[25] ვკითხულობთ საქართველოს კანონში ,,საგანგებო მდგომარეობის შესახებ''.

საგანგებო მდგომარეობის არსებობა მისი შინაარსობრივი გააზრებისთანავე ქმნის წარმოდგენას, დროებითი, განსაკუთრებული სამართლებრივი რეჟიმის დაწესების შესახებ, რაც ფაქტობრივად შეესაბამება კიდეც სიმართლეს. საგანგებო მდგომარეობის პირობებში სახელმწიფო იღებს უფლებამოსილებას შეზღუდოს კონსტიტუციით გარანტირებული

[25] მუხლი 1,საქართველოს კანონი ,,საგანგებო მდგომარეობის შესახებ'' 17/10/1997.

გარკვეული უფლებები, რომლებიც numerus clausus პრინციპით განისაზღვრება კონსტიტუციის დანაწესითვე[26]

Covid-19-ის საფუძელზე საქართველოში იყო გამოცხადებული საგანგებო მდგომარეობა განსაზღვრული დროით, ამიტომ შეგვძლია მიმოვიხილოთ ჯანმრთელობასთან დაკავშირებული პერსონალურ მონაცემთა მოწესრიგების საკითხი 2020 წლის 21 მარტის პრეზიდენტის დეკრეტის პირობებში და შესაბამისად მიმოვიხილოთ რა სახის მოწესრიგება შეიძლება იყოს განსაზღვრული პოტენციური საგანგებო მდგომარეობის გამოცხადების შემთხვევაში.

2020 წლის 23 მარტს საქართველომ ნოტით შეატყობინა ევროპის საბჭოს ადამიანის უფლებათა ევროპული კონვენციის მე-15 მუხლის ფარგლებში გადახვევების გაკეთების შესახებ. ნოტაში საუბარი იყო, როგორც უშუალოდ ევროკონვენციის დებულებებიდან გადახვევის, ისე შესაბამისი უფლებებისა და თავისუფლებების განმსაზღვრებლი ყველა საერთაშორისო დოკუმენტიდან გადახვევის გაკეთების შესახებ, რაც თავის მხრივ უკავშირდებოდა Covid-19-ის გავრცელების პრევენციას. ნოტას თან ერთვოდა საქართველოს პრეზიდენტის დეკრეტი ,,საქართველოს მთელ ტერიტორიაზე საგანგებო მდგომარეობის გამოცხადების შესახებ" , რომელშიც პირდაპირ არის ჩამოთვლილი ყველა ის კონსტიტუციური ნორმა ნორმელიც იზღუდებოდა საგანგებო მდგომარეობის გავრცელების პერიოდში, მათ შორის იყო საქართველოს კონსტიტუციის მე-15 მუხლი - პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები, რომელიც ცალსახად მოიცავს პერსონალური მონაცემების დაცვის უფლებას, მათ შორის ჯანმრთელობასთან დაკავშირებული მონაცემებისას. ამას გარდა, 2020 წლის 23 მარტის დადგენილებით მთავრობამ შეაჩერა საჯარო ინფორმაციისა და პერსონალური ინფორმაციის გაცემისთვის კანონმდებლობით დადგენილი ვადები.

აქედან გამომდინარე, ერთი შეხედვით, აღნიშნული უფლება პრორპოციულობისა და აუცილებლობის ფარგლებში საჭიროებისამებრ შესაძლებელი იყო შეზღუდულიყო, თუმცა დეკრეტი აუცილებელია აკონკრეტებდეს შეზღუდვის ფარგლებს, ნახსენებ შემთხვევაში კი მე-15 მუხლის ფარგლებს მოიცავდა მხოლოდ შემდეგი - ,,შეჩერდეს პენიტენციურ დაწესებულებებში პატიმრობის კოდექსით გათვალისწინებული პაემნის უფლების მოქმედება."[27] რაც ნიშნავს იმას, რომ მიუხედავად იმისა რომ სახელმწიფომ ზოგადი გადახვევა გააკეთა მე-15 მუხლისგან, უშუალოდ პერსონალური მონაცემების(მათ შორის ჯანმრთელობასთან დაკავშირებული) დაცვის საკითხი დარჩა აბსოლუტურად იმ სამართლებრივ რეჟიმში, როგორიც მოქმედებდა საგანგებო მდგომარეობამდე. მნიშვნელოვანია ხაზი გაესვას, რომ მიუხედავად აღნიშნულისა, ეს გარემოება არ ნიშნავს იმას, რომ იმ შემთხვევაში თუ ქვეყანაში კვლავ გამოცხადდება საგანგებო მდგომარეობა Covid-19-ის გავრცელების პრევენციის საფუძველზე არსებობს გარანტია, პერსონალური მონაცემების არ შეზღუდვისა. პროპორციულობის, აუცილებლობის, მიზანშეწონილობის კრიტერიუმების დაკმაყოფილების შემთხვევაში აღნიშნულ უფლებაში ჩარევა სრულიად ლეგიტიმურ ნაბიჯად უნდა იქნეს მიჩნეული. შესაბამისად, საგანგებო მდგომარეობის მოქმედებასთან

[26]მუხლი 71, ნაწილი 4, საქართველოს კონსტიტუცია; საგანგებო და საომარი მდგომარეობა.

[27]მუხლი 1 (3), საქართველოს პრეზიდენტის დეკრეტი №1; 2020 წლის 21 მარტი;ქ. თბილისი ,,საქართველოს მთელ ტერიტორიაზე საგანგებო მდგომარეობის გამოცხადებასთან დაკავშირებით გასატარებელ ღონისძიებათა შესახებ".

დაკავშირებით უნდა დავასკვნათ ის, რომ კონკრეტული პრეზიდენტის დეკრეტის გარეშე შეუძლებელია დავადგინოთ უფლების შეზღუდვის ფარგლები, ზემოთ ნახსენები დეკრეტის პირობებში კი საქართველოში, პერსონალური მონაცემების კონტექსტში საგანგებო მდგომარეობის პირობებში არ არსებულა არანაირი სპეციალური გადახვევა, ე.ი სრულად შენარჩუნდა მოქმედი სამართლებრივი ნორმების მოქმედება, თუმცაღა პერსონალური მონაცემების(მათ შორის ჯანმრთელობასთან დაკავშირებული) დაცვა, როგორც კონსტიტუციის მე-15 მუხლის(რომლით დაცული უფლებაც არაა აბსოლუტური) შემადგენელი, ნაგულისხმევი ნაწილი, აბსოლუტურად შესაძლებელია სამართლებრივად იქნას შეზღუდული პოტენციური საგანგებო მდგომარეობის შემთხვევაში, კანონის შესაბამისად, პრორპოციულობის, აუცილებლობის, დემოკრატიულ საზოგადოებაში ეროვნული უშიშროების, საზოგადოებრივი უსაფრთხოების, ჯანმრთელობის ან მორალისა თუ სხვათა უფლებათა და თავისუფლებათა დასაცავად.

დასკვნა

დასკვნის სახით, უნდა ითქვას, რომ Covid-19-ის, როგორც უპრეცედენტო გამოწვევის, პირობებში განსაკუთრებულად გამოიკვეთა პირის ჯანმრთელობის მდგომარეობის შესახებ მონაცემების, შესაბამისად განსაკუთრებული კატეგორიის მონაცემების დაცვის მნიშვნელობა. მსოფლიო ჯანდაცვის კრიზისის რეალობაში აშკარა გახდა მიმოხილული სახის პერსონალური მონაცემების დაცვასთან დაკავშირებული მთავარი საკვანძო საკითხები:

1. საჯაროდ გავრცელებულიყო ინფიცირებულთა ვინაობა საჯარო ინტერესიდან გამომდინარე

მოცემულ საკითხთან დაკავშირებით, ვფიქრობ აუცილებელია არსებობდეს ერთგვაროვანი მიდგომა, რაც გულისხმობს აღნიშნული მოწოდების სრულ უარყოფას. რამდენადაც ნაშრომში მიმოვიხილეთ პერსონალური მონაცემების დაცვის განუზომელი მნიშვნელობა და არსი, იმის გათვალისწინებით, რომ ინფიცირებულთა ვინაობის მასშტაბური გავრცელებით ირღვევა არსებული სტანდარტები, რადგანაც თუნდაც საჯარო ინტერესის გათვალისწინებით, პროპორციულობის კუთხით, ინფორმაციის გავრცელება ვერ იქნება ვირუსის პრევენციის პროპორციული საშუალება, სრულად შეილახება განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საკანონმდებლო ფარგლები. შედეგად,კი მსოფლიო, ჯანდაცვის კრიზისის პარალელურად აღმოჩნდება უფლებათა დაცვის კრიზისშიც.

2. ვის უნდა მიუწვდებოდეს ხელი კოვიდ-ინფიცირებულთა პერსონალურ მონაცემებზე

ისევე, როგორც საერთაშორისო სამართლებრივი დოკუმენტებით დადგენილი სტანდარტით, ასევე მათი წარმატებული იმპლემენტირების შედეგად, ეროვნული კანონმდებლობის შესაბამისად, აღნიშნულზე ხელი უნდა მიუწვდებოდეთ:

1. ჯანდაცვის სფეროს წარმომადგენლებს(როგორც სამედიცინო პერსონალს, ისე კარანტინის რეჟიმის აღსრულებაზე პასუხისმგებელ პირებს);
2. იმ პირებს, რომელთა სიცოცხლეს ან ჯანმრთელობას საფრთხე ექმნება აღნიშნული ინფორმაციის არ ცოდნით (მაგ. ინფიცირებულთან კონტაქტში მყოფ პირებს);
3. ნებისმიერ პირს, მონაცემის სუბიექტის ნამდვილი ნების გამოხატვის შედეგად

3. ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დაცვის საკითხი, ნოვაციის, კოვიდ-პრევენციული აპლიკაციების პირობებში

რამდენადაც, ნაშრომში განვიხილეთ აპლიკაციის დადებითი და უარყოფითი მხარეები, მათი შეპირისპირება ძირითადად დამოკიდებულია სხვადასხვა ქვეყნის მიერ შემუშავებულ პოლიტიკაზე. დასკვნის სახით, უნდა ითქვას, რომ იმ შემთხვევაში, თუ აპლიკაცია საჭიროებს რეგისტრაციას, ახდენს პირთა იდენტიფიცირებას მათი გადაადგილების მეთვალყურეობის პარალელურად, თუ ამუშავებს პერსონალურ მონაცემებს, ცხადია აღნიშნული პოლიტიკა არის სრულიად დისპროპორციული და შეუსაბამო, თუმცა აპლიკაციები, რომლებიც, ექვემდებარება სურვილისამებრ ჩამოტვირთვას და არა არანებაყოფლობით მონაცემთა დამუშავებას, წვდომა აქვს მხოლოდ Bluetooth სისტემაზე, არის აბსოლუტურად გამჭირვალე და ხაზგასმით ითხოვს მომხმარებლის თანხმობას თითოეული წვდომის ნებართვაზე, ფაქტობრივად არ ამუშავებს არცერთი სახის პერსონალურ მონაცემს ავტომატურად, ამ სახის აპლიკაციები სრულიად უსაფრთხო და გამოსაყენებლად მიზანშეწონილია, ხოლო საჯარო ინტერესთან შეპირისპირების პირობებში, მათი ჩამოტვირთვის იძულება(იმისათვის რომ იყოს მაქსიმალურად ეფექტიანი) ვფიქრობ სრულიად მიუღებელია და საკანონმდებლო მოწესრიგებასთან შეუსაბამოა.

4. მონაცემთა დაცვა საგანგებო მდგომარეობის გამოცხადების პირობებში

საგანგებო მდგომარეობის გამოცხადების პირობებში, რამდენადაც დასაშვებია საქართველოს კონსტიტუციის მე-15 მუხლიდან გადახვევა, დასაშვებია ცვლილება ჩვენს მიერ განხილული თემის კონტექსტშიც, თუმცა 2020 წელს პრეზიდენტის დეკრეტით გამოცხადებულ საგანგებო მდგომარეობის ტექსტში, მიუხედავად მე-15 მუხლიდან გადახვევისა, პერსონალურ მონაცემებთან დაკავშირებით არანაირი ცვლილება არ განხორციელებულა. ე.ი საგანგებო მდგომარეობის გამოცხადება ავტომატურად არცერთ შემთხვევაში არ უნდა დავუკავშიროთ უფლებათა გადახვევიდან, თუკი დეკრეტში უშუალოდ არაა მასზე მითითება გაკეთებული.

საბოლოოდ, ვფიქრობ ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დაცვა მაქსიმალურად უნდა შენარჩუნდეს Covid-19-ის პანდემიის პირობებშიც, მიუხედავად იმისა, რომ სრულიად გასათვალისწინებელია საზოგადოებრივი ჯანმრთელობა და ზოგადი საჯარო ინტერესი, აუცილებელია თითოეული ჩარევა პერსონალურ მონაცემთა დაცვაში იყოს

1. ადამიანის ძირითად უფლებათა და თავისუფლებათა დაცვისაკენ მიმართული
2. აუცილებელი დემოკრატიულ საზოგადოებაში
3. არადისკრიმინაციული
4. პროპორციული; აუცილებელია დაცული სიკეთე აღემატებოდეს შეზღუდვით მიყენებულ ზიანს
5. მონაცემები იყოს მინიმალიზებული
6. მონაცემზე ხელმისაწვდომობა იყოს ლიმიტიზირებული
7. მონაცემი იყოს შენახული და გამოყენებული მხოლოდ რაციონალური დროის განმავლობაში, შემდეგ კი წაიშალოს
8. პროცესი იყოს გამჭირვალე

მსოფლიო ჯანდაცვის კრიზისის პირობებში, საკითხი აღარ უნდა დაისვას იმგვარად, მთავრობებს შეუძლიათ თუ არა ჯანმრთელობასთან დაკავშირებული მონაცემების გამოყენება, არამედ უნდა ვკონცენტრირდეთ იმაზე, როგორ უნდა განხორციელდეს ეს

მაქსიმალურად პროპორციულად.სახელმწიფოებმა არ უნდა დააყენონ მოქალაქეები არჩევანის წინაშე - ჯანმრთელობასა და პერსონალური მონაცემების დაცვას შორის, პანდემიის წინააღმდეგ კოლექტიური ბრძოლისთვის, აუცილებელია მოქალაქეები ენდობოდნენ საკუთარ სახელმწიფოს და არ გრძნობდნენ თავს კონტროლის ან/და ზედამხედველობის ქვეშ, არ ფიქრობდნენ რომ Covid-19-ის მიზეზით, მათი პერსონალური მონაცემის დამუშავებაზე არსებობს შეუზღუდავი უფლებამოსილება.

ბიბლიოგრაფია

1. Universal Declaration of Human Rights;
2. International Covenant on Civil and Political Rights;
3. European Convention on Human Rights;
4. Convention 108;
5. Convention 108 +; Convention for the protection of individuals with regard to the processing of personal data;
6. Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997);
7. Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data;
8. General Data Protection Regulation GDPR; 23.5.2018;
9. Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015);
10. Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe;
11. საქართველოს კონსტიტუცია;
12. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ;
13. საქართველოს პრეზიდენტი დეკრეტი №1; 2020 წლის 21 მარტი; საქართველოს მთელ ტერიტორიაზე საგანგებო მდგომარეობის გამოცხადებასთან დაკავშირებით გასატარებელ ღონისძიებათა შესახებ;
14. საქართველოს კანონი ,,საგანგებო მდგომარეობის შესახებ’’;
15. საქართველოს კანონი ,,პაციენტის უფლებების შესახებ’’;
16. NOTE VERBALE Strasbourg, 23 March 2020 https://rm.coe.int/16809cff20 [უკანასკნელად გადამოწმდა 5. 01. 2021.];
17. https://www.coe.int/en/web/data-protection/covid-19-data-protection [უკანასკნელად გადამოწმდა 5. 01. 2021.];
18. https://www.coe.int/en/web/data-protection/contact-tracing-apps [უკანასკნელად გადამოწმდა 5. 01. 2021.];
19. ,,რეკომენდაცია ჯანმრთელობის დაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ’’; პერსონალურ მონაცემთა დაცვის ინსპექტორის სამსახური;
20. Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence; Council of Europe;
21. Joint Statement on Data Protection and Privacy in the COVID-19 Response; WHOhttps://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response [უკანასკნელად გადამოწმდა 5. 01. 2021];
22. F. Liang COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. Social Media + Society. July 2020;
23. Cho, Hyunghoon, Daphne Ippolito, and Yun William Yu. "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs." arXiv preprint arXiv:2003.11511 (2020);

24. M.Kędzior, The right to data protection and the COVID-19 pandemic: the European approach. ERA Forum 21, 533–543 (2021).

Bibliography

1. Universal Declaration of Human Rights;
2. International Covenant on Civil and Political Rights;
3. European Convention on Human Rights;
4. Convention 108;
5. Convention 108 +; Convention for the protection of individuals with regard to the processing of personal data;
6. Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997);
7. Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data;
8. General Data Protection Regulation GDPR; 23.5.2018;
9. Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015);
10. Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe;
11. Constitution of Georgia;
12. Law of Georgia on Personal Data Protection;
13. President of Georgia Edict No 2, 21 April 2020, Tbilisi, On the Declaration of the State of Emergency throughout the Whole Territory of Georgia;
14. Law of Georgia on the state of emergency;
15. Law of Georgia on patient rights;
16. NOTE VERBALE Strasbourg, 23 March 2020 https://rm.coe.int/16809cff20 [Last seen 5.01.2021];
17. https://www.coe.int/en/web/data-protection/covid-19-data-protection [Last seen 5.01.2021];
18. https://www.coe.int/en/web/data-protection/contact-tracing-apps. [Last seen 5.01.2021];
19. ,,recommendations on healthcare data protection''; Office of the Personal Data Protection Inspector. ;
20. Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence; Council of Europe.;
21. Joint Statement on Data Protection and Privacy in the COVID-19 Response; WHOhttps://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response.;
22. F. Liang COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. Social Media + Society. July 2020;

23. Cho, Hyunghoon, Daphne Ippolito, and Yun William Yu. "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs." arXiv preprint arXiv:2003.11511 (2020).;
24. M. Kędzior, The right to data protection and the COVID-19 pandemic: the European approach. ERA Forum 21, 533–543 (2021).

COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვა

მარიამ ჭიკაძე,
თბილისის სახელმწიფო უნივერსიტეტი

აბსტრაქტი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის[1] მე-2 მუხლის „ბ“ ქვეპუნქტის მიხედვით, პირის ჯანმრთელობასთან დაკავშირებული ინფორმაცია განსაკუთრებული კატეგორიის პერსონალურ მონაცემს წარმოადგენს. მიუხედავად მისი გამორჩეული ხასიათისა, ყოველდღიურ ცხოვრებაში სახელწიფო ხელისუფლების ორგანოებისა თუ კერძო დამსაქმებლების მხრიდან არც თუ იშვიათია კანონით დაცულ უფლებათა სფეროში არამართლზომიერი ჩარევა, გამოხატული ისეთ „უწყინარ“ ქმედებებში, რომელსაც ყოველდღიურ ცხოვრებაში ვხვდებით სამედიცინო დაწესებულებებში, დამსაქმებლებთან გასაუბრებისას, აპლიკაციების შევსებისა თუ ონლაინ მომსახურებისას.

სახელწიფოთა მიერ პირველადი გადაუდებელი ზომების მიღების მიუხედავად, Covid-19-თან ბრძოლა თანამედროვე მსოფლიოსთვის კვლავაც ერთ-ერთ მთავარ გამოწვევად რჩება. ინფიცირებულთა იდენტიფიცირებისა და მათი რიცხვის შემცირების მიზნით, აქტიურად ხდება როგორც ტრადიციული, ასევე ნოვაციური საშუალებების გამოყენება. მაგალითად, შეიქმნა მობილური აპლიკაცია[2], რომელიც იმის განსაზღვრით თუ რამდენად არის კონტაქტში შენთან ახლოს მყოფი პირი კორონავირუსის მატარებელი, არაპირდაპირ ადგენს ადამიანის ჯანმრთელობის მდგომარეობას. აგრეთვე, ქვეყანაში არსებული ეპიდსიტუაციის გაცნობის მიზნით, მედია საშუალებებით თითქმის ყოველდღიურად ვეცნობით დაინფიცირებულ თუ გამოჯანმრთელებულ პაციენტთა რაოდენობას, მათი ვინაობისა და მოთავსების ადგილის ჩათვლით. ეს ხდება მაშინ პერსონალურ მონაცემთა დაცვასთან დაკავშირებით მიღებულმა რეგულაცია GPDR (General Data Protection Regulation) - მა კორონავირუსის ტესტის შედეგების შენახვა და გავრცელება პერსონალურ მონაცემთა დარღვევად დაადგინა. შესაბამისად, ცალსახად ჩანს ის სირთულეები, რომელსაც კორონავირუსი არაერთი სფეროს (ჯანდაცვა, განათლება, კულტურა, ფინანსები და ა.შ) გარდა, პირველ რიგში საფრთხეს უქმნის ჩვენი გასანკუთრებული კატეგორიის პერსონალური მონაცემის დაცულობას. ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემის კონფიდენციალობის დაცვა კი მნიშვნელოვანია იმდენად, რამდენადაც მისმა გამჟღავნებამ შესაძლოა არსებითი ზიანი მიაყენოს ადამიანის პირად და ოჯახურ ცხოვრებას, პიროვნების თავისუფალ განვითარებას, მისი დასაქმების პერსპექტივასა და საზოგადოებაში ჩართულობას.

როდესაც ერთმანეთს უპირისპირდება საზოგადოებრივი ჯანმრთელობის დაცვისა და კერძო პირის უსაფრთხოების უზრუნველყოფის ინტერესები, აუცილებელია სახელმწიფომ უზრუნველყოს მათ შორის სამართლიანი ბალანსის დაცვა[3]. წინააღმდეგ შემთხვევაში

[1] მუხლი 2, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ”, 28 დეკემბერი, 2011.

[2] დ. მიკელსენი, ჰ. სოლერი, მ. სრანდელ- ჯანსონი, „Privacy, security, and public health in a pandemic year“, 2020 წლის 15 ივნისი, https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year# [უ.გ. 28.02.2020].

[3] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება №1/1/477 საქმეზე „საქართველოს სახალხო დამცველი საქართველოს პარლამენტის წინააღმდეგ“, 2011 წლის 22 დეკემბრი. II-45.

შეუძლებელი გახდება უფლებით პრაქტიკულად, რეალურად და ეფექტურად სარგებლობა და ის თეორიულ, ილუზორულ უფლებამდე გამოიფიტება[4], ასევე არ არის გამორიცხული სათანადო პირობების არსებობისას პერსონალური მონაცემების ხელყოფისათვის დადგეს სისხლისსამართლებრივი პასუხისმგებლობა.

ნაშრომის მიზანია ჯანმრთელობასთან დაკავშირებული ინფორმაციის დაცვასთან დაკავშირებული სირთულეების პრაქტიკულ ჭრილში წარმოჩენა, მათი გამჟღავნების რისკებისა და აღმოფხვრის გზების იდენტიფიცირება Covid-19ის პირობებში. თემის ფარგლებში განვიხილავ ამ მხრივ არსებულ ეროვნულ თუ საერთაშორისო კანონმდებლობას, პრეცედენტულ სამართალს და ბერკეტს რომლებსაც ECtHR-ის, ECHR-ის, IOM-ს, HDO-ს უახლეს რეკომენდაციებსა თუ დასკვნებში ვხვდებით.

საკითხის კომპლექსურობიდან გამომდინარე, ნაშრომის ფარგლებში გამოყენებული იქნება შედარებით-სამართლებრივი, ლოგიკური და სისტემური კვლევის მეთოდები, მოძიებული ინფორმაცია კი ანალიტიკური მეთოდის მეშვეობით დამუშავდება.

საკვანძო სიტყვები: პერსონალური მონაცემი, განსაკუთრებული კატეგორიის პეროსნალური მონაცემი, ჯანმრთელობასთან დაკავშირებული ინფორმაცია, ურთიერთდაპირისპირებული ინტერესები, არამართლზომიერი ხელყოფისაგან დაცვა, Covid-19, გადაჭრის მექანიზმები.

Abstract

According to Article 2 (b) of the Law of Georgia on Personal Data Protection, information related to a person's health is a special category of personal data. Despite its distinctive character, it is not uncommon for state authorities or private employers to interfere in the day-to-day life of a law-abiding human being, expressed in the "harmless" actions we encounter in our daily lives in medical facilities, interviewing employers, filling out applications or providing online servicesDespite state emergency measures, the fight against Covid-19 remains one of the major challenges facing the modern world. In order to identify the infected and reduce their number, both traditional and innovative means are actively used. For example, a mobile app was created, which, by determining how close a person in contact with you is to the carrier of the coronavirus, indirectly determines the state of human health. Also, in order to get acquainted with the epidemiological situation in the country, we inform the media almost daily about the number of infected or recovered patients, including their identities and places of placement. This happens when the General Data Protection Regulation (GPDR), then a personal data protection regulation, found that the storage and dissemination of coronavirus test results was a violation of personal data. Consequently, the difficulties faced by the coronavirus in a number of areas are clearly visible (Besides health, education, culture, finances, etc.), in the first place, there is a threat to the protection of personal data of our special category. Protecting the privacy of personal data related to health is so important that to the extent that its disclosure may cause substantial damage to a person's personal and family life, the free development of the individual, his or her employment prospects and involvement in society.

When the interests of public health and public safety are at odds with each other, it is essential that the state ensure a fair balance between them. Otherwise it will become impossible to practice rightly real

[4] მუხლი 157, საქართველოს კანონი „საქართველოს სისხლის სამართლის კოდექსი", 22 ივლისი, 1999.

and effective use and it is exhausted to the theoretical, illusory right, it is also not excluded that criminal proceedings may be instituted for the violation of personal data in the presence of proper conditions.

The aim of this paper is to present in a practical way the difficulties related to the protection of health information, to identify the risks of their disclosure and the ways to eliminate them under Covid-19. Within the topic, I will discuss the existing national or international legislation, case law and leverage, which we find in the latest recommendations or conclusions of the ECtHR, ECHR, IOM, HDO.

Due to the complexity of the issue, comparative-legal, logical and systematic research methods will be used within the paper, and the obtained information will be processed through analytical method.

Key words: Personal data, special category personal data, health information, conflicting interests, protection against unlawful encroachment, Covid-19, resolution mechanisms.

შესავალი

COVID-19– ით ინფიცირებულთა და გარდაცვლილთა რაოდენობის ზრდა ნათელს ხდის პანდემიასთან ბრძოლის ეფექტური მექანიზმების შემუშავების აუცილებლობას. თუმცა ეს გარემოება თავისთავად არ ნიშნავს პაციენტის პერსონალური მონაცემების კონფიდენციალურობის დაცვაზე უარი თქმას. მიუხედავად იმისა, რომ კორონავირუსი და მისი გავრცელების მასშტაბი ნოვაციური აღმოჩნდა სახელწიფოებისათვის, დღეისათვის აქტუალურ და ფართო მსჯელობის საგნად იქცა პერსონალურ მონაცემებზე მისი გავლენის საკითხი, რაც საზოგადოების ჯანმრთელობისა და პირის კონფიდენციალურობის ურთიერთდაპირისპირებაში გამოიხატება[5].

მრავალპროფილიანი საავადმყოფოები, კლინიკები, დამოუკიდებელი საექიმო და საექთნო საქმიანობის განმახორციელებელი პირები, საქართველოს შრომის, ჯანმრთელობის და სოციალური დაცვის სამინისტროს და მის დაქვემდებარებაში მყოფი საჯარო სამართლის იურიდიული პირები, ლაბორატორიები, სადაზღვევო კომპანიები თუ სხვა სამედიცინო დაწესებულებები ტიპური მაგალითია იმ ორგანიზაციებისა, რომლებიც აქტიურად ამუშავებენ პაციენტის ჯანმრთელობის შესახებ ინფორმაციას[6]. საინტერეოა, ტესტირების შედეგებს , მითუმეტეს თუ იგი ადასტურებს კორონავირუსით ინფიცირებას, რა ბედი ეწევა შემდგომ. როგორც ცნობილია, ისინი ირიცხება ეროვნული, სახელმწიფო და ადგილობრივი მთავრობების მთლიან სტატისტიკურ მონაცემებში. თუმცა ხაზგასამელია იმის დადგენა, თუ რა სამართლებრივი საფუძვლებით ხდება პერსონალური მონაცემთა ამ სახის მოპოვება, გამოყენება, დამუშავება, რამდენად ეფექტურია ამგვარ საქმიანობაზე განხორციელებული კონტროლის მექანიზმები და რამდენად უზრუნველყოფს ის ადამიანის პირადი ცხოვრებისა და მისთვის არასასურველი ცნობების გავრცელებისაგან დაცვას თანაზომიერების პრინციპის დაცვით.

სამართლებრივ სახელმწიფოში ადამიანის ბუნებითი თუ შეძენილი უფლების დაცვის პოზიტიური და ნეგატიური ვალდებულება პირველ რიგში გააჩნია ხელისუფლების

[5] D. Wartenberg, W.D. Thompson, "Privacy Versus Public Health: The Impact of Current Confidentiality Rules", *Am J Public Health*. 2010 წლის 18 მარტი.

[6] თ. კლაუპოლი, „COVID-19 and Data Privacy: Health vs. Privacy", 2020 წლის 26 მარტი. https://businesslawtoday.org/2020/03/covid-19-data-privacy-health vsprivacy/?fbclid=IwAR3nXt2YqeEcA4mzKUFdqUDvqTCzvOX4D9s9DVdYFHBr3ABX_bjK1nsAQqs [უ.გ. 08.02.2020].

ორგანოებს. სწორედ მათ უნდა გაატარონ ქვეყნის მასშტაბით ისეთი ღონისძიებები, რომლებიც თითოეულ ადამიანს მისი კუთვნილი უფლებებითა და ძირითადი თავისუფლებებით ჯეროვნად სარგებლობის შესაძლებლობას მისცემს. ეს კი შეუძლებელია გამართული და საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანილი კანონმდებლობის გარეშე. შესაბამისად, თავდაპირველად უნდა განსაზღვროს, მოქმედი ეროვნული კანონმდებლობა რამდენად პასუხობს Covid-19-ით გამოწვეულ ნოვაციებსა თუ სირთულეებს და ხომ არ დგას მისი გადახედვის საჭიროების საკითხი. მეორე მხრივ, მხოლოდ საკანონმდებლო სისტემა არ არის საკმარისი, არამედ აუცილებელია ამავდროულად პრაქტიკაში მისი დანერგვა.

1.პერსონალური მონაცემების მარეგულირებელი ეროვნული კანონმდებლობა

„ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის“ 1950 წლის ევროპული კონვენცია პირველივე მუხლში[7] ადგენს მაღალი ხელშემკვრელი სახელწიფოების ვალდებულებას, დაიცვან თავიანთ იურისდიქციაში მყოფი ნებისმიერი პირის უფლებები. ადამიანის პირადი და ოჯახური ცხოვრების ხელშეუხებლობა ეროვნულ დონეზე განმტკიცებულია ქვეყნის უზენაესი კანონის - საქართველოს კონსტიტუციის მეთხუთმეტე მუხლში[8]. საქართველოს საკონსტიტუციო სასამართლოს განმარტებით „ეს უფლება სასიცოცხლოდ აუცილებელია ადამიანის თავისუფლების, თვითმყოფადობისა და თვითრეალიზაციისათვის, მისი სრულყოფილად გამოყენების ხელშეწყობა და დაცვა არსებითად განმსაზღვრელია დემოკრატიული საზოგადოების განვითარებისათვის“[9]...., უფლება პირად ცხოვრებაზე ნიშნავს ინდივიდის შესაძლებლობას იყოს დაცული და უზრუნველყოფილი მის კერძო სფეროში სახელმწიფოს, ისევე როგორც ნებისმიერი სხვა პირების ჩარევისგან. იგი უზრუნველყოფს პიროვნების თავისუფალ განვითარებას, რადგან საშუალებას აძლევს მას, კერძო სფეროში საზოგადოების ჩარევისა და ყურადღებისაგან თავისუფალ პირობებში მოახდინოს ინფორმაციის, მოსაზრებებისა და შთაბეჭდილებების გაცვლა-გაზიარება”.[10] ადამიანი უნდა იყოს დაცული იმ ინფორმაციის გამჟღავნებისგან, რომლის მიმართაც მას პრივატულობის ობიექტური მოლოდინი გააჩნია.[11] ასეთი კატეგორიის ინფორმაციაში კი, უპირველეს ყოვლისა, სწორედ პერსონალური მონაცემები უნდა მოვიაზროთ, ვინაიდან „პერსონალურ მონაცემთა ,,ხელშეუხებლობა არის ინდივიდის ავტონომიურობის, დამოუკიდებელი განვითარების, მისი ღირსების დაცვის წინაპირობა“.[12]

[7] მუხლი 1, „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია“, 1950.

[8] მუხლი 15, „საქართველოს კონსტიტუცია“, 24 სექტემბერი, 1995.

[9]საქართველოს საკონსტიტუციო სასამართლოს N1/2/519 გადაწყვეტილება საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ჩუგოშვილი საქართველოს პარლამენტის წინააღმდეგ“, 2012 წლის 24 ოქტომბრი, II-2.

[10] საკონსტიტუციო სასამართლოს გადაწყვეტილება N1/3/407 საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ”,2007 წლის 26 დეკემბრის, II-4.

[11] საქართველოს საკონსტიტუციო სასამართლოს N2/3/1444 საოქმო ჩანაწერი საქმეზე „ნიკოლოზ აკოფოვი საქართველოს პარლამენტის წინააღმდეგ“, 2020 წლის 29 აპრილი. II-14.

[12] საქართველოს საკონსტიტუციო სასამართლოს N1/2/458 განჩინება საქმეზე, „საქართველოს მოქალაქეები - დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ“, 2009 წლის 10 ივნისი.

სწორედ ამ ასპექტების მხედველობაში მიღებით გამომდინარებს მისი კანონიერად დამუშავების მნიშვნელობაც.[13]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მეოთხე მუხლის თანახმად, პერსონალური მონაცემები უნდა დამუშავდეს 1. მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის; 2. ხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად (ე.წ. „მინიმიზაციის პრინციპი“; 3. შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მეექვსე მუხლის პირველი პუქტი კრძალავს განსაკუთრებული კატეგორიის პერსონალური მონაცემის დამუშავებას, გარდა იმ შემთხვევებისა თუ არსებობს 1. მონაცემთა სუბიექტის წერილობითი თანხმობა ან 2. იმავე მუხლის მეორე პუნქტით გათავლისწინებული კონკრეტული საგამონაკლისო საფუძვლები. ამ მხრივ საინტერესოა, კანონის მეექვე მუხლის მეორე პუნქტის „გ“ ქვეპუნტი, რომლის მიხედვითაც განსაკუთრებული კატეგორიის მონაცემების დამუშავება დასაშვებია, მაშინ როდესაც „მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის“.

Covid 19-ის პირობებში სულ უფრო და უფრო აქტუალური ხდება დაინფიცირებულ, გამოჯანმრთელებულ თუ გარდაცვლილ პაციენტთა რიცხობრივი მონაცემები. სტატისტიკის შედგენითა და რაოდენობის ურთიერთშედარების გზით შესაძლებელი ხდება იმის შეფასება, თუ სახელწიფოს მიერ გატარებული რომელი ღონისძიება (მაგალითად: სავაჭრო ცენტრების დახურვა, დისტანციურ მომსახურებაზე და სწავლებაზე გადასვლა, გადაადგილების თავისუფლები შეზღუდვა და ა.შ.) აღმოჩნდა ეფექტური და შედეგის მომტანი, განისაზღვრება მკაცრი რეგულაციების გატარების, ძალაში დატოვებისა თუ გაუქმების აუცილებლობის საკითხი (მაგალითად, კომენდანტის საათის დაწესება). ეს ყოველივე კი შეუძლებელია თუ არ იქნება ცნობილი და ხელმისაწვდომი თითოეული პაციენტის ჯანმრთელობის მდგომარეობა, ჩატარებული ტესტის რაოდენობა, ინფიცირებულის ვინაობის დადგენა კი აუცილებელია იმდენად, რამდენადაც უნდა მოხდეს მასთან კონტაქტში ახლო მყოფი პირების იდენტიფიცირება, დადგინდეს კონტაქტის ხანგრძლივობა, სიხშირე, სიახლოვის მანძილი და ასევე გადამოწმდეს აქვთ თუ არა მათ კორონავირუსისთვის დამახასიათებელი სიმპტომები და ა.შ. აქვე ხაზგასმით უნდა აღინიშნოს, რომ სამართლებრივი საფუძვლის არსებობა არ არის საკმარისი, არამედ მონაცემთა დამუშავების ნებისმიერ ეტაპზე ასევე აუცილებელია მისი თანაზომიერების პრინციპთან შესაბამისობა და მონაცემთა უსაფრთხოების დაცვა.[14] Covid-19-ით შექმნილი რეალობის გათვალისწინებით, ჯანმრთელობის შესახებ ინფორმაციის დამუშავების ლეგიტიმურ მიზნად უნდა მოვიაზროთ საზოგადოებრივი უსაფრთხოების დაცვა (ე.წ. „ჯაჭვების“ შემცირება), შესაძლოა ასეთი მონაცემების მოპოვება შესაბამისი იყოს კორონავირუსის გავრცელების ფარგლებისა და ამ გზით კანონიერი მიზნის მისაღწევად,

[13] პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაცია „ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ“, გვ. 6.

[14] პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაცია „ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ“, გვ. 11.

თუმცა კითხვის ნიშნის ქვეშ დგას მოცულობის საკითხი. კერძოდ, მართალია, მონაცემთა დამმუშავებელმა არ უნდა დაამუშაოს იმაზე მეტი მოცულობის ან კატეგორიის მონაცემი, ვიდრე ეს კანონიერი მიზნის მისაღწევად არის საჭირო, თუმცა ხშირად ხდება პაციენტის თანმდევი დაავადებების, ფიზიკური აქტივობის, საზღვარგარეთ მოგზაურობის, სამუშაო ადგილის შესახებ ინფორმაციის დამუშავება. აღნიშნული გარემოება სამედიცინო მონაცემების დაცვის თვალსაზრისით განსაკუთრებით პრობლემატურია ერთი მხრივ, იმ ასპექტით, რომ ფართო საზოგადოებისათვის უმრავლეს შემთხვევაში ცნობილი ხდება კოვიდინფიცირებულის სხვა დაავადებების ქონის შესახებ. მაგალითად, მახსენდება ინტერნეტსივრცეში თუ მედიაში გაშუქებული არაერთი სიუჟეტი, სადაც ნათქვამია რომ კონკრეტული პირის გარდაცვალება გამოწვეული იყო არა კორონავირუსით, არამედ იმ ქრონიკული დაავადებით (დიაბეტი, ჰეპატიტი, ტუბერკულიოზი), რომელიც პაციენტს ჰქონდა. მეორე მხრივ, თუკი პაციენტს აქვს გენეტიკური დაავადება, უნდა გამოირიცხოს მისი ოჯახის წევრის ან ახლო ნათესავის მიმართ ამგავრი მონაცემების შეგროვება. ვფიქრობ, დამუშავებული თუ მოპოვებული ინფორმაციის მოცულობა პრობლემატურია პრაქტიკული თვალსაზრისით და მასზე ეფექტური კონტროლის მექანიზმები უნდა ხორციელდებოდეს სახელწიფო ინსპექტორის მხრიდან.[15] ამას ემსახურება სახელწიფო ინსპექტორის უახლესი რეკომენდაციაც: „საზოგადოებრივი ინტერესის დასაკმაყოფილებლად საკმარისია პაციენტისა და მასთან დაკავშირებული პირების შესახებ *არაიდენტიფიცირებადი* ფორმით ინფორმაციის გავრცელება.[16]“ რაც შეეხება აუცილებლობის კრიტერიუმს, სახელწიფოს მოსახლეობის ჯანმრთელობის უსაფრთხოების დასაცავად, პირადი ცხოვრების უფლების მზღუდავი სხვა, შედარებით ნაკლებად მზღუდავი საშუალება, ვიდრე ეს ჯანმრთელობასთან დაკავშრებული პერსონალური მონაცემის დამუშავებაა, ამ ეტაპზე არ გააჩნია. ამასთანავე, „აუცილებელია, უფლებაშემზღუდველი ღონისძიების შემუშავებისას სახელმწიფომ დაადგინოს სამართლიანი ბალანსი იმგვარად, რომ დაცული სიკეთე და მისი დაცვის ინტერესი აღემატებოდეს შეზღუდული უფლების დაცვის ინტერესს.”[17] პანდემიის გათვალისწინებით, ერთი შეხედვით ეჭვს არ იწვევს ის ფაქტი, რომ ინფიცირებული პირების გამოვლენა, მათი იზოლაცია და საკარანტინო წესების დაცვა აუცილებელია სხვა პირთა უფლებებისა და ზოგადად, საზოგადოების ჯანმრთელობის (დაცული სიკეთე და მისი დაცვის ინტერესი) უზრუნველსაყოფად, თუმცა ასევე საყურადღებოა თავად შეზღუდული უფლების ბუნება და მისი ხასიათი - „ადამიანის პირადი ცხოვრების უფლება არის ერთ-ერთი ყველაზე სენსიტიური სფერო და საქართველოს კონსტიტუციაც მის დასაცავად განსაკუთრებით მაღალ სტანდარტს აწესებს“.[18] ხოლო ამ უფლების შეზღუდვით გამოწვეული რისკების მხედველობაში მიღებით, როგორც არის სამომავლო დასაქმების სირთულე, სტიგმატიზაცია, შესაძლო დისკრიმინაცია, პიროვნების თავისუფალი განვითარების ცალკეული ასპექტების (მათ შორის, რა ინფორმაცია იყოს სხვებისთვის ცნობილი და რა არა) რთულია იმის რადიკალურად თქმა, რომ დაკმაყოფილებულია პროპორციულობა ვიწრო გაგებით.

---

[15] სახელწიფო ინსპექტორის ბრძანება №2 , 2019 წლის 2 ივლისი.

[16] სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები “COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავება“, 2020 წელი, გვ. 2.

[17] საქართველოს საკონსტიტუციო სასამართლოს №3/1/752 გადაწყვეტილება საქმეზე „ა(ა)იპ „მწვანე ალტერნატივა“ საქართველოს პარლამენტის წინააღმდეგ“, 2018 წლის 14 დეკემბრი, II-28.

[18] საქართველოს საკონსტიტუციო სასამართლოს №2/1/484 გადაწყვეტილება საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ხიდაშელი საქართველოს პარლამენტის წინააღმდეგ“, 2012 წლის 29 თებერვლი, II- 15,17.

2. პერსონალურ მონაცემთა საერთაშორიო რეგულაცია და პრეცედენტული სამართალი

ადამიანის უფლებათა უკეთ დაცვის მიზნით კვლავ აქტუალურად რჩება საერთაშორისო სტანდარტების, საერთაშორისო სასამართლოების პრაქტიკისა და სხვა ქვეყნების გამოცდილების გაზიარება. ამ მხრივ, თავისი მნიშვნელობით აღსანიშნავია 1950 წლის ევროპული კონვენცია, რომელიც ადამიანის უფლებათა ევროპულმა სასამართლომ და ევროპულმა კომისიამ „ევროპული საჯარო წესრიგის კონსტიტუციურ აქტად“ აღიარა[19], რომელმაც უნდა შეასრულოს მთავარი როლი, რაზეც დამოკიდებულია კონტინენტის დემოკრატიული სტაბილურობა.[20]

Covid-19-ის პირობებში ჯანმრთელობის მდგომარეობის შესახებ მონაცემების დამუშავებასა და პირადი ცხოვრების უფლების ურთიერთმიმართებაზე სტრასბურგის სასამართლოს ჯერჯერობით არ უმსჯელია, რაც პანდემიის ნოვაციური ხასიათის გათვალისწინებით, ალბათ ლოგიკურადაც უნდა ჩაითვალოს. თუმცა მომავალში ამ საფუძვლით საჩივრების წარდგენა არ არის გამორიცხული. ზოგადი მიდგომის მიხედვით, ადამიანის უფლებათა ევროპული სასამართლო თავის პრეცედენტულ სამართალში ერთგვაროვნად განმარტავს, რომ „პერსონალური მონაცემების დაცვის უფლება წარმოადგენს იმ უფლებათა ნაწილს, რომელიც დაცულია კონვენციის მერვე მუხლში („პირადი და ოჯახური ცხოვრების დაცულობის უფლება)“[21]. „მონაცემთა დაცვის დირექტივის[22]“ მე-8 მუხლის პირველი პუნქტისა და „108-ე კონვენციის“ მე-6 მუხლის“[23] მსგავსად, ევროპული კონვენციაც განსაკუთრებულ მონაცემებად მიიჩნევს ინფორმაციას პირის ჯანმრთელობის მდგომარეობის შესახებ და სამედიცინო მონაცემების დამუშავებისთვის არასენსიტიურ მონაცემებთან შედარებით გამკაცრებულ სტანდარტს ადგენს. წინააღმდეგ შემთხვევაში, თუკი ინდივიდს არ ექნება მისი კონფიდენციალური ინფორმაციის დაცვის გარანტია, მას, ვისაც სამედიცინო დახმარება სჭირდება, ინტიმური დეტალების გამჟღავნების შიშის მოტივით, შესაძლოა თავი აარიდოს შესაბამისი სამედიცინო დაწესებულისადმი მიმართვას. ეს კი, თავის მხრივ, საფრთხის შემქმნელია როგორც პაციენტის, ასევე საზოგადოების ჯანმრთელობისათვის (გადამდები დაავადებების შემთხვევაში)[24]. სასამართლო სამედიცინო დიაგნოზებს შორის განსაკუთრებული სენსიტიურობით გამოყოფს „აივ ინფექციას“, ვინაიდან იგი სტიგმატიზაციის მაღალი რისკის შემცველია როგორც ოჯახურ, ისე სოციალურ თუ შრომით ურთიერთობებში. ამის ნათელი მაგალითია გადაწყვეტილება საქმეზე „ზ. ფინეთის

[19] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „Chrysostomos v. Turkey“, 1991 წლის 4 მარტი, პარაგრაგი 22; ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „Loizidou v. Turkey“, 1995 წლის 23 მარტი, პარაგრაფი 75.

[20] Declaration “The European Convention on Human Rights at 50: What Future for the Protection of Human Rights in Europe”, in: Texts adopted by the European Ministerial Conference on Human Rights, (2000)1,10.

[21] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე No. 20511/03 „I. v. Fin land “, 2008 წლის 17 ივლისი; ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე No. 2872/02 „K.U. v. Fin land “, 2008 წლის 2 დეკემბერი.

[22] მუხლი 8, დირექტივა 95/46/EC/ „პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკური პირის დაცვის შესახებ“ (მონაცემთა დაცვის დირექტივა), 24 ოქტომბერი, 1995.

[23] მუხლი 6, კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“, 28 იანვარი, 1981 წელი.

[24] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N7508/02 „L.L. v. France“, 2006 წლის 10 ოქტომბერი.

წინააღმდეგ“[25]. ფაქტობრივი გარემოებების მიხედვით, ეროვნული სასამართლოების მიერ გამოტანილი განაჩენ შეიცავდა ინფორმაციას მსჯავრდებულის დაავადების შესახებ, ისევე როგორც, განმცხადებლისა და მისი მეუღლის სრულ სახელებს. აღნიშნული შემაჯამებელი გადაწყვეტილების გასაჯაროება თუნდაც 10 წლის შემდეგ (რა ვადაშიც იგი რჩებოდა კონფიდენციალურად) ვერ აკმაყოფილებდა უფლებაშ ჩარევისათვის აუცილებლობის კრიტერიუმს, რის გამოც დადგინდა მოსარჩელის პირადი ცხოვრების უფლების დარღვევას. ევროპულმა სასამართლომ დარღვევად მიიჩნია ასევე პაციენტის თანხმობის გარეშე მისი სამედიცინო ისტორიის გარეშე პირებისათვის ხელმისაწვდომობა, ისევე როგორც ამგვარი ინფორმაციის დიდი ხნის განმავლობაში შენახვა.[26]

„ევროსაბჭოს 1997 წლის რეკომენდაცია სამედიცინო მონაცემების შესახებ“[27] კიდევ უფრო აფართოებს დაცვის სფეროებს და გარდა იმისა, რომ ჯანმრთელობი შესახებ ინფორმაციის დამუშავებას დასაშვებად მიიჩნევს მხოლოდ სამედიცინო პერსონალის მიერ პროფესიული საიდუმლოს დაცვის ვალდებულებით[28], იგი შეიცავს სპეციალურ დებულებებს ჯერ კიდევ დაუბადებელი ბავშვებისა და უნარწართმეული პირების სამედიცინო მონაცემების რეგულაციასთან დაკავშირებით. გასათვალიწინებელია ის გარემოებაც, რომ თუკი პერსონალური მონაცემები მუშავდება სტატისტიკური მიზნებისათვის, დაცული უნდა იყოს რამდენიმე კრიტერიუმი: 1. იგი არ შეიძლება გამოყენებულ იქნას სხვა მიზნისათვის; 2. შიდასახელწიფოებრივი კანონმდებლობა უნდა ადგენდეს დაცვის ადექვატურ მექანიზმებს.[29] სტატისტიკის შესახებ ევროპული რეგულაცია 223/2009-ის მიხედვით კი ოფიციალური სტატისტიკის ოპერაციებს ესაჭიროებათ საკმარისად ზუსტი სამართლებრივი საფუძველი[30]. აღსანიშნავია , ასევე მინისტრთა კომიტეტის მიერ შემუშავებული უახლესი რეკომენდაცია, მრავალ მნიშვნელოვან საკითხთან ერთად ადგენს მონაცემთა დამმუშავებლის ვალდებულებას, დამუშავების დაწყებამდე და დროის რეგულარულ ინტერვალებში, შეაფასოს მონაცემთა დაგეგმილი დამუშავების პოტენციური გავლენა მონაცემთა დაცვასა და პირადი ცხოვრების ხელშეუხებლობაზე[31].

საერთაშორისო რეგულაციის მიმოხილვის შედეგად გამოიკვეთა, რომ სამედიცინო მონაცემების დამუშავება უნდა აკმაყოფილებდეს მკაცრად გაწერილ კრიტერიუმებს, წინააღმდეგ შემთხვევაში დადგინდება პირადი ცხოვრებისის უფლების დარღვევა.

---

[25] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N22009/93 „Z. v. Finland“, 1997 წლის 25 თებერვალი, პარაგრაფები 94,112.

[26] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N42788/06 „SURIKOV v. UKRAINE“, 2017 წლის 26 იანვარი, პარაგრაფები 70, 89.

[27] ევროპის საბჭო, მინისტრთა კომიტეტი (1997), რეკომენდაცია „(97)5 წევრი ქვეყნებისთვის სამედიცინო მონაცემების დაცვის შესახებ“, 13 თებერვალი, 1997 წელი.

[28] იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N23373/03 „Biriuk v. Lithuania“, 25 თებერვალი 2009 წლის 25 თებერვალი.

[29] Handbook on European Data Protection Law, 2020.

[30] ევროპული პარლამენტისა და საბჭოს 2009 წლის 11 მარტის რეგულაცია (EC) N223/2009 “ევროპული სტატისტიკის შესახებ”.

[31] მინისტრთა კომიტეტის რეკომენდაცია CM/Rec(2019) 2 წევრი სახელმწიფოების მიმართ “ჯანმრთელობასთან დაკავშირებული მონაცემების დაცვის შესახებ”.

3. პრობლემის გადაჭრის ჩემეული ხედვა

საჯარო და კერძო ინტერესების ურთიერთდაპირისპირება თითოეული სახელწიფოსთვის პრობლემატური და აქტუალური საკითხია, რომელმაც კიდევ უფრო მეტი დატვირთვა შეიძინა Covid-19-ის პირობებში. კაცობრიობა განვითარების სხვადასხვა ეტაპზე არაერთი გამოწვევის წინ იდგა და კვლავაც დგას, თუმცა ნებისმიერ შემთხვევაში ამოსავალი წერტილი უნდა იყოს ადამიანის უფლებებისა და ძირითადი თავისუფლებების დაცვა. შესაძლოა, ეროვნული რეგულაცია ერთი შეხედვით არავითარ პრობლემას არ ქმნის პეროსნალურ მონაცემთა დაცვის გარანტიასთან მიმართებით, მაგრამ განსხვავებული სიტუაცია გვხვდება ჩვენს ყოველდღიურ ცხოვრებაში. ეს კი იმაზე მიუთითებს, რომ პრაქტიკული თვალსაზრისით საკითხის კანონიერად და სამართლიანად რეალიზაცია კითხვის ნიშნის ქვეშ დგას. შესაბამისად, გათვალისწინებულ უნდა იქნეს GPDR-ის მიერ შემუშავებული უახლესი რეკომენდაციები, რომლითაც მოითხოვება სამედიცინო მონაცემების დამუშავებით გამოწვეული რისკების შეფასება, კონტროლის განხორციელება, კონფიდენციალურობის დაცვა, მიზნების დავიწროვება და მოცულობის მინიმიზაცია. რაც მთავარია, პაციენტს უნდა გაუჩნდეს ნდობა და თავი იგრძნოს უსაფრთხოდ, დაცულად.[32]

პრაქტიკაში არსებული მდგომარეობის გათვალისწინებით, ვფიქრობ განსაკუთრებული ყურადღება უნდა მიექცეს ისეთ საკითხებს, როგორებიცაა: 1. *ინფორმაციის გაცემა* - კოვიდ ტესტის პასუხი მატერიალური ან ელექტრონული ფორმით გაიცეს მხოლოდ იმ პირზე, ვინც კვლევას იტარებს და არ გახდეს იგი ხელმისაწვდომი ნებისმიერი სხვა პირისათვის (იქნება ეს ნათესავი თუ ოჯახის წევრი), თუნდაც მას თან ჰქონდეს პაციენტის პირადობის დამადასტურებელი დოკუმენტი. განსაკუთრებით უნდა გაკონტროლდეს რეგიონში არსებული კლინიკები. 2. *სტატისტიკის დამუშავება* - საზოგადოების ინფორმირება უნდა მოხდეს მხოლოდ მაიდენტიფიცირებელი ინფორმაციის გამომრიცხველი ფორმით. ქართულ რეალობაში ეს წესი ძირითადად დაცულია, რაც დადებითად უნდა შეფასდეს. 3. *ცნობადი სახეების* დაინფიცირების დროს, საზოგადოების ინტერესი განსაკუთრებით მაღალია, რის გამოც მედიასაშუალებები ყოველმხრივ ცდილობენ მათი ჯანმრთელობის მდგომარეობის შესახებ დეტალური ინფორმაციის მოპოვებას. ასეთ დროს, მკურნალმა ექიმებმა თავი უნდა შეიკავონ დეტალური ინფორმაციის გავრცელებისაგან, პაციენტის ნებართვის გარეშე; 4. სახელწიფო თუ კერძო დაწესებულებების მიმართ გატარდეს კონტროლი და შემუშავდეს მკაცრი რეგულაციები. მაგალითად, თუკი სასამართლოში გადამოწმებისას პროცესის მონაწილეს დაუდასტურდა ტემპერატურა ან კორონავირუსის სხვა სიმპტომი, ეს არ გაჟღერდეს ღია სასამართლო სხდომაზე, ამ პირის თანხმობის გარეშე. უფრო მეტიც, თუ არსებობს სამედიცინო დოკუმენტაცია რომ პროცესის მონაწილის გამოუხადებლობა გამოწვეულია საპატიო მიზეზით - Covid-19-ის დადასტურებით, სხდომა ამ ნაწილში დაიხუროს. ვფიქრობ, ზემოაღნიშნული საკითხები განსაკუთრებით სენსიტიურია არასრუწლოვნების მიმართ, ვინაიდან მათი სამომავლო განვითარების პერსპექტივა მრავალი ასპექტით შეიძლება პრობლემატური გახდეს. მხედველობაშია მისაღები ის გარემოებაც, რომ როდესაც კოვიდინფიცირებული იმყოფება თვითიზოლაციაში ან თუნდაც

[32] ე. ვენტრელა, „Privacy in emergency circumstances: data protection and the COVID-19 pandemic“, 2020 წლის 22 სექტემბერი, ხელმისაწვდომია აქ:
https://link.springer.com/article/10.1007/s12027-020-00629-3?fbclid=IwAR1Nnx30tG-xybji19oGQf2YTmDnPZ-gObBofOVEcmfsB2adl3rFAnqg_MI [უ.გ. 28.02.2020].

საზღვარგარეთიდან დაბრუნებული ადამიანი ემორჩილება სავალდებულო საკარანტინო ზომებს, რითაც აპრიორი ცნობილი ხდება მის შესახებ კონკრეტული მონაცემები, რამდენად დაცულია პირადი ცხოვრების უფლების ის შემადგენელი ნაწილი, რომელიც გულისხმობს პირის შესაძლებლობას, თავად გადაწყვიტოს საზოგადოებისათვის რა ინფორმაციას გახდის ცნობილს?!

ეს მხოლოდ მოკლე ჩამონათვალია იმ საკითხებისა, რომელიც ადასტურებს, რომ კანონმდებლობა ,,ვალდებულია“ მუდმივად განახლებად რეჟიმში იმყოფებოდეს, მაქსიმალურად ფეხი აუწყოს Covid-19-ით გამოწვეულ სიახლეებს, რათა პიროვნებამ ,,დამოუკიდებლად განსაზღვროს გარესამყაროსთან კავშირის ინტენსივობა და ფორმები.“[33] ამ მხრივ, მნიშვნელოვანია სახელწიფო ინსპექტორის როლი, რომელმაც სამედიცინო მონაცემების დამუშავების ყოველ კონკრეტულ შემთხვევაზე ეფექტური კონტროლი უნდა განახორციელოს.

დასკვნა

ნაშრომში დასმული საკითების ანალიზის შედეგად გამოიკვეთა, რომ Covid-19-თან ბრძოლა არ შემოიფარგლება მხოლოდ ვირუსის გავრცელების მასშტაბების შეცმირებით. ის გაცილებით ფართოა და თავის მხრივ, არაერთ სამართლებრივ პრობლემას წარმოშობს, რომელთა შორის ფუნდამენტური მნიშვნელობისაა სამედიცინო მონაცემების დაცვა.

მართალია, პერსონალურ მონაცემთა დაცვა არ არის აბსოლუტური უფლება და როგორც ეროვნული, ისე საერთაშორისო კანონმდებლობა ადგენს მისი დამუშავების შესაძლებლობას, თუმცა ყოველ კონკრეტულ შემთხვევაში უნდა შეფასდეს რამდენად ხორციელდება ეს აქტივობები დადგენილი სტანდარტის შესაბამისად. Covid -19-ის პირობებშიც არ უნდა დაგვავიწყდეს ნებისმიერი ღონისძიების კანონიერებისა თუ სამართლიანობის საზომი არის ადამიანის უფლებები (ჩვენს შემთხვევაში პირადი ცხოვრებისა და პიროვნების თავისუფალი განვითარების უფლება).

იქიდან გამოდინარე, რომ ერთიანი და მკაცრად დადგენილი საუკეთესო რეგულაცია არ არებობს, რომელიც დაიცავდა ბალანსს ერთი მრივ Covid-19-თან გასამკლავებლად და მეორე მრივ, სამედიცინო მონაცების გამოყენებასთან დაკავშრებით, ვფიქრობ, პრობლემის გადასაჭრელი ძირითადი ზომები იქნება, თუკი მაქსიმალურად გამკაცრდება კონტროლის მექანიზმები, ამაღლდეს ცნობიერება პერსონალურ მონაცემთა რაობისა და არსის შესახებ. ეს კი შესაძლებლობას მოგვცემს, თითოეულმა ჩვენგანმა შევძლოთ კუთვნილი უფლების ეფექტურად სარგებლობა და არ გამოიფიტოს იგი ილუზორულ და თეორიულ უფლებამდე[68].

[33] ლ. ფაფიაშვილი, „პირადი ცხოვრების ხელშეუხებლობა პირადი ჩხრეკისას მობილურ ტელეფონებთან მიმართებით“, *საკონსტიტუციო სამართლის მიმოხილვა,* 2015, VIII, გვ. 81.

[68] ადამიანის უფლებათა ევროპული სასამართლოს 1980 წლის 13 მაისის გადაწყვეტილება საქმეზე "არტიკო იტალიის წინააღმდეგ", პარაგრაფი 33.

ბიბლიოგრაფია

1. საქართველოს კონსტიტუცია;
2. საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ;
3. საქართველოს სისხლის სამართლის კოდექსი;
4. ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის 1950 წლის ევროპული კონვენცია;
5. კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ;
6. დირექტივა 95/46/EC/ პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკური პირის დაცვის შესახებ (მონაცემთა დაცვის დირექტივა);
7. კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“;
8. ევროპული პარლამენტისა და საბჭოს რეგულაცია „ევროპული სტატისტიკის შესახებ“;
9. მინისტრთა კომიტეტის რეკომენდაცია „ჯანმრთელობასთან დაკავშირებული მონაცემების დაცვის შესახებ“;
10. ევროპის საბჭო, მინისტრთა კომიტეტის რეკომენდაცია „ წევრი ქვეყნებისთვის სამედიცინო მონაცემების დაცვის შესახებ“;
11. სახელწიფო ინსპექტორის ბრძანება №2;
12. სახელწიფო ინსპექტორის სამსახურის რეკომენდაციები “COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონახემთა დამუშავების შესახებ“;
13. Declaration “The European Convention on Human Rights „ What Future for the Protection of Human Rights in Europe “;
14. პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაცია „ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ“;
15. საქართველოს საკონსტიტუციო სასამართლო გადაწყვეტილება №1/1/477 საქმეზე „საქართველოს სახალხო დამცველი საქართველოს პარლამენტის წინააღმდეგ“, 22.12.2011;
16. საქართველოს საკონსტიტუციო სასამართლოს N1/2/519 გადაწყვეტილება საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ჩუგოშვილი საქართველოს პარლამენტის წინააღმდეგ“, 24.10. 2012;
17. საკონსტიტუციო სასამართლოს გადაწყვეტილება N1/3/407 საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ”, 26.12.2007;
18. საქართველოს საკონსტიტუციო სასამართლოს N2/3/1444 საოქმო ჩანაწერი საქმეზე „ნიკოლოზ აკოფოვი საქართველოს პარლამენტის წინააღმდეგ“, 29.04.2020;
19. საქართველოს საკონსტიტუციო სასამართლოს N1/2/458 განჩინება საქმეზე, „საქართველოს მოქალაქეები - დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ“, 10.06.2009;
20. საქართველოს საკონსტიტუციო სასამართლოს №3/1/752 გადაწყვეტილება საქმეზე „ა(ა) იპ „მწვანე ალტერნატივა“ საქართველოს პარლამენტის წინააღმდეგ“, 14.12.2018;

21. საქართველოს საკონსტიტუციო სასამართლოს №2/1/484 გადაწყვეტილება საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ხიდაშელი საქართველოს პარლამენტის წინააღმდეგ“, 29.02.2012;
22. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე "არტიკო იტალიის წინააღმდეგ", 13.05.1980;
23. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ლ.ლ საფრანგეთის წინააღმდეგ“, 10.10.2006;
24. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ზ ფინეთის წინააღმდეგ“, 25.02.1997;
25. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „სურიკოვი უკრაინიის წინააღმდეგ“, 26.01.2017;
26. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ბირიუკოვი ლიტვის წინააღმდეგ“, 25.02.2009;
27. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ქრისოსტომოსი თურქეთის წინააღმდეგ“, 04.03.1995;
28. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ლოიზიდოუ თურქეთის წინააღმდეგ“, 23.03.1995;
29. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „ი. ფინეთის წინააღმდეგ“,17.07.2008;
30. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „კ.უ. ფინეთის წინააღმდე“;
31. დენიელ მიკელსენი, ჰენინგ სოლერიდა მალინ სრანდელ- ჯანსონი, „უსაფრთხოება და საზოგადოებრივი ჯანმრთელობა პანდემიის პირობებში“;
32. ლალი ფაფიაშვილი, „პირადი ცხოვრების ხელშეუხებლობა პირადი ჩხრეკისას მობილურ ტელეფონებთან მიმართებით“;
33. ემანუელ ვენტრელა, „უსაფრთხოება საგანგებო ვითარებაში : „პერსონალურ მონაცემთა დაცვა და COVID-19“;
34. პერსონალურ მონაცემთა ევროპული დაცვის სამართლის გზამკვლევი.

Bibliography

1. The Constitution of Georgia;
2. Law of Georgia on Personal Data Protection;
3. Criminal Code of Georgia;
4. 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms;
5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;
6. Directive 95/46 / EC / on the processing of personal data and the protection of individuals with regard to the free movement of such data (Data Protection Directive);
7. Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data;
8. Regulation of the European Parliament and of the Council on European Statistics.
9. Recommendation of the Committee of Ministers on the protection of health-related data;

10. Council of Europe, Recommendation of the Committee of Ministers on the protection of medical data for Member States;
11. Order of the State Inspector №2;
12. Recommendations of the State Inspector's Office on the processing of personal belongings in the fight against COVID-19;
13. Declaration "The European Convention on Human Rights" What Future for the Protection of Human Rights in Europe ";
14. Recommendation of the Personal Data Protection Inspector on the processing of personal data in the field of healthcare;
15. The Constitutional Court of Georgia of 22 December 2011 № 1/1/477 in the case "Public Defender of Georgia v. Parliament of Georgia";
16. Decision N1 / 2/519 of the Constitutional Court of Georgia of October 24, 2012 on the case "Georgian Young Lawyers Association and Tamar Chugoshvili, Citizen of Georgia v. Parliament of Georgia";
17. Judgment of the Constitutional Court of 26 December 2007 in the case N1 / 3/407 "Georgian Young Lawyers Association and Citizen of Georgia Ekaterine Lomtatidze v. Parliament of Georgia";
18. Minutes of the Constitutional Court of Georgia N2 / 3/1444 of April 29, 2020 on the case "Nikoloz Akofov v. Parliament of Georgia";
19. 5.Judgment N1 / 2/458 of the Constitutional Court of Georgia of 10 June 2009 on the case "Citizens of Georgia - Davit Sartania and Aleksandre Macharashvili v. Parliament of Georgia and the Ministry of Justice of Georgia";
20. Decision of the Constitutional Court of Georgia №3 / 1/752 of 14 December 2018 on the case A (A) IP Green Alternative v. Parliament of Georgia;
21. 7.Judgment of the Constitutional Court of Georgia №2 / 1/484 of 29 February 2012 in the case "Georgian Young Lawyers Association and Tamar Khidasheli, Citizen of Georgia v. Parliament of Georgia";
22. Judgment of the European Court of Human Rights of 13 May 1980 in Artico v. Italy;
23. Judgment of the European Court of Human Rights of 10 October 2006 in the case of L.L. v. France;
24. Judgment of the European Court of Human Rights of 25 February 1997 in the case of Z v. Finland;
25. Judgment of the European Court of Human Rights of 26 January 2017 in the case of Surikov v. Ukraine;
26. Judgment of the European Court of Human Rights of 25 February 2009 in the case of Biryukov v. Lithuania;
27. Judgment of the European Court of Human Rights of 4 March 1995 in the case of Chrysostom v. Turkey;
28. Judgment of the European Court of Human Rights of 23 March 1995 in the case of Loisidow v. Turkey;
29. The judgment of the European Court of Human Rights of 17 July 2008 in the case "I. V. Finland";
30. The judgment of the European Court of Human Rights of 2 December 2008 in the case of K.U. V. Finland";

31. Daniel Mickelsen, Henning Solerida and Malin Srandel-Johnson, "Safety and Public Health in a Pandemic";
32. Lali Papiashvili, "Inviolability of personal life in connection with personal search of mobile phones";
33. Emmanuel Ventrela, "Emergency Security: Personal Data Protection and COVID-19";
34. Guide to European Personal Data Protection Law.

არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები

თამარ ფაჩულია,
თბილისის სახელმწიფო უნივერსიტეტი

აბსტრაქტი

მართალია, საქართველოს კანონმდებლობა პერსონალურ მონაცემთა დაცვის სუბიექტის განსაზღვრის საკითხში სრულად ეხმიანება ევროპის სახელმწიფოთა უმრავლესობის მიდგომას და სუბიექტის სტატუსს ანიჭებს ნებისმიერ ფიზიკურ პირს, მაგრამ გამოკვეთილია არასრულწლოვანი პირების პერსონალური მონაცემების დამუშავებისას მათი ძირითადი უფლებებისა თუ თავისუფლებების დაცვის განსაკუთრებული საჭიროება, ვინაიდან ისინი ხშირად ვერ აცნობიერებენ სხვადასხვა სახის პერსონალური მონაცემების ინტერნეტში გავრცელების რისკებსა თუ მოსალოდნელ შედეგებს. არასასურველი მასალის გავრცელებამ შესაძლოა ხელი შეუწყოს არასრულწლოვანთა მიმართ კიბერბულინგის განხორციელებას, რაც განსაკუთრებით საფრთხისშემცველია იმის გათვალისწინებით, რომ ინტერნეტი ბულინგისთვის გაცილებით დიდ მასშტაბს იძლევა და შესაბამისად, მისი შეჩერება რთულდება, განსაკუთრებით კი მაშინ, როდესაც მსხვერპლის როლში არის არასრულწლოვანი.

აღნიშნული საფრთხეების გათვალისწინებით არასრულწლოვანთა პერსონალური მონაცემების დაცვის საჭიროება დღის წესრიგში იდგა და დგას ყოველთვის, თუმცა დღევანდელი რეალობის გათვალისწინებით, ახალ კორონავირუსთან- „COVID-19" ბრძოლის პროცესში, კიდევ უფრო იმატა ამ საკითხის აქტუალობამ. მიუხედავად შესაძლო საჯარო ინტერესისა, ნებისმიერი პაციენტის, განსაკუთრებით კი არასრულწლოვანი პაციენტების, ჯანმრთელობასთან დაკავშირებული ინფორმაციის ხელმისაწვდომობის უზრუნველყოფისას აუცილებელია განსაკუთრებული სიფრთხილის გამოჩენა, რადგან „პერსონალური მონაცემთა დაცვის შესახებ" საქართველოს კანონი ჯანმრთელობის შესახებ ცნობებს განსაკუთრებული კატეგორიის მონაცემთა შორის ასახელებს. აქედან გამომდინარე, ნაშრომში ყურადღება იქნება გამახვილებული პანდემიის პირობებში პერსონალური მონაცემების მიმართ საქართველოსა და სხვა სახელმწიფოების კანონმდებლობის მიდგომასა და გამოვლენილი დარღვევების ხასიათზე.

არასრულწლოვანთა პერსონალური მონაცემების დამუშავებისას კანონის მოთხოვნათა დარღვევის ფაქტები ვლინდება სხვადასხვა დაწესებულებებში, განსაკუთრებით ხშირად ვხვდებით ამგვარ შემთხვევებს საგანმანათლებლო დაწესებულებებში, სადაც მოზარდი დღის დიდ ნაწილს (20-30%) ატარებს. აღნიშნული დაწესებულებები არასრულწლოვანთა შესახებ არაერთ პერსონალურ ცნობას ფლობენ, თუმცა ინტერნეტში მათი გავრცელების რისკები დისტანციური სწავლების პერიოდში უფრო მეტად იჩენს თავს. სწორედ ამიტომ ნაშრომში წარმოჩენილი იქნება დარღვევის კონკრეტული შემთხვევები და მათი პრევენციის გზები.

ნაშრომში ასევე ყურადღება იქნება გამახვილებული პერსონალური მონაცემების დაცვის უფლების ფარგლებზე, მისი შეზღუდვის თანაზომიერებასა და კონსტიტუციაში სახელდებითა და პირდაპირ გათვალისწინებული უფლებების მნიშვნელობასთან აღნიშნული უფლების შეპირისპირებაზე. განხილული იქნება არასრულწლოვანთა პერსონალური

მონაცემების დამუშავების საკითხზე საერთო სასამართლოებისა და საკონსტიტუციო სასამართლოს პრაქტიკის შესაბამისობა საერთაშორისო სტანდარტებთან.

და ბოლოს, ვინაიდან საქართველოში პერსონალური მონაცემების დაცვის საკითხმა განსაკუთრებული აქტუალობა შეიძინა ,,პერსონალურ მონაცემთა დაცვის ინსპექტორის საქმიანობისა და მისი უფლებამოსილების განხორციელების წესის შესახებ დებულების დამტკიცების თაობაზე“ მთავრობის დადგენილების გამოცემის შემდეგ, ნაშრომში განხილული იქნება სახელმწიფო ინსპექტორის სამსახურის, როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამონაცვლის, როლზე კონკრეტულად არასრულწლოვანთა პერსონალური მონაცემების დაცვის სფეროში.

საკვანძო სიტყვები: არასრულწლოვნის პერსონალური მონაცემები, კიბერბულინგი, პანდემია, თანაზომიერება.

Abstract

It is true that, Georgian legislation fully answers the approach of majority of European countries in determining the subject of personal data protection and grants the status of a subject to any natural person, but there is a particular need to protect the fundamental rights or freedoms of minors in the processing of personal data, because they often could not realize the risks or expected consequences of disclosing personal information on the Internet. Dissemination of unwanted materials may facilitate cyberbullying of minors; this is especially dangerous because the internet provides much larger scale for bullying and therefore makes it difficult to stop it, especially when the victim is a minor.

According to this danger, the need to protect the personal data of minors has always been on the agenda, however in today's reality in the fight against the new coronavirus - "COVID-19" the urgency of this issue has increased even more. Despite the possible public interest, special care must be taken when providing access to health information for any patients, especially minor patients, because the Law of Georgia on "Personal Data Protection" names information about health among the special categories of data. Therefore, the work will focus on the approach of personal data of Georgian and other countries' legislation and the nature of the identified violations in the conditions of the pandemic. Violations of the law during the processing of personal data of minors are revealed in various institutions, especially we often face such cases in educational institutions, where adults spend most of the day (20-30%).These institutions have a lot of personal information about minors, but the risks of spreading them on the Internet are more apparent during distance learning. That is why this work will present specific cases of violations and ways to prevent them. The work will also focus on the scope of the right to protection of personal data, the proportionality of its restriction and designation in the Constitution and contradiction of the said rights with the importance of directly provided rights. Compliance of common courts and the practice of the Constitutional Court with international standards on the processing of personal data of minors will be discussed.

Finally, since the issue of personal data protection in Georgia has gained special urgency after the issuance of a Government Decree on the "approval of the Regulation on the activities of the Personal Data Protection Inspector and the exercise of his authorities", this work will discuss the role of the State Inspector's work as a successor of Personal Data Protection Inspector, specifically in the field of personal data protection of minors.

Key words: Personal data about minors, cyberbullying, pandemic, proportionality.

შესავალი

ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-12 მუხლი ადგენს, რომ ყველა ადამიანს აქვს უფლება, დაცული იყოს პირად ცხოვრებაში თვითნებური ჩარევისგან. შესაბამისად, პერსონალურ მონაცემთა დაცვის უფლება, როგორც პირადი ცხოვრების უფლების ერთ-ერთი შემადგენელი ნაწილი, ყველა ფიზიკურ პირზე ვრცელდება. პერსონალური მონაცემების დაცვის შესახებ საქართველოს კანონმდებლობა შესაბამისობაშია დეკლარაციის მოთხოვნებთან და მიზნად ისახავს პერსონალური მონაცემების დამუშავების პროცესში ყველა ადამიანის უფლებებისა და თავისუფლებების დაცვას. იმის გათვალისწინებით, რომ დეკლარაციით განმტკიცებული პირადი ცხოვრების უფლება მრავალი უფლებრივი კომპონენტისგან შედგება და შესაბამისად, დაცვის სფეროსა და დაცული სუბიექტების ფართო წრეს ადგენს, დღის წესრიგში დადგა, ერთი მხრივ, უშუალოდ პერსონალურ მონაცემებზე აქცენტირებული დოკუმენტის შემუშავების საკითხი,[1] (კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ) ხოლო მეორე მხრივ, არასრულწლოვანთა პერსონალური მონაცემების განსაკუთრებულად დაცვის საჭიროების ხაზგასმა, რომელიც 1989 წლის 20 ნოემბერს გაეროს გენერალური ასამბლეის მიერ ბავშვის უფლებათა კონვენციის მიღებით განხორციელდა.

პერსონალური მონაცემების საკანონმდებლო დეფინიცია განსაზღვრულია როგორც საერთაშორისო დონეზე, (პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ კონვენციის მე-2 მუხლი) ისე ეროვნული კანონმდებლობით, (პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-2 მუხლი, აღნიშნული კანონის მიღებამდე კი საქართველოს ზოგადი ადმინისტრაციული კოდექსის 1999 წლის რედაქციის ჩანაწერი[2]) თუმცა საქართველოს კონსტიტუცია პერსონალური ინფორმაციის ცნებას არ შეიცავს. ვფიქრობ, ეს არ აკნინებს პერსონალური მონაცემების დაცვის უფლების მნიშვნელობას, ვინაიდან კონსტიტუცია წარმოადგენს ისეთ სამართლებრივ დოკუმენტს, რომელშიც გაწერილია მხოლოდ ზოგადი და ფუნდამენტური პრინციპები თუ ღირებულებები. ამასთანავე, პერსონალური მონაცემების დაცვის უფლება არ არის იზოლირებული კონსტიტუციაში რეგულირებული საკითხებისგან, რადგან ის, ერთი მხრივ, პირადი ცხოვრების ხელშეუხებლობის უფლებისგან გამომდინარეობს, რომელიც კონსტიტუციის მე-15 მუხლითაა განმტკიცებული, მეორე მხრივ, კი მჭიდრო კავშირი აქვს კონსტიტუციის მე-18 მუხლით განმტკიცებულ ინფორმაციული თვითგამორკვევის უფლებასთან, თუმცა იქიდან გამომდინარე, რომ ამ უფლებებს სხვადასხვა დანიშნულება აქვთ, ზოგიერთი სახელმწიფოს კონსტიტუცია (შვედეთი, ფინეთი, პოლონეთი და სხვა) დათქმას აკეთებს პერსონალური მონაცემების დაცვასთან დაკავშირებითაც. [3]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი არასრულწლოვან პირებთან მიმართებით სპეციალურ რეგულირებას არ ითვალისწინებს, რაც არ უნდა ჩაითვალოს მიზანშეწონილად, ვინაიდან არასრულწლოვნები საჭიროებენ განსაკუთრებულ დაცვას, რაც

[1] კ. გოშაძე „პერსონალურ მონაცემთა დაცვისა და დამუშავების კონსტიტუციურ-სამართლებრივი გარანტიები“ თბილისი, 2017 წელი, გვ 95.

[2] თ. არჩუაძე „პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე დამუშავებისას“ თბილისი 0178, საქართველო 2016 წელი. გვ. 9.

[3] კ. გოშაძე „პერსონალურ მონაცემთა დაცვის ძირითადი უფლება“ თბილისი, 2020 წელი. გვ 129-134.

გამოწვეულია, ერთი მხრივ, მათ მიერ რისკების გაუთვალისწინებლობის მაღალი ალბათობით, ხოლო, მეორე მხრივ, პერსონალური მონაცემების უკანონოდ გამოყენების შედეგების მიმართ განსაკუთრებული მგრძნობელობით. ამის გათვალისწინებით არასრულწლოვანთა პერსონალური მონაცემების დამუშავების საკითხის სპეციალური რეგულირების საჭიროება ხაზგასმულია ევროპარლამენტისა და ევროკავშირის საბჭოს მონაცემთა დაცვის ზოგად რეგულაციაში.(GDPR) ევროკავშირის მიდგომებთან ქართული კანონმდებლობის შესაბამისობაში მოყვანის მიზნით საქართველოს პარლამენტში დარეგისტრირდა საკანონმდებლო ინიციატივა, რომელიც სხვა საკითხებთან ერთად ითვალისწინებს ცვლილებების განხორციელებას არასრულწლოვნებთან მიმართებით.[4] კერძოდ კი შემოთავაზებული ცვლილება ითვალისწინებს არასრულწლოვან პირთა კატეგორიაში 2 ასაკობრივი ჯგუფის გამოყოფას. 14 წლამდე არასრულწლოვანი პირის მონაცემთა დამუშავება დასაშვებია მხოლოდ მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობის საფუძველზე, ხოლო 14 წლის ასაკს მიღწეული პირის მონაცემების დამუშავება საჭიროებს მხოლოდ არასრულწლოვნის თანხმობას. მართალია, მონაცემთა დაცვის ზოგადი რეგულაცია კანონიერი წარმომადგენლის თანხმობის აუცილებლობას ითვალისწინებს 16 წლამდე პირების მიმართ, თუმცა აღნიშნულ წესს იმპერატიული და უპირობო ხასიათი არ აქვს და გათვალისწინებულია წევრი სახელმწიფოების მიერ სხვა ასაკის განსაზღვრის შესაძლებლობა, იმ დათქმით, რომ ის არანაკლებ 13 წელი უნდა იყოს.

1. არასრულწლოვანთა მიერ ინტერნეტის გამოყენების დადებითი და უარყოფითი მხარეები

ინტერნეტი თანამედროვე საზოგადოებაში გლობალური, საინფორმაციო სივრცის შექმნის ყველაზე მოთხოვნადი საშუალებაა, განსაკუთრებით კი დღევანდელ რეალობაში, როდესაც პანდემიის გამო სოციალურმა და საგანმანათლებლო აქტივობებმა ციფრულ სამყაროში გადაინაცვლა. 18 წლამდე ასაკის პირები მსოფლიოს ინტერნეტის მომხმარებელთა დაახლოებით მესამედს შეადგენს.[5] ყოველი 3 დან 1 ბავშვი ინტერნეტმომხმარებელია. ინტერნეტით დაინტერესებული ბავშვების ასაკი დღითიდღე მცირდება არამხოლოდ საქართველოში, არამედ მთელს მსოფლიოში. თავისთავად ის ფაქტი, რომ არასრულწლოვნებს მიუწვდებათ ხელი ინტერნეტზე, უარყოფითად ვერ შეფასდება. UNICEF-ის მიერ 2017 წელს გამოქვეყნებულ ანგარიშში წერია, რომ დადგინდა კავშირი ბავშვობის ასაკში ინტერნეტით სარგებლობასა და მომავალში, ზრდასრულ ასაკში, თავის რჩენის შესაძლებლობებს შორის, რადგან ინტერნეტის გამოყენება ავითარებს ვიზუალურ-სივრცით უნარებს, რაც აისახება არასრულწლოვნის აკადემიურ შედეგებზე. ეს ინტერნეტის დემონიზების საწინააღმდეგოდ ერთ-ერთი სერიოზული არგუმენტია, თუმცა გასათვალისწინებელია ისიც, რომ არასრულწლოვნების მიერ ინტერნეტით სარგებლობა მათი პერსონალური მონაცემების ხელყოფის საფრთხეს შეიცავს. [6]

[4] „საერთაშორისო გამჭირვალობა საქართველო“-„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში დაგეგმილი ცვლილებების შეფასება.

[5] Unicef მსოფლიოს ბავშვთა მდგომარეობა, შემაჯამებელი ანგარიში 2017 წელი.

[6] არასამთავრობო ორგანიზაცია „მშობლები განათლებისთვის“ საჯარო ლექცია თემაზე „როგორ დავიცვათ ბავშვები და მოზარდები ციფრული საფრთხეებისგან?“.

2. ინტერნეტსივრცეში არასრულწლოვანი პირის მონაცემების გაზიარების გზები

პერსონალურ ინფორმაციას ზოგიერთ შემთხვევაში ადამიანები (მათ შორის არასრულწლოვანი პირებიც) თავიანთი სურვილით ხდიან სხვებისათვის ხელმისაწვდომს, თუმცა არის შემთხვევები, როდესაც ასეთი ინფორმაციის მითითება მოთხოვნილია გარკვეული მომსახურეობით სარგებლობისათვის, ვებგვერდზე რეგისტრაციისთვის ან სხვადასხვა დაწესებულებებში: მაგ კერძო თუ საჯარო სკოლებში მოსწავლეთა დასარეგისტრირებლად. დავიწყოთ ისეთი შემთხვევების განხილვით, როდესაც პერსონალური ინფორმაციის ხელმისაწვდომობის უზრუნველყოფა არასრულწლოვნის სურვილით ხდება.

2.1 არასრულწლოვნის მიერ სოციალური ქსელების მეშვეობით მონაცემების გაზიარება

საქართველოს სტატისტიკის ეროვნული სამსახურის (საქსტატი) 2020 წლის ივლისის სტატისტიკური ინფორმაციის საფუძველზე დგინდება, რომ ინტერნეტის გამოყენების ძირითადი მიზანი სოციალური ქსელებით სარგებლობაა.[7] ბავშვებისა და ახალგაზრდების ორ მესამედზე მეტს (74%) აქვს ანგარიში ზოგიერთ სოციალურ ქსელში. მიუხედავად იმისა, რომ ელექტრონული ფოსტის გამოყენება 13 წლის ასაკიდან არის შესაძლებელი, ხოლო სოციალური ქსელებისთვის ანგარიშის შექმნა კი, როგორც წესი, მოითხოვს ელექტრონული ფოსტის მისამართის მითითებას, ხშირია შემთხვევები, როდესაც არასრულწლოვნები არასწორად უთითებენ თავიანთ ასაკს და უფრო ადრეული ასაკიდან ახერხებენ ამ პლატფორმებით სარგებლობას. სოციალური ქსელების ადმინისტრატორებს არ აქვთ მექანიზმი, რომელიც სრულად გამოირიცხავს 13 წლამდე პირის დარეგისტრირების შესაძლებლობას. პერსონალური მონაცემები ყველაზე დაუცველი სოციალურ ქსელებშია, რადგან მომხმარებელი ამ დროს კარგავს კონტროლს მის მიერ გაზიარებულ ინფორმაციაზე, რაც საფრთხეს უქმნის პერსონალური მონაცემების კონფიდენციალურობას. მართალია, სოციალური ქსელების უმრავლესობა იძლევა მომხმარებლის მიერ ინფორმაციის საჯაროობის ფარგლების გაკონტროლების შესაძლებლობას, რაც გულისხმობს იმას, რომ კონფიდენციალურობის პარამეტრების გამოყენებით შესაძლებელია ინფორმაციის გაზიარება პირთა მხოლოდ ვიწრო წრისთვის, თუმცა პრობლემას ვაწყდებით არასრულწლოვან მომხმარებლებთან მიმართებით, რადგან ისინი ხშირ შემთხვევაში სათანადოდ ვერ აღიქვამენ პერსონალური მონაცემების გაზიარების შედეგებს. სოციალური ქსელების არასრულწლოვანი მომხმარებლები ხშირად ხდიან საჯაროს ისეთ პერსონალურ მონაცემებს, როგორიცაა: სახელი, გვარი, ფოტო/ვიდეო მასალა, პირადი ნომერი, საკონტაქტო ინფორმაცია, საცხოვრებელი ადგილი და სხვა.

2.2 აპლიკაცია Tik Tok-ის კონფიდენციალურობის პოლიტიკა

არასრულწლოვანთა კიბერუსაფრთხოების საკითხზე მსჯელობის განსაკუთრებული ყურადღება უნდა მიექცეს აპლიკაცია-Tik Tok-ს, რომელიც მთელს მსოფლიოში, მათ შორის საქართველოშიც, დიდი პოპულარობით სარგებლობს. თემის აქტუალობიდან გამომდინარე სახელმწიფო ინსპექტორის სამსახურმა გამოაქვეყნა პუბლიკაცია და შეაფასა აღნიშნული

[7] საქართველოს სტატისტიკის ეროვნული სამსახურის 2020 წლის ივლისის მონაცემები-მოსახლეობის განაწილება ინტერნეტის გამოყენების ძირითადი მიზნების მიხედვით.

აპლიკაციის კონფიდენციალურობის პოლიტიკა. როგორც ნაშრომშია მოცემული, მომხმარებლის საცხოვრებელი ადგილის მიხედვით აპლიკაციის კონფიდენციალურობის პოლიტიკა განსხვავებულია. Tik Tok ჩინური აპლიკაციაა, საქართველოში კი აპლიკაციის მომხმარებელი არასრულწლოვნების პერსონალური მონაცემების დაცვის ბერკეტი ნაკლებია, ვიდრე დიდ სახელმწიფოებში, მაგალითად ამერიკის შეერთებულ შტატებში, სადაც აპლიკაციის კომპანიის დაჯარიმების შემდეგ დაცვის სხვადასხვა მექანიზმები ამოქმედდა.[8]

2.3 არასრულწლოვანთა პერსონალური მონაცემების დაცულობა ვიდეოთამაშების აპლიკაციებით სარგებლობისას

არასრულწლოვნებთან მიმართებით სენსიტიური თემაა ვიდეო თამაშები, განსაკუთრებით კი ქსელური თამაშები, რომელიც მოთამაშეებს შორის კომუნიკაციის დამყარების შესაძლებლობას იძლევა. პერსონალური მონაცემების დაცულობას კი სწორედ ინტერაქციის მეშვეობით ექმნება საფრთხე. შესაძლოა, ყალბი ანგარიშით დარეგისტრირებული არაიდენტიფიცირებადი მოთამაშე არასრულწლოვანს გაეცნოს თანატოლად, მისგან გარკვეული ინფორმაცია მიიღოს და გამოიყენოს ის არასრულწლოვანი პირის ინტერესების საწინააღმდეგოდ.

3. არასრულწლოვანთა პერსონალური მონაცემების დაცულობა პანდემიის დროს

გარდა ისეთი შემთხვევებისა, როდესაც არასრულწლოვნები შედეგების გაცნობიერების გარეშე ან მათი გათვალისწინებით პერსონალურ ინფორმაციას თავად ხდიან საჯაროდ, შესაძლოა, ამგვარი ინფორმაცია ინტერნეტსივრცეში არასრულწლოვნის ნებისგან დამოუკიდებლადაც აღმოჩნდეს. ვინაიდან პერსონალური მონაცემები ფიზიკური პირის იდენტიფიკაციას ემსახურება, ის შესაძლოა მოთხოვნილ იქნეს სხვადასხვა დაწესებულების მიერ. ეს ძირითადად ეხება ობიექტურ ბუნების პერსონალურ ინფორმაციას (მაგალითად: სახელი, გვარი, პირადი ნომერი, სისხლის ჯგუფი და სხვა) და ნაკლებად სუბიექტური კატეგორიის მონაცემებს[9] (პირის შეხედულებები და შეფასებები) საგანმანათლებლო დაწესებულებებში (კერძო და საჯარო სკოლა, უმაღლესი სასწავლებლები) არასრულწლოვანთა შესახებ არაერთი პერსონალური მონაცემი გროვდება. პერსონალურ მონაცემებს შეიცავს საკლასო თუ ელექტრონული ჟურნალი, მოსწავლის პირადი საქმე, მოსწავლის რვეული, სადაც მისი შეფასებებია მოცემული,[10] თუმცა აღნიშნული მონაცემების ინტერნეტში გაზიარების საფრთხე დისტანციური სწავლების დროს უფრო მეტად იჩენს თავს. ონლაინ შეხვედრების ამსახველი ფოტო/ვიდეო მასალა პერსონალურ მონაცემებს წარმოადგენს.[11] შესაბამისად, გამოსახულების გავრცელებისას მიზანშეწონილია მასალის გამოყენებაზე იმ პირის თანხმობა იქნეს დადასტურებული, ვისი გამოსახულების გავრცელებასაც აპირებს დაწესებულება.

---

[8] სახელმწიფო ინსექტორის სამსახური-„ Tik Tok" რამდგადამენად უსაფრთხოა თქვენი საყვარელი აპლიკაცია?" გვ.3 https://personaldata.ge/ka/recommendations [უ.გ. 10.01.2021].

[9] ნ. სხირტლაძე-„პერსონალურ მონაცემთა დაცვის სამართლებრივი ასპექტები" თბილისი 2017 წელი. გვ 26.

[10] ლ. ალაფიშვილი „პერსონალური მონაცემების სახელმძღვანელო სკოლებისთვის" მშობლები განათლებისთვის, 2020 წ. გვ 5.

[11] სახელმწიფო ინსპექტორის სამსახურის განცხადება კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით https://personaldata.ge/ka/press/post/6349 [უ.გ. 11.01.2021].

დისტანციური სწავლების ამსახველი ფოტო/ვიდეო მასალის გარდა, პანდემიის პირობებში პრობლემატური გახდა არასრულწლოვნის ჯანმრთელობის შესახებ ინფორმაციის დაცვის საკითხი. ვირუსით ინფიცირებულ ან/და მათთან კონტაქტში მყოფ პირთა ვინაობის (სახელის, გვარის) საჯაროდ გავრცელება, როგორც წესი, აუცილებელი არ არის და საზოგადოებრივი ინტერესის დასაკმაყოფილებლად საკმარისია მათ შესახებ არაიდენტიფიცირებადი ფორმით ინფორმაციის გავრცელება.[12] (ასაკი, სამუშაო ადგილი, მათი გადაადგილების მარშრუტი და სხვა მონაცემები) აქედან გამომდინარე, საქართველოში პანდემიის პირობებში პაციენტების, მათ შორის არასრულწლოვანი პაციენტების, ჯანმრთელობასთან დაკავშირებული ინფორმაციის გავრცელებას მათი თანხმობის გარეშე ადგილი არ ჰქონია, თუმცა ასეთი დარღვევები გამოვლინდა სხვა სახელმწიფოებში. მაგალითად: მონტენეგროში მედიის წარმომადგენლების მიერ გავრცელდა დაინფიცირებულ პირთა ოჯახის წევრების სურათები. რუმინეთში ვირუსთან დაკავშირებულ ვებ-გვერდებზე კიბერშეტევის შემთხვევა დაფიქსირდა.[13]

4. არასრულწლოვანი პირის პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები

4.1 კიბერბულინგი

კიბერბულინგი შეიძლება გამოიწვიოს ინტერნეტში არასრულწლოვნის შესახებ სხვადასხვა სახის პერსონალური მონაცემების გავრცელებამ. გამოთქმულია შეხედულება, რომ მნიშვნელობა არ ენიჭება იმას, დარწმუნებული იყო თუ არა გამვრცელებელი პირი ინფორმაციის უტყუარობაში, ვინაიდან პერსონალურ მონაცემთა ცნება აერთიანებს სიმართლესა და საეჭვო ინფორმაციას.[14] მართალია, ბულინგი არ არის ახლადწარმოქმნილი ფენომენი და ის ყოველთვის არსებობდა ინტერნეტ (კიბერ) სივრცის მიღმა, თუმცა კიბერბულინგი გაცილებით დიდი საფრთხისშემცველია არასრულწლოვნის ფიზიკური თუ ემოციურ-ფსიქოლოგიური მდგომარეობისთვის, ვიდრე „ტრადიციული“ ბულინგი. მომეტებული რისკები რამდენიმე ფაქტორით შეიძლება აიხსნას.

- კიბერბულინგი უფრო თვალსაჩინოა, ვიდრე პირისპირ განხორციელებული ბულინგი, რადგან ინტერნეტი ბულინგისთვის გაცილებით დიდ მასშტაბს იძლევა.[15]
- კიბერბულინგის გამტარებელი პირი ვერ ხედავს ადრესატს, რაც ზრდის მისი მხრიდან საკუთარი ქმედების უწყინარ ხუმრობად აღქმის ალბათობას.
- კიბერბულინგი თან სდევს ადამიანს, მსხვერპლი ვერ პოულობს უსაფრთხო გარემოს.
- მიუხედავად მძიმე ფსიქოლოგიური მდგომარეობისა, (დეპრესია, შიში, თვითშეფასების დაკარგვა, თვითმკვლელობაზე ფიქრი და სხვა) არასრულწლოვანი

[12] ახალი უმაღლესი სასწავლებელი განცხადება „ Covid-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავება" [უ.გ. 15.02.2021].

[13] COVID-19 pandemic adversely affects digital rights in the Balkan https://edri.org/our-work/covid-19-pandemic-adversely-affects-digital-rights-in-the-balkans/ [უ.გ. 15.02.2021].

[14] ნ. სხირტლაძე. იხ. სქოლიო 9 გვ. 26.

[15] კიბერბულინგი-http://millab.ge/ka/mil-resources/any/28/any/%E1%83%99%E1%83%98%E1%83%91%E1%83%94%E1%83%A0%E1%83%98/0/ [უ.გ. 10.01.2021].

მსხვერპლები ხშირად არ უმხელენ მშობლებსა თუ სხვა ზრდასრულ პირებს კიბერბულინგის შესახებ, რადგან ეშინიათ, რომ ამის გამო ინტერნეტთან წვდომა შეეზღუდებათ.

4.2 ონლაინ თამაში-გამოწვევების (challenge) შედეგად თვითმკვლელობა/ თვითდაზიანება

განსაკუთრებით პოპულარულია თამაში „ლურჯი ვეშაპი“, რომელიც თავდაპირველად რუსეთში გამოჩნდა და შემდეგ სხვადასხვა ქვეყნებში გავრცელდა. მიუხედავად იმისა, რომ დღემდე საზოგადოების ნაწილი თამაშის არსებობასა და მოზარდების თვითმკვლელობამდე მიყვანაში მისი როლის დამადასტურებელი მტკიცებულებების სანდოობას ეჭქვეშ აყენებს, არაერთ ქვეყანაში, მათ შორის საქართველოშიც, ბევრი არასრულწლოვანი პირის თვითმკვლელობის სავარაუდო მიზეზად სწორედ ამ ტიპის თამაშები იქნა დასახელებული. ერთი შეხედვით, შესაძლოა ნაკლებად იკვეთებოდეს, ის რომ ფატალური შედეგის დადგომას მნიშვნელოვნად უწყობს ხელს არასრულწლოვანთა მიერ პერსონალური მონაცემების ინტერნეტსივრცეში გაზიარება, თუმცა გასათვალისწინებელია ის გარემოება, რომ ხშირად მოზარდები თვითმკვლელობის გადაწყვეტილებამდე მათი ოჯახის წევრისადმი მიმართული მუქარის შემდეგ მიდიან. შესაბამისად, ჩნდება კითხვა: საიდან შეიძლება ფლობდნენ თამაშის შემქმნელები მოზარდის ტელეფონის ნომერს, ინფორმაციას მათი ოჯახის წევრების ვინაობის, სამუშაო თუ საცხოვრებელი ადგილის შესახებ? ერთი ვერსიით, აღნიშნული მონაცემები სოციალურ ქსელებში არასრულწლოვნების გაზიარებული ინფორმაციის მეშვეობით არის მოპოვებული.[16] მართალია, არ არსებობს ლურჯი ვეშაპის ვებგვერდი, აპლიკაცია, ან სოციალური ქსელი, თუმცა თამაშის შემქმნელები ინფორმაციის მოსაპოვებლად უკვე არსებულ სოციალურ ქსელებს და ამ ქსელებში არასრულწლოვნების გამოქვეყნებულ ინფორმაციას იყენებენ. ამასთანავე, არსებობს მეორე ვერსიაც, რომლის თანახმადაც თამაშის დასაწყისში არასრულწლოვანს თავს წარუდგენენ უწყინარ მოთამაშეებად, ცდილობენ მეგობრული დამოკიდებულების მოპოვებას და ინტერაქციის პროცესში მისგან ნელ-ნელა იღებენ საჭირო მონაცემებს. როგორიც არ უნდა იყოს თამაშის შემქმნელთა ტაქტიკა, ფაქტი ერთია: არასრულწლოვნებს უჩნდებათ შიში, რომ მუქარა სისრულეში იქმნება მოყვანილი, რადგან დარწმუნებულები არიან, რომ მუდმივი კონტროლის ქვეშ იმყოფებიან და ორგანიზატორებმა მათ შესახებ ყველაფერი იციან. შესაბამისად, რომ არა მათ მიერ პერსონალური მონაცემების საჯაროდ გაზიარება სოციალურ ქსელში ან კომუნიკაციის დროს გაუცნობიერებლად ინფორმაციის მიწოდება მათთვის, მუქარა ნაკლებად რეალური და დამაშინებელი იქნებოდა, რაც თამაშის თვითმკვლელობით დამთავრების ალბათობას, ცხადია, შეამცირებდა.

4.3 არასრულწლოვნის ვიქტიმიზება (მსხვერპლად გახდომა)

კრიმინოლოგიაში ვიქტიმოლოგიას განიხილავენ ვიწრო და ფართო გაგებით. ვისწრო გაგება დაკავშირებულია სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაულის მსხვერპლად გახდომასთან, ხოლო ფართო გაგება სხვადასხვა საზოგადოებრივი

[16] მოკლემეტრაჟიანი ფილმი „ლურჯი ვეშაპი“ (რეჟისორი: ლ. გაბაძე).

ურთიერთობის მსხვერპლსაც მოიცავს.[17] არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარებამ ორივე ზემოთ აღნიშნული შედეგი შეიძლება გამოიწვიოს.

4.3.1 დანაშაულის მსხვერპლად გახდომა (ვიქტიმიზაცია ვიწრო გაგებით)

სისხლის სამართლის კოდექსის 157-ე მუხლით გათვალისწინებულია პასუხისმგებლობა პირადი ცხოვრების ამსახველი ინფორმაციისა და პერსონალური მონაცემების ხელყოფისთვის, თუ მან მნიშვნელოვანი ზიანი გამოიწვია. ხოლო ამავე მუხლის მე-2 ნაწილით პასუხისმგებლობის დამამძიმებელ გარემოებადაა მიჩნეული ამგვარი ინფორმაციის გავრცელება ინტერნეტით, მასობრივი მაუწყებლობის ან საჯარო გამოსვლების მეშვეობით. მართალია, აღნიშნული მუხლი პასუხისმგებლობის დამამძიმებელ გარემოებად არ ითვალისწინებს არასრულწლოვანი პირის პერსონალური მონაცემების ხელყოფას, თუმცა ეს ფაქტი შესაძლოა გათვალისწინებულ იქნას მოსამართლის მიერ სასჯელის დანიშვნისას. სასამართლო პრაქტიკაში იყო შემთხვევა, [18]როდესაც სოციალურ ქსელში დარეგისტრირებული არასრულწლოვანი პირის მიმართ ჩადენილ იქნა სსკ 157-ე მუხლის მე-2 ნაწილით გათვალისწინებული ქმედება (სხვა დანაშაულებრივ ქმედებებთან ერთად) რაც გამოიხატა არასრულწლოვანი პირის შიშველ მდგომარეობაში გადაღებული ფოტოსურათების სოციალური ქსელის საშუალებით გავრცელებაში. ეს ფოტომასალა დაზარალებულს გაგზავნილი ჰქონდა ბრალდებულისთვის პირად შეტყობინებებში. გარდა აღნიშნული დანაშაულისა, არასრულწლოვანის პერსონალური მონაცემების ინტერნეტში გაზიარება შესაძლოა გახდეს სისხლის სამართლის კოდექსის 157[1]-ე მუხლით გათვალისწინებული დანაშაულის (პირადი ცხოვრების საიდუმლოს ხელყოფა) მსხვერპლად გახდომის წინაპირობა, თუ მაგალითად ხელყოფილ იქნა განსაკუთრებული კატეგორიის პერსონალური მონაცემი- ჯანმრთელობის შესახებ ინფორმაცია, რომელიც პირად ან ოჯახურ საიდუმლოს წარმოადგენდა.

4.3.2 საზოგადოებრივი ურთიერთობის მსხვერპლი (ვიქტიმიზაცია ფართო გაგებით)

ზოგიერთი პერსონალური მონაცემის ინტერნეტში გაზიარებას შესაძლოა მოჰყვეს საზოგადოებაში არასრულწლოვანი პირის ეტიკეტირება. ეს განსაკუთრებით ეხება ნასამართლეობის შესახებ ინფორმაციას, რომელსაც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაკუთრებული კატეგორიის მონაცემებს მიაკუთვნებს. მოზარდის ეტიკეტირების შემდეგ კი წარმოიშვება საზოგადოებაში მისი ინტეგრირების პრობლემა.[19] ბულინგისგან განსხვავებით, ამ დროს შესაძლოა ადგილი არ ჰქონდეს აგრესიულ ქცევას არასრულწლოვნის მიმართ, მაგრამ საზოგადოების წევრები ინფორმაციის გავრცელების შემდეგ თავს იკავებდნენ ეტიკეტირებულ მოზარდთან მანამდე არსებული ურთიერთობის გაგრძელებაზე. არ არის გამორიცხული არასრულწლოვანს შეექმნას პრობლემები დასაქმების კუთხითაც.

[17] მ. შალიკაშვილი-„კრიმინოლოგია“ თბილისი, 2017წ გვ 191.
[18] საქართველოს უზენაესი სასამართლოს 2017 წლის 11 ოქტომბრის გადაწყვეტილება საქმეზე 2კ-227ა3.-17 .
[19] მ. შალიკაშვილი. იხ. სქოლიო 17 გვ. 45.

5. უფლების დაცვის მექანიზმები

არასრულწლოვნის პერსონალური მონაცემების კონფიდენციალურობის დარღვევისა და ინტერნეტში გავრცელების შემთხვევაში წარმოიშვება უფლების დაცვის საჭიროება. დარღვევის ხასიათის მიხედვით არასრულწლოვანს აქვს შესაძლებლობა, მიმართოს სოციალური ქსელების ადმინისტრაციას, სახელმწიფო ინსპექტორის სამსახურს ან სასამართლოს.[20] თუ სოციალურ ქსელში არასრულწლოვნის მიერ საჯაროდ გავრცელებული ფოტო სხვა პირმა ატვირთა თავის გვერდზე ან სოციალური ქსელის ჯგუფში, სანქცირების საფუძველი არ არსებობს, არასრულწლოვნისთვის უფლების დაცვა მხოლოდ სოციალური ქსელის ადმინისტრაციისთვის მიმართვისა და ფოტო-მასალის წაშლის მოთხოვნის გზით არის შესაძლებელი.

„სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-2 მუხლის თანახმად, სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ერთ-ერთი ძირითადი მიმართულება პერსონალური მონაცემების დამუშავების კანონიერების კონტროლია, შესაბამისად არასრულწლოვნის პერსონალური მონაცემების დამუშავების პროცესში წარმოშობილი დარღვევის შემთხვევაში უფლების დაცვა ამ ორგანოში განცხადების შეტანის გზით არის შესაძლებელი. სახელმწიფო ინსპექტორის სამსახურმა 2019 წელს არასრულწლოვანთა პერსონალური მონაცემების დამუშავების 13 შემთხვევა შეისწავლა, რის შედეგადაც გამოვლინდა ადმინისტრაციული სამართალდარღვევის 9 ფაქტი, ასევე შეიმუშავა რეკომენდაციები საჯარო და კერძო დაწესებულებებისთვის არასრულწლოვანთა ინტერესების დაცვის მიზნით.[21]

როგორც უკვე აღინიშნა, პერსონალური მონაცემი სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაულის საგანიცაა (სსკ 157, 157[1]) შესაბამისად, თუ პერსონალური მონაცემის დამმუშავებელი პირის/ორგანოს ქმედება დანაშაულის ნიშნებს შეიცავს, საქმე არა სახელმწიფო ინსპექტორის, არამედ საერთო სასამართლოების (სისხლის სამართლის პალატა) განსჯადია. პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილების გასაჩივრების შემთხვევაში მონაცემების დამუშავების კანონიერებას შეამოწმებს ადმინისტრაციულ საქმეთა პალატა.

გარდა საერთო სასამართლოებისა, პერსონალური მონაცემების დაცვის მიმართულებით მნიშვნელოვანი როლი აქვს საკონსტიტუციო სასამართლოს, ვინაიდან ის ამოწმებს არა მხოლოდ ნორმის შინაარსის, არამედ მისი გამოყენების პრაქტიკის კონსტიტუციურობასაც.[22] მიუხედავად იმისა, რომ საკონსტიტუციო სასამართლოს პრაქტიკა პერსონალური მონაცემების დაცვასთან დაკავშირებით მრავალფეროვანი არ არის, გადაწყვეტილებებში მაინც ვხვდებით მნიშვნელოვან განმარტებებს არასრულწლოვანი პირების პერსონალური ინფორმაციის დაცვასა და საჯარო ინფორმაციის ხელმისაწვდომობის დაბალანსების თაობაზე. მაგალითად: ერთ-ერთ გადაწყვეტილებაში საკონსტიტუციო სასამართლო აღნიშნავს,[23] რომ

---

[20] რას ნიშნავს პერსონალური მონაცემების დამუშავება? https://personaldata.ge/ka/ukanono-damushaveba [უ.გ. 09.01.2021].

[21] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში 2019 წ. გვ. 65.

[22] თ. არჩუაძე. იხ. სქოლიო 2- გვ. 47.

[23] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე №1/4/693,857 „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ. 2019 წლის 7 ივნისი, პარაგრაფი 66.

მონაცემები არასრულწლოვანი პირების შესახებ შესაძლოა მივაკუთვნოთ ისეთი კატეგორიის ინფორმაციას, რომლის კონფიდენციალობის დაცვის მომეტებულმა ინტერესმა, შესაძლოა, გადაწონოს საზოგადოების ინტერესი, რომ სასამართლოს აქტების გაცნობის გზით განახორციელოს მართლმსაჯულებაზე ზედამხედველობა, შესაბამისად არ გაიცეს სასამართლო აქტებში მოცემული პერსონალური მონაცემები სუბიექტის თანხმობის გარეშე.

დასკვნა

არასრულწლოვნის პერსონალური მონაცემების განსაკუთრებულად დაცვის საჭიროება, რომელიც ბავშვის უფლებათა კონვენციის პრეამბულაშია ხაზგასმული, არასრულწლოვნის განსაკუთრებულობიდან გამომდინარეობს. ის ფაქტი, რომ საქართველოს კანონმდებლობა პერსონალურ მონაცემების დაცვის საკითხებში არასრულწლოვნის მიმართ სპეციალურ რეგულაციებს არ ითვალისწინებს ზრდის არასრულწლოვანთა მიერ კიბერუსაფრთხოების წესების დაცვის და მონაცემების ინტერნეტსივრცეში გაზიარების მოსალოდნელი შედეგების გაცნობიერების საჭიროებას. აღნიშნულის თაობაზე არასრულწლოვანის ინფორმირება შეიძლება განხორციელდეს მშობლებისა და საგანმანათლებლო დაწესებულებებში მომუშავე პირების მიერ. ამასთანავე, მნიშვნელოვანია, პერსონალური მონაცემების დამუშავებაზე უფლებამოსილი პირები განსაკუთრებული სიფრთხილით მოეკიდონ არასრულწლოვნის პერსონალური მონაცემების დაცვის საკითხს, რათა გამოირიცხოს მათი თანხმობის გარეშე მონაცემების ინტერნეტში გავრცელება.

ბიბლიოგრაფია

1. თამთა არჩუაძე „პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე დამუშავებისას“ თბილისი 0178, საქართველო 2016 წელი;
2. კახაბერ გოშაძე „პერსონალურ მონაცემთა დაცვისა და დამუშავების კონსტიტუციურ-სამართლებრივი გარანტიები“ თბილისი, 2017 წელი;
3. ლევან ალაფიშვილი „პერსონალური მონაცემების სახელმძღვანელო სკოლებისთვის“ მშობლები განათლებისთვის, 2020 წელი;
4. მორის შალიკაშვილი „კრიმინოლოგია“ თბილისი, 2017 წელი;
5. ნუგზარ სხირტლაძე „პერსონალურ მონაცემთა დაცვის სამართლებრივი ასპექტები“ თბილისი 2017 წელი;
6. „საერთაშორისო გამჭირვალობა საქართველო“ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში დაგეგმილი ცვლილებების შეფასება. https://transparency.ge/sites/default/files/personalur_monacemta_dacvis_shesaxeb_kanonproektis_cvlilebebi_0.pdf [უკანასკნელად გადამოწმდა 05.01.2021];
7. სახელმწიფო ინსექტორის სამსახური „Tik Tok” რამდენად უსაფრთხოა თქვენი საყვარელი აპლიკაცია?“ https://personaldata.ge/ka/recommendations [უკანასკნელად გადამოწმდა 10.01.2021];
8. Unicef მსოფლიოს ბავშვთა მდგომარეობა, შემაჯამებელი ანგარიში 2017 წელი https://www.unicef.org/georgia/ka [უკანასკნელად გადამოწმდა 9.01.2021];
9. საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 7ივნისის გადაწყვეტილება საქმეზე №1/4/693,857 - „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ.
10. საქართველოს უზენაესი სასამართლოს 2017 წლის 11 ოქტომბრის გადაწყვეტილება საქმეზე 2კ-227ა3.-17 (მხარეები: აჭარის ა/რ-ის პროკურატურის უფროსი პროკურორის - ვ. თურმანიძე, ბრალდებული-დ.ფ.);
11. სახელმწიფო ინსპექტორის სამსახურის განცხადება კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით https://personaldata.ge/ka/press/post/6349-[უკანასკნელად გადამოწმდა 11.01.2021];
12. Millab-კიბერბულინგი [უკანასკნელად გადამოწმდა 10.01.202];
13. ახალი უმაღლესი სასწავლებელი განცხადება „Covid-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავება" https://newuni.edu.ge/covid-19 [უკანასკნელად გადამოწმდა 15.02.2021];
14. EDRI- COVID-19 pandemic adversely affects digital rights in the Balkans https://edri.org/our-work/covid-19-pandemic-adversely-affects-digital-rights-in-the-balkans/ [უკანასკნელად გადამოწმდა 15.02.2021];
15. საქართველოს სტატისტიკის ეროვნული სამსახურის 2020 წლის ივლისის მონაცემები
16. რას ნიშნავს პერსონალური მონაცემების დამუშავება? https://personaldata.ge/ka/ukanono-damushaveba [უკანასკნელად გადამოწმდა 09.01.2021].
17. ნორმატიული აქტები https://www.matsne.gov.ge/ [უკანასკნელად გადამოწმდა 19.02.2021]

- საქართველოს კონსტიტუცია;
- „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი;
- ადამიანის უფლებათა საყოველთაო დეკლარაცია;

- ბავშვის უფლებათა კონვენცია;
- ევროპული კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ – (CETS No.108);
- „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონი;
- საქართველოს სისხლის სამართლის კოდექსი;
- ევროპარლამენტისა და ევროკავშირის საბჭოს მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR);

Bibliography

1. Tamta Archuadze- "Guarantees of protection of personal data during processing without the consent of the person" Tbilisi 0178, Georgia 2016;
2. Kakhaber Goshadze "Constitutional-Legal Guarantees for Personal Data Protection and Processing" Tbilisi, 2017;
3. Levan Alapishvili "Personal Data Guide for Schools" Parents for Education, 2020;
4. Morris Shalikashvili - "Criminology" Tbilisi, 2017;
5. Nugzar Skhirtladze - "Legal Aspects of Personal Data Protection" Tbilisi 2017;
6. „Transparency International Georgia''-about the future changes in" law of personal information protection https://transparency.ge/sites/default/files/personalur_monacemta_dacvis_shesaxeb_kanonproektis_cvlilebebi_0.pdf [Last seen 05.01.2021];
7. State Inspector Service- "Tik Tok" -how safe is your favourite application? https://personaldata.ge/ka/recommendations [Last seen 10.01.2021];
8. Unicef World Children's Condition, Summary Report 2017;
9. Judgment of the Constitutional Court of Georgia of June 7, 2019 in the case №1 / 4 / 693,857;
10. Judgment of the Supreme Court of Georgia of October 11, 2017 in the case 2K-227 Ap.-17;
11. State Inspector Service statement about fight for personal information due corona virus https://personaldata.ge/ka/press/post/6349-[Last seen 11.01.2021];
12. Cyberbullying- [Last seen 10.01.2021];
13. New High School - Announcement - "Processing of personal data in the fight against Covid-19" https://newuni.edu.ge/covid-19 [Last seen 15.02.2021];
14. EDRI- COVID-19 pandemic adversely affects digital rights in the Balkans [Last seen 15.02.2021]
15. Data of the National Statistics Office of Georgia for July 2020;
16. State Inspector Service – „What does it mean to process personal data? " https://personaldata.ge/ka/ukanono-damushaveba_[Last seen 09.01.2021];
17. Normative Legas Acts Available at: https://www.matsne.gov.ge/ [Last seen 19.02.2021];
    - CONSTITUTION OF GEORGIA;
    - Law of Georgia on Personal Data Protection;
    - Universal Declaration of Human Rights;
    - Convention on the Rights of the Child;
    - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;
    - Law of Georgia on the State Inspector Service;

- CRIMINAL CODE OF GEORGIA ;
- General Data Protection Regulation of the European Parliament and the Council of the European Union (GDPR);

COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალურ მონაცემების დაცვა

ანა ნიჟარაძე,
ვიადრინას ევროპული უნივერსიტეტი (გერმანია)

აბსტრაქტი

Covid-19-ით ცნობილი პანდემიის დროს, მთავრობას და სხვადასხვა საჯარო თუ კერძო სექტორს უწევთ ორი პრიორიტეტის დაბალანსება - საზოგადოებრივი ჯანმრთელობის დაცვა და პირადი კონფიდენციალურობის დაცვა. ზოგიერთ ღონისძიებას, რომელიც მიზნად ისახავს ვირუსის გავრცელების შეზღუდვას და სიცოცხლის პოტენციურად გადარჩენას, შეიძლება სერიოზული გავლენა იქონიოს ადამიანის უფლებებზე. მიუხედავად იმისა, რომ ბევრი საზოგადოებრივი ჯანმრთელობის ღონისძიება შეიძლება არ საჭიროებდეს მონაცემთა შეგროვებას, სხვები შეიძლება ხელყოფდნენ იმ დაცვას, რომელიც იცავს ინდივიდების პერსონალურ მონაცემებს. აღნიშნული საკითხი დღევანდელობის აქტუალური პრობლემაა და სწორედ ამიტომაც ნაშრომში მთავარი აქცენტები და საუბარი სწორედ პაციენტის ჯანმრთელობის შესახებ ინფორმაციის კონფიდენციალურობასთან დაკავშირებულ საკითხებზე იქნება.

თავიდანვე უნდა აღინიშნოს, რომ ისეთი პერსონალური მონაცემების დამუშავება, როგორიცაა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია მნიშვნელოვანი და აუცილებელია ვირუსის გავრცელების შემცირების და მისი შედეგების შესამსუბუქებლად კონკრეტული ზომების მისაღებად. ნაშრომში საუბარი იქნება თუ ვის აქვს უფლება მოიძიოს პაციენტთა შესახებ ინფორმაცია და რა შემთხვევაშია დასაშვები მათი გაზიარება. ასევე, თუ რა ზომით შეუძლია ჯანდაცვის ან სხვა უფლებამოსილ დაწესებულებებს სხვადასხვა პერსონალური მონაცემის შეგროვება და დამუშავება ჯანდაცვის სისტემის უკეთ ფუნქციონირებისთვის. რამდენად გამამართლებელი საფუძველი შეიძლება იყოს საგანგებო მდომარეობის გამოცხადება პირის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის მოსაპოვებლად. მონაცემთა მინიმიზაცია, მიზნის შეზღუდვა, გამჭვირვალობა და კიდევ სხვა, ის ძირითადი კრიტერიუმებია, რომელიც აუცილებლად უნდა იქნეს გათვალისწინებული ამგვარი ინფორმაციის მოძიებასა და გაზიარებისას. აქვე განმარტებული იქნება ამ კონკრეტულ სფეროში ჩარევის კონკრეტული საფუძვლები, ანუ ინფიცირებულთა შესახებ ისეთი ინფორმაციის მოპოვება, რომელიც კანონთან შესაბამისობაშია და არ წარმოადგენს პირად ცხოვრებაში და პერსონალურ მონაცემების დაცვის უფლებაში ჩარევას Covid-19 პანდემიისას.

ამ კონტექსტით ყურადღება დაეთმობა დასაქმების სფეროს, რადგანაც აღნიშნული, შეიძლება ითქვას რომ ერთ-ერთი ყველაზე დაზარალებულია კორონა ვირუსით მძვინვარე პერიოდში. კონკრეტულად საუბარი იქნება თუ რამდენად, როგორ და რა დოზითაა დამსაქმებელი უფლებამოსილი შეაგროვოს დასაქმებულის შესახებ ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია შემდგომი დამუშავებისთვის და საჭიროა თუ არა ამგვარი ქმედებისთვის მისი ნების გამოხატვა. საუბარი ასევე იქნება სხვადასხვა დაწესებულებების მიერ ამგვარი ინფორმაციის მოპოვება-დამუშავებაზე, მაგალითად მედიით ამგვარი ინფორმაციის გასაჯაროების შესაძლებლობაზე.

თემის აქტუალურობიდან გამომდინარე ნაშრომში ასევე განხილული იქნება სხვა მნიშვნელოვანი საკითხები ჯანმრთელობის შესახებ პერსონალური მონაცემების დაცვასთან დაკავშირებით და ამისთვის გამოყენებულ იქნება უახლესი წყაროები.

საკვანძო სიტყვები: პირის პერსონალური მონაცემი, ჯანმრთელობის მდგომარეობის შესახებ მონაცემი, შეზღუდვის სამართლებრივი საფუძვლები, დამუშავების სამართლებრივი მასშტაბი, კოვიდ ვირუსი, საზოგადოებრივი ჯანმრთელობის დაცვა, დასაქმების სფერო, მედია

Abstract

During the Covid-19 pandemic, the government and various public and private sectors have to balance two priorities - public health and privacy. Some measures aimed at limiting the spread of the virus and potentially saving lives can have a serious impact on human rights. While many public health measures may not require data collection, others may violate the protection that protects individuals' personal data. This issue is a topical issue today and that is why the main focus of the paper and the conversation will be on issues related to the confidentiality of health information of individuals.

It should be noted at the outset that the processing of personal data such as health information is important and necessary to take specific measures to reduce the spread of the virus and mitigate its effects. The paper will discuss who has the right to seek information about health information of individuals and in what cases it is permissible to share them. As well as the extent to which health care or other authorized institutions can collect and process various personal data for the better functioning of the health care system. How justifiable can be the declaration of a state of emergency to obtain information about a person's state of health. Data minimization, goal limitation, transparency and more are the key criteria that must be considered when retrieving and sharing such information. It will also explain the specific grounds for intervening in this particular area, i.e. obtaining information about the infected that is in accordance with the law and does not constitute an interference with the right to privacy and personal data protection during the Covid-19 pandemic.

In this context, attention will be paid to the field of employment, as mentioned, it can be said that it is one of the most affected by the corona virus during the raging period. Specifically, it will be discussed to what extent and how the employer is authorized to collect information about the employee's health status for further processing and whether it is necessary to express his will for such action. There will also be mentioned about obtaining and processing such information by various institutions, for example, the possibility of publishing such information through the media.

Due to the urgency of the topic, the paper will also discuss other important issues related to the protection of personal data on health and will be based on the latest sources.

Key words: Personal Data, Personal Health Information, Legal Grounds of Restriction, Legal Scope of Processing, Covid Virus, Public Health, Employment, Media.

შესავალი

Covid-19-ის მოულოდნელმა გლობალურმა აფეთქებამ უდიდესი გამოწვევები მოუტანა მსოფლიოს და ადამიანთა ყოველდღიურ ცხოვრებას.[1] ვირუსით დაინფიცირებისგან თავის დასაცავად მხოლოდ რამდენიმე გზა არსებობს. ესაა სოციალური დისტანციის და ჰიგიენის დაცვა. ჯერჯერობით სხვა იარაღი მასთან საბრძოლველად არ არსებობს. ამ მხრივ ასევე მნიშვნელოვან საკითხს წარმოადგენს პირთა პერსონალური მონაცემების დამუშავება, რომელთა შორისაა ჯანმრთელობის შესახებ ინფორმაცია. ნაშრომის მთავარი თემაც სწორედ ესაა. თავიდანვე უნდა გაივლოს ზღვარი უსაფრთხოების ზომებს, რომელთა მიზანია საზოგადოებრივი ჯანმრთელობის დაცვა და პირთა კონფიდენციალური ინფორმაციის დაცვას შორის. ამ საკითხზე, ევროპულ დონეზე მიღებულ იქნა ევროპის მონაცემთა დაცვის საბჭოს (European Data Protection Board (EDPB)) სახელმძღვანელო მითითებები, რომლებიც ეხება პერსონალური მონაცემების შეგროვებას, გაზიარებასა და გამოყენების ფარგლებს, განსაკუთრებით კი ჯანმრთელობის მდგომარეობის შესახებ.[2] საბჭოს თავმჯომარემ, ანდრეა ჯელინეკმა განაცხადა, რომ მონაცემთა დაცვა არ წარმოადგენს ბარიერს კორონა ვირუსთან საბრძოლველად საჭირო ზომების მიღებისთვის.[3]

1. ჯანმრთელობის შესახებ ინფორმაციის დამუშავება როგორც ვირუსის შემცირების ფაქტორი

კორონა ვირუსის არსებობიდან გამომდინარე მსოფლიოს მასშტაბით წარმოიშვა ძალიან მნიშვნელოვანი საკითხი პირთა ჯანმრთელობის დაცვის სფეროში პერსონალური მონაცემის გასაჯაროებასთან დაკავშირებით, რომელსაც შესაძლოა მნიშვნელოვანი როლი ჰქონდეს ინფექციის გავრცელების თავიდან ასაცილებლად.[4] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-2 მუხლი „ბ“ პუნქტით აღნიშნულია რომ ეს მონაცემი არის განსაკუთრებული კატეგორიის მონაცემი.[5] ამავე კანონის 6-ე მუხლის 2 ნაწილის „ე“ ქვეპუნქტით კი განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ხორციელდება საზოგადოებრივი ჯანმრთელობის დაცვის მიზნებისათვის და ასევე „თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის”.
იმ პერიოდში კი, როდესაც Covid-19 მძვინვარებს, ამგვარი ინფორმაციის მოძიება-გავრცელებისას უფრო მეტი ყურადღებაა საჭირო. დღევანდელ დღეს ჯანდაცვის დაწესებულებებს უფრო დეტალურად უწევთ თითეულ ინფიცირებულ თუ რისკის ქვეშ მყოფ პირთა შესახებ პერსონალური ინფორმაციის მოძიება და დამუშავება, ვიდრე ეს სხვა დროს ხდება. ამ დროს აუცილებლად გასათვალისწინებელია ამ ინფორმაციის მოძიების მასშტაბები.

---

[1] ე. ვენტრელა, „კონფიდენციალურობა საგანგებო ვითარებაში: მონაცემთა დაცვა და კოვიდ-19 პანდემია“, 2020 წლის 28 სექტემბერი, *ერა ფორუმი*, გვ. 379-393 [უ.გ.11.01.2021].

[2] „კონფიდენციალობა და მონაცემთა დაცვა კოვიდ-19-ის დროს”, *დელოიტე*, 2020 წლის მარტი, გვ. 1-4, https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf [უ.გ. 04.01.2021].

[3] ა. ჯელინეკი, „EDPB-ის თავმჯდომარის განცხადება პერსონალური მონაცემების დამუშავების შესახებ კოვიდ-19 ეპიდემიის ფონზე“, 2020 წლის 19 მარტი, გვ. 1-2, https://edpb.europa.eu/sites/edpb/files/files/news/edpb _covid-19_20200316_press_statement_en.pdf [უ.გ. 04.01.2021].

[4] მაგალითად, ისეთი ღონისძიებების დასაგეგმად და განსახორციელებლად, რომლებსაც გადამწყვეტი მნიშვნელობა შეიძლება ჰქონდეს საზოგადოებრივი ჯანმრთელობის დაცვისთვის.

[5] ეს აღნიშნულია ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ რეკომენდაციაშიც, https://personaldata.ge/cdn/ [უ.გ. 06.01.2021].

ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემის შეგროვებას აქვს კონკრეტული მიზნები. ასეთია მაგალითად, ინფორმაცია პირთა გადაადგილების შესახებ, როგორც ქვეყნის შიგნით, ასევე მის ფარგლებს გარეთ, ამასთანავე ინფორმაცია ახლო კონტაქტში მყოფ პირთა შესახებ, სამუშაო და საცხოვრებელი ადგილის შესახებ, მათთვის სათანადო მკურნალობის გასაწევად, მკურნალობის ინდივიდუალური გეგმის შესადგენად, იზოლაციის წესების დაცვაზე კონტროლისთვის, კვლევების ჩასატარებლად და სტატისტიკის შესადგენად და სხვა ამგვარი დეტალები, რომელთა გაშიფრვა მნიშვნელოვანია ვირუსის გავრცელების შესაჩერებლად და ადამიანთა ჯანმრთელობის დასაცავად. აღსანიშნავია, რომ ამგვარი ინფორმაციის მოძიება გამომდინარეობს მნიშვნელოვანი საჭიროებიდან და არანაირად არ მოდის კანონთან წინააღმდგობაში.[6] ამგვარი ინფორმაციის მოპოვებისა და დამუშავების გარეშე უბრალოდ შეუძლებელია ჯანდაცვის სისტემის გამართულად მართვა და ფუნქციონირება. თუმცა პარალელურად მნიშვნელოვანია ადამიანის პირადი ცხოვრების პატივისცემაც.[7] ამისთვის, ჯანდაცვის სფეროში არსებული დაწესებულებები და არა მხოლოდ ისინი, ყოველთვის მოქმედი კანონმდებლობის საფუძველზე უნდა ხელმძღვანელობდნენ, რათა ზედმიწევნით დაიცვან პირთა ჯანმრთელობის შესახებ პერსონალური მონაცემების კონფიდენციალობა.[8]

2. ვის, რა შემთხვევაში და რა დოზით აქვს უფლება მოიძიოს პირთა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია

კოვიდ ვირუსმა წარმოშვა იმგვარი საკითხი, როდესაც ამისთვის უფლაბამოსილ ორგანოს უფლება აქვს საზოგადოებრივი ჯანმრთელობის დასაცავად ხელი მიუწვდებოდეს ადამიანთა ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემზე. ამდენად, ამ ვირუსის გავრცელების სიმარტივისთვის ხელის შეშლა ამგვარი ინფორმაციის მოპოვებისთვის სამართლებრივ საფუძვლად იქნა დასახელებული.

ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის მოძიების უფლება აქვთ მხოლოდ იმ დაწესებულებებს და მათი სახელით მოქმედ პირებს, რომელთაც ევალებათ ჯანმრთელობის დაცვა. ამგვარი დაწესებულებები საქართველოში დღეს ყველასთვის ნაცნობია. ესენია დაავადებათა კონტროლის ეროვნული ცენტრი, ე.წ. ინფექციური საავადმყოფო, ლაბორატორიები, უწყებები, რომლებიც საკარანტინო ზონებზე არიან პასუხისმგებელნი,[9] რა თქმა უნდა თავად ე.წ. ჯანდაცვის სამინისტრო და სხვა.[10] თავისთავად ამგვარ ინფორმაციაზე ხელი მიუწვდება თავად პაციენტებს პერსონალურად, და ასევე მათი თანხმობით ნებისმიერ პირს.[11] როგორც ვხედავთ, ნებისმიერ გარე პირს არ შეუძლია უცხო პირის შესახებ

[6]პირადი ჯანმრთელობის ინფორმაციის შეგროვებისა და გამოყენების პრინციპები, https://choicesforchange.ca/principles-for-collection-use-of-personal-health-information/ [უ.გ. 04.01.2021].

[7]რეკომენდაცია ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ.

[8]სახელმწიფო ინსპექტორის სამსახურის განცხადება კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით, https://personaldata.ge/ka/press/post/6349 [უ.გ. 04.01.2021].

[9]მაგალითად, საკარანტინო ზონად მოწყობილ სივრცეებში განთავსებულ პირთა ჯანმრთელობის მდგომარეობის შესახებ მონაცემების აღრიცხვა ძალზე მნიშვნელოვანია პირთა ჯანმრთელობის დასაცავად, კონკრეტულად კი მათთვის სამედიცინო დახმარების აღმოჩენისთვის და ვირუსის გავრცელების შესაკავებლად.

[10]მაგალითად, სამართალდამცავ ორგანოს აქვს უფლება მოითხოვოს პირთა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია. თუმცა დღევანდელი ეპიდემიის აქტუალობიდან გამომდინარე ძირითადად ზემოთ ჩამოთვლილ დაწესებულებებს უფრო აქტიურად მიუწვდებათ ხელი ამგვარ მონაცემებზე.

[11]დ. მიკელსენი, ჰ. სოლერი და მ. სტრანდელ-ჯანსონი, „კონფიდენციალურობა, უსაფრთხოება და საზოგადოებრივი ჯანმრთელობა პანდემიურ წელს", 2020 წლის 15 ივნისი, https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year [უ.გ. 04.01.2021].

ჯანმრთელობის მდგომარეობის მონაცემის მოძიება და გავრცელება ამისთვის აუცილებელი ნებართვის გარეშე. აღნიშნული არა მხოლოდ კოვიდ პანდემიის დროსაა საჭირო, არამედ მშვიდობიანობის დროსაც, რადგან ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცის ხელმისაწვდომობა და მათი გასაჯაროება თანხმობის გარეშე დაუშვებელია. ის პირის პერსონალური ინფორმაციაა და მისი უკანონო გამჟღავნება წარმოადგენს პირად ცხოვრებაში უხეშ ჩარევას.[12]

Covid-19-ით ინფიცირებულთა, შესაძლო ინფიცირებულ და ასევე, ინფიცირებულთან კონტაქტში მყოფ პირთა შესახებ ინფორმაციის მოძიება და შეგროვება დასაშვებია მხოლოდ კანონით დადგენილ ფარგლებში მხოლოდ კონკრეტული მიზნის მისაღწევად რაც შეიძლება შეზღუდული ჩარჩოებით.[13] ეს მიზანი კარგად ნაცნობია, მოსახლეობის ვირუსით ინფიცირების მაქსიმალურად ნაკლები შემთხვევის ქონა. ამგვარი ინფორმაციის მოძიება და გასაჯაროება მხოლოდ იმ მოცულობითაა დასაშვები, რომელიც აუცილებელია ვირუსის გავრცელების ფარგლების კონტროლისა და მართვისთვის.[14]

უნდა ითქვას, რომ ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია წარმოადგენს მეტად „სენსიტიურ“ ინფორმაციას, რა დროსაც მისი მოძიება-გავრცელებისას უფრო მეტი სიფრთხილეა საჭირო.[15] მაგალითად, არაერთ ქვეყანაში შეიქმნა პროგრამა,[16] რომელიც აფიქსირებს როგორც ინფიცირებულთან ახლო კონტაქტის არსებობას, ასევე აგროვებს მოქალაქეთა შესახებ ჯანმრთელობის მდგომარეობას. აღნიშნულ პროგრამას მოპოვებული აქვს ამგვარ მონაცემზე წვდომის უფლება, რაც ამასთანავე თავად პირთა თანხმობის მიცემის შემდეგ ხორციელდება. პროგრამა შეიძლება ინახავდეს ისეთ ინფორმაციას, მაგალითად როგორიცაა პირთა გადაადგილება, შესაძლო ინფიცირებულთან კონტაქტის არსებობა, ასევე პირთა შეტყობინება საფრთხის შემცველი ადგილების ვიზიტისგან თავის შესაკავებლად და სხვა. ამგვარი პროგრამები არ წარმოადგენს პირის პერსონალური ინფორმაციის უკანონო მოპოვებას, რადგან ასეთი ინფორმაციის დამუშავებას კონკრეტული მიზანი აქვს და ის სასურველი შედეგის მიღწევისთანავე ნადგურდება. ასევე მნიშვნელოვანია იმის აღნიშნვაც, რომ ყოველ კონკრეტულ შემთხვევში აუცილებელია იმ პირის ინფორმირება, რომლის პერსონალური მონაცემის დამუშავებაც მიმდინარეობს.[17]

---

[12]ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემაში (EHR) პერსონალურ მონაცემთა დაცვა, ანგარიში, 2020 წელი, http://irc.ge/new/uploads/ .pdf [უ.გ. 04.01.2021].

[13]ზ. ოკუმუს და ს. სავურან, „კოვიდ-19 და პერსონალურ მონაცემთა დაცვა“, 2020 წლის 25 სექტემბერი, გვ. 1-6, https://gun.av.tr/insights/guides/covid-19-and-personal-data-protection [უ.გ. 04.01.2021]

[14]სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები, Covid-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცმეთა დამუშავება, 2020 წელი, https://personaldata.ge/cdn/ [უ.გ. 06.01.2021].

[15]ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემაში (EHR) პერსონალურ მონაცემთა დაცვა, ანგარიში, 2020 წელი;_ჰ. ფედერმან, „ჩვენი ჯანმრთელობის მონაცემები ხელს შეუწყობს კოვიდ-19-ის შეჩერებას, მაგრამ მისი დასაცავად მკაცრი დაცვა გვჭირდება”, 2020 წლის 6 იანვარი, https://www.fastcompany.com/90510579/our-health-data-can-help-stop-covid-19-but-we-need-strong-safeguards-to-protect-it [უ.გ.12.01.2021]. ასევე, რეკომენდაცია ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ.

[16]მაგალითად, ისრაელში, ჩინეთში, რუსეთში, ტაივანში, სინგაპურში, სამხრეთ კორეაში, პოლონეთში, გერმნიაში და სხვა. დეტალურად: „კონფიდენციალობა და მონაცემთა დაცვა კოვიდ-19-ის დროს”, *დელოიტე,* 2020 წლის მარტი, გვ. 1-4.

[17]პირადი ჯანმრთელობის ინფორმაციის შეგროვებისა და გამოყენების პრინციპები; ამგვარი თანხმობის არსებობა აღიარებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონითაც.

3.საგანგებო მდგომარეობა, როგორც პირის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის მოპოვების სამართლებრივი საფუძველი

თავიდანვე უნდა აღინიშნოს, რომ პერსონალური მონაცემთა დაცვის უფლება არაა აბსოლუტური. აუცილებელია ამ უფლებაში ჩარევა იყოს კანონით გათვალისწინებული, აუცილებელი დემოკრატიულ საზოგადოებაში და წარმოადგენდეს ლეგიტიმურ საჯარო მიზანს. ადამიანთა ჯანმრთელობის დაცვა და ვირუსის მაქსიმალურად შემცირება კი ნამდვილად წარმოადგენს ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის მოძიება-გავრცელების ასეთ მიზანს, მითუმეტეს ისეთ ვითარებაში, როგორშიც დღეს მსოფლიო საზოგადოებას უწევს არსებობა.[18]

ვირუსის საქართველოში გავრცელებიდან მალევე, 2020 წლის 21 მარტს, პარლამენტის მიერ მიღებულ იქნა პრეზიდენტის ბრძანება საქართველოს ტერიტორიაზე საგანგებო მდგომარეობის გამოცხადების შესახებ, რომლის მიხედვითაც შეგვიძლია ვთქვათ, რომ ეს დოკუმენტი არანაირად არ ახდენს ადამიანის უფლებების შეზღუდვას. მიუხედავად ქვეყანაში საგანგებო მდგომარეობის არსებობისა, მიღებული კანონმდებლობა მით უფრო უფლებამოსილი დაწესებულებების მიერ პერსონალური მონაცემის, ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის უკანონო მოპოვებას და დამუშავებას, რადგანაც დღეს არსებული მდგომარეობა იძლევა ამგვარი ღონისძიებების გატარების საჭიროებას. ამ დოკუმენტის მიღება ნამდვილად წარმოადგენდა მოსახლეობის კეთიდღეობისთვის აუცილებელ და გადაუდებელ საშუალებას.[19] ამდენად, ამგვარი გლობალური პრობლემები, რომელთაც სრულიად შეუძლია ადამიანთა ცხოვრების შეცვლა, და ამ პრობლემათა აღმოსაფხვრელად მიღებული თუ გასატარებელი ღონისძიებები, ვერ უშლის ხელს პირთა ჯანმრთელობს მდგომარეობის შესახებ ინფორმაციის დამუშავებას.[20]

4.დასაქმების სფერო და მედია

კორონა ვირუსის ფონზე დამსაქმებლები ცდილობენ უწყვეტად განაგრძონ საქმიანობა, რისთვისაც აუცილებელია თანამშრომელთა შორის ჯანმრთელობისთვის უსაფრთხო გარემოს არსებობა. მნიშვნელოვანია როგორც საჯარო, ასევე კერძო დამსაქმებლებმა იცოდნენ აქვთ თუ არა უფლება მოიძიონ მათი დასაქმებულების ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია და თუ კი, რამდენად დეტალურად, იმის გათვალისწინებით, რომ ასეთი ინფორმაცია შეიძლება ძალიან პერსონალური მონაცემის შემცველი იყოს. აქვე გასათვალისწინებელია ისიც, თუ რამდენად შედის დამსაქმებელი ამგვარი ინფორმაციის მოძიების უფლებამოსილ დაწესებულებად და საჭიროა თუ არა ამ ინფორმაციის მოსაძიებლად პირის ნების არსებობა.[21]

ზოგადად დამსაქმებელს არ აქვს უფლება მოიძიოს მისი თანამშრომლის ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემი. თუმცა არის გამონაკლისი, რაც

---

[18]ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემაში (EHR) პერსონალურ მონაცემთა დაცვა, ანგარიში, 2020 წელი; ა. ჯელინეკი, „EDPB-ის თავმჯდომარის განცხადება პერსონალური მონაცემების დამუშავების შესახებ კოვიდ-19 ეპიდემიის ფონზე“, 2020 წლის 19 მარტი, გვ. 1-2.

[19]იქვე; განცხადება პარლამენტის მიერ საგანგებო მდგომარეობის გამოცხადების შესახებ საქართველოს პრეზიდენტის ბრძანების დამტკიცების შესახებ, http://www.parliament.ge/ge/saparlamento-saqmianoba/plenaruli-sxdomebi/plenaruli-sxdomebi_news/parlamentma-sagangebo-mdgomareobis-gamocxadebis-shesaxeb-saqartvelos-prezidentis-brdzaneba-daamtkica.page [უ.გ. 12.01.2021].

[20]სახელმწიფო ინსპექტორის სამსახურის განცხადება კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით, 2020 წლის 20 მარტი.

[21]ბ. ოკუმუს და ს. სავურან, „კოვიდ-19 და პერსონალურ მონაცემთა დაცვა“, 2020 წლის 25 სექტემბერი, გვ. 1-6.

საზოგადოებრივი ინტერესების დაცვას ეხება. იმის გათვალისწინებით, რომ კოვიდ პანდემიისას პირთა შესახებ ხდება გარკვეული მნიშვნელობის საკითხების მოძიება, რომლებიც აიოლებს ინფიცირებულთა ჯაჭვის განსაზღვრას, დამსაქმებლებს ამ შემთხვევაში უფლება აქვთ შეაგროვონ ინფორმაცია მათი თანამშრომლების ჯანმრთელობის მდგომარეობის შესახებ, რისი დამუშავებაც უზრუნველყოფს უსაფრთხო სამუშაო გარემოს შექმნას.[22] ნებისმიერ შემთხვევაში დამსაქმებელი ვალდებულია ყოველი პერსონალური მონაცემი დაამუშაოს კანონიერად, გამჭირვალედ და მხოლოდ წინასწარ განსაზღვრული, მკაფიო და ლეგიტიმური მიზნებისთვის, მხოლოდ იმ დოზით რაც საჭირო იქნება კონკრეტული მიზნის მისაღწევად.[23] პირთა ამგვარი ინფორმაცია აუცილებლად კონფიდენციალურად უნდა იქნეს შენახული. ამასთანავე, თავისთავად დასაქმებულებსაც აქვთ სამოქალაქო ვალდებულება იზრუნონ გარშემო მყოფებზე და ვირუსისთვის დამახასიათებელი ნებისმიერი სიმპტომის აღმოჩენისას ან მაგალითად ვირუსის დაინფიცირებულთა მაღალი რისკის ქვეყანაში მოგზაურობის შემდეგ[24] მიიღოს იმგვარი ზომები, რომლებიც დაიცავს სხვათა ჯანმრთელობას. ხოლო რაც შეეხება ასეთი ინფორმაციის შეგროვებაზე პირის თანხმობას, აღნიშნული დასაშვებია ასეთი ნების გამოხატვის გარეშე თუ რა თქმა უნდა მისი შეგროვების მიზანია სამუშაო ადგილზე უსაფრთხოების შენარჩუნება და თანამშრომელთა ჯანმრთელობის დაცვა. ნებისმიერ შემთხვევაში კი აუცილებელია პირს ეცნობოს მისი პერსონალური მონაცემის დამუშავების შესახებ.[25] ხოლო მას შემდეგ რაც მიზანი მიღწეულ იქნება, პირის პერსონალური მონაცემი აუცილებლად უნდა განადგურდეს.[26]

დღევანდელ რთულ პერიოდში, მედიას აქტიური როლი აქვს ვირუსთან დაკავშირებით მოსახლეობის ინფორმირებაზე. მათი ძირითადი კვლევის ობიექტი სამედიცინო დაწესებულებებია, რომლებიც პანდემიის წინააღმდეგ პირველ ხაზზე იბრძვიან. ამიტომაც მედიას თითქმის არაფერი გამორჩება, ისინი ხალხისთვის მთავარ საინფორმაციო წყაროს წარმოადგენენ. სწორედ ამ დროს მართებს მედიას დიდი ყურადღება. უნდა ითქვას, რომ „პერსონალურ მონაცემთა დაცის შესახებ“ საქართველოს კანონი არ მოიცავს დებულებებს მედიასაშუალებების მიერ პირთა პერსონალურ მონაცემთა დამუშავებაზე.[27] თუ დავუკვირდებით, საქართველოში ვირუსით გავრცელების შესახებ უახლოეს სიახლეების გადმოცემისას, პირთა ინფიცირების შესახებ ინფორმაციის გავრცელება მხოლოდ რაიმე არაიდენტიფიცირებადი ნიშნის მიხედვით ხდება. მაგალითად, ასაკობრივი ჯგუფის, თანმდევი დაავადების, სამუშაო ადგილის, გადაადგილების მარშრუტის, და სხვა ამგვარი. შესაბამისად თუ არ არსებობს საჯარო ინტერესი, როგორიც მაგალითად შეიძლება იყოს პირის ცნობადობა, ჩვენ ვერ შევხვდებით ისეთ ინფორმაციას, რომელშიც პირი სახელი და გვარით, პირადი ნომრით ან სხვა პირადი მონაცემითაა იდენტიფიცირებული.

---

[22]სახელმწიფო ინსპექტორის სამსახურის განცხადება კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით, 2020 წლის 20 მარტი.

[23]ზ. ოკუმუს და ს. სავურან, „კოვიდ-19 და პერსონალურ მონაცემთა დაცვა“, 2020 წლის 25 სექტემბერი, გვ. 1-6.

[24]მოგზაურობის ისტორიაც პირის პერსონალურ ინორმაციას განეკუთვნება, თუმცა მისი გასაჯაროება მნიშვნელოვანი და აუცილებელია ვირუსის მართვისთვის.

[25]ზ. ოკუმუს და ს. სავურან, „კოვიდ-19 და პერსონალურ მონაცემთა დაცვა“, 2020 წლის 25 სექტემბერი, გვ. 1-6

[26]სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები, Covid-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცმეთა დამუშავება.

[27]ძირითადად ხშირია შემთხვევები, როდესაც თავად სამედიცინო პერსონალი ასაჯაროებს პირის ჯანმრთელობის შესახებ მონაცემებს, რაც რეგულირდება ზემოთ აღნიშნული კანონით.

დასკვნა

როგორც ვხედავთ, პირთა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის მოძიებას და დამუშავებას მნიშვნელოვანი გავლენა შეუძლია იქონიოს ვირუსის გავრცელების თავიდან ასაცილებლად და მოსახლეობის ჯანმრთელობის დასაცავად. სწორედ ამიტომ, კანონმდებლობა დასაშვებად აცხადებს ამგვარი პერსონალური მონაცემის გამჟღავნების საგამონაკლისო შემთხვევას. პირის პერსონალური მონაცემების დაცვა „არ უნდა იქცეს ჯანდაცვის სისტემის ფუნქციონირებისთვის დაბრკოლებად“.[28] ყველა შემთხვევაში აუცილებელია, ამგვარი ინფორმაციის შეგროვება-დამუშავება-გავრცელება მკაცრად შეიზღუდოს მონაცემთა მინიმიზაციის, მიზნის შეზღუდვის, გამჭვირვალობისა და მონაცემთა დაცვის პრინციპების შესაბამისად. ხოლო მას შემდეგ რაც დასახული მიზანი მიღწეულ იქნება, იგი უნდა განადგურდეს.[29] ქვეყანაში დღეს არსებული ყოველივე რეგულაცია კი მიმართულია ადამიანთა კეთილდღეობისა და ცხოვრების ჩვეულ რიტმში დასაბრუნებლად და მისასალმებელია ის, რომ ჩვენს ქვეყანაში ვირუსით ინფიცირებულ პირთა შესახებ პერსონალური მონაცემები დაცულია უკანონო გასაჯაროებისგან.

[28]რეკომენდაცია ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ.

[29]დ. მიკელსენი, ჰ. სოლერი და მ. სტრანდელ-ჯანსონი, „კონფიდენციალურობა, უსაფრთხოება და საზოგადოებრივი ჯანმრთელობა პანდემიურ წელს”.

ბიბლიოგრაფია

1. „კონფიდენციალობა და მონაცემთა დაცვა კოვიდ-19-ის დროს", *დელოიტე,* 2020 წლის მარტი, გვ. 1-4, https://www2.deloitte.com/content/dam/Deloitte/be/Documents /risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf [უკანასკნელად გადამოწმდა 04.01.2021];
2. FindLaw Attorney Writers, 2016 წლის 26 ივლისი, https://corporate.findlaw.com/litigation-disputes/the-confidentiality-of-personal-health-information-in-the.html[უკანასკნელად გადამოწმდა 04.01.2021];
3. Principles for Collection and Use of Personal Health Information, https://choicesforchange.ca/principles-for-collection-use-of-personal-health-information/ [უკანასკნელად გადამოწმდა 04.01.2021];
4. ანდრეა ჯელინეკი, „EDPB-ის თავმჯდომარის განცხადება პერსონალური მონაცემების დამუშავების შესახებ კოვიდ-19 ეპიდემიის ფონზე", 2020 წლის 19 მარტი, გვ. 1-2, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_covid19_20200316_press_statement_en.pdf [უკანასკნელად გადამოწმდა 04.01.2021];
5. ბეგუმ იავუზდოგან ოკუმუს და სელინ ბასარან სავურან, „„კოვიდ-19 და პერსონალურ მონაცემთა დაცვა",", 2020 წლის 25 სექტემბერი, გვ. 1-6, https://gun.av.tr/insights/guides/covid-19-and-personal-data-protection [უკანასკნელად გადამოწმდა 04.01.2021];
6. განცხადება პარლამენტის მიერ საგანგებო მდგომარეობის გამოცხადების შესახებ საქართველოს პრეზიდენტის ბრძანების დამტკიცების შესახებ, 2020 წლის 21 მარტი, ინტერნეტ წყარო [უკანასკნელად გადამოწმდა 12.01.2021];
7. დანიელ მიკელსენი, ჰენინგ სოლერი და მალინ სტრანდელ-ჯანსონი, „კონფიდენციალურობა, უსაფრთხოება და საზოგადოებრივი ჯანმრთელობა პანდემიურ წელს", 2020 წლის 15 ივნისი, https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year [უკანასკნელად გადამოწმდა 04.01.2021];
8. ემანუელე ვენტრელა, „კონფიდენციალურობა საგანგებო ვითარებაში: მონაცემთა დაცვა და კოვიდ-19 პანდემია", 2020 წლის 28 სექტემბერი, *ერა ფორუმი,* გვ. 379-393, https://link.springer.com/article/10.1007/s12027-020-00629-3 [უკანასკნელად გადამოწმდა 11.01.2021];
9. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი;
10. რეკომენდაცია ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ, ინტერნეტ წყარო [უკანასკნელად გადამოწმდა 06.01.2021];
11. სეილი სუდერ, „თანამშრომელთა პირადი მონაცემების დამუშავება კოვიდ -19 პანდემიის დროს", შრომის სამართლის ევროპული ჟურნალი, 2020, გვ. 1-16, https://journals.sagepub.com/doi/pdf/10.1177/2031952520978994 [უკანასკნელად გადამოწმდა 04.01.2021];
12. სახელმწიფო ინსპექტორის სამსახურის განცხადება კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით, 2020 წლის 20 მარტი, https://personaldata.ge/ka/press/post/6349 [უკანასკნელად გადამოწმდა 04.01.2021];
13. სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები, Covid-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცმეთა დამუშავება, 2020 წელი, ინტერნეტ წყარო, [უკანასკნელად გადამოწმდა 06.01.2021];

14. ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემაში (EHR) პერსონალურ მონაცემთა დაცვა, ანგარიში, 2020 წელი, http://irc.ge/new/uploads/.pdf [უკანასკნელად გადამოწმდა 04.01.2021];
15. ჰიათერ ფედერმან, „ჩვენი ჯანმრთელობის მონაცემები ხელს შეუწყობს კოვიდ-19-ის შეჩერებას, მაგრამ მისი დასაცავად მკაცრი დაცვა გვჭირდება", 2020 წლის 6 იანვარი, ინტერნეტ წყარო, [უკანასკნელად გადამოწმდა 12.01.2021].

Bibliography

1. „Privacy and Data Protection in the age of COVID-19", *Deloitte,* March 2020, pg. 1-4, https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf [last visited 04.01.2021];
2. FindLaw Attorney Writers, July 26, 2016, https://corporate.findlaw.com/litigation-disputes/the-confidentiality-of-personal-health-information-in-the.html [last visited 04.01.2021];
3. Principles of collecting and using personal health information, https://choicesforchange.ca/principles-for-collection-use-of-personal-health-information/ [last visited 04.01.2021];
4. Andrea Jelinek, „Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak", 19 March, 2020, pg. 1-2, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_covid-19_20200316_press_statement en.pdf [last visited 04.01.2021];
5. Begüm Yavuzdoğan Okumuş and Selin Başaran Savuran, „COVID-19 and Personal Data Protection", 25 September, 2020, pg.1-6, https://gun.av.tr/insights/guides/covid-19-and-personal-data-protection [last visited 04.01.2021];
6. Statement on the Approval of the Decree of the President of Georgia on the Declaration of the State of Emergency by the Parliament, March 21, 2020, http://www.parliament.ge/ge/saparlamento-saqmianoba/plenaruli-sxdomebi/plenaruli-sxdomebi_news/parlamentma-sagangebo-mdgomareobis-gamocxadebis-shesaxeb-saqartvelos-prezidentis-brdzaneba-daamtkica.page [last visited 12.01.2021];
7. Daniel Mikkelsen, Henning Soller, and Malin Strandell-Jansson, „Privacy, security, and public health in a pandemic year", 15 June, 2020, https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year [last visited 04.01.2021];
8. Emanuele. Ventrella, „Privacy in emergency circumstances: data protection and the COVID-19 pandemic", *ERA Forum*, 28 September, 2020, pg. 379-393, https://link.springer.com/article/10.1007/s12027-020-00629-3 [last visited 11.01.2021];
9. Law of Georgia on Personal Data Protection;
10. Recommendation on personal data processing in the field of healthcare, https://personaldata.ge/cdn/2018/12 [last visited 06.01.2021];
11. Seili. Suder, „Processing employees' personal data during the Covid-19 pandemic", *European Labour Law Journal,* 2020, 1-16, https://journals.sagepub.com/ [last visited 04.01.2021];
12. Statement by the Office of the State Inspector General regarding the protection of personal data in the fight against coronavirus, 20 March, 2020, https://personaldata.ge/ka/press/post/6349 [last visited 04.01.2021];

13. Recommendations of the State Inspector's Office, processing of personal data in the fight against Covid-19, 2020, https://personaldata.ge/cdn/2020/04/COVID-19 [last visited 06.01.2021];
14. Protection of personal data in the Electronic Health Record System (EHR), report, 2020, http://irc.ge/new/uploads/.pdf [last visited 04.01.2021];
15. Heather. Federman, „Our health data can help stop COVID-19—but we need strong safeguards to protect it", 6 January, 2020, https://www.fastcompany.com/90510579/our-health-data-can-help-stop-covid-19-but-we-need-strong-safeguards-to-protect-it?fbclid=IwAR3ttc5rcFfYQHd3SfIuYr9e5Z10RroMwtsgWuSzqIkCOYG9pq3_nr0t2Yk [last visited 12.01.2021.

COVID-19-ის გავლენა მონაცემთა უსაფრთხოებაზე

მარიამ გიორგაძე,
თბილისის სახელმწიფო უნივერსიტეტი

აბსტრაქტი

2020 წელს კოვიდ-19-ის ფართომასშტაბიანმა აფეთქებამ რადიკალური ცვლილებების აუცილებლობა გამოიწვია-მრავალი გამოწვევების წინაშე დადგა ყველა ქვეყნის ჯანდაცვის სისტემა, მასშტაბური შეზღუდვები მიადგა ადამიანის ძირითად უფლებებსა და თავისუფლებებს, პირის პერსონალურ მონაცემებს. სახელმწიფოები იყენებენ ისეთ ზომებს,რომელიც ჩვეულებრივ პირობებში აკრძალული იქნებოდა და ფუნდამენტურ უფლებებში დაუშვებელ ჩარევად შეფასდებოდა, მაგრამ საქართველოს, ასევე საერთაშორისო კანონმდებლობა ისეთი ლეგიტიმური მიზნებისათვის,როგორიცაა საზოგადოებისა და სახელმწიფოს უსაფრთხოება, დასაშვებად მიიჩნევს ამ ჩარევას. სახელმწიფოებს დასჭირდათ სწრაფი რეაგირება,რათა თავიდან აეცილებინათ ვირუსის შემდგომი გავრცელება, სწორედ ამ მიზნისათვის საზოგადოებას მოუწია ბევრ „დათმობაზე“ წასვლა. პანდემიასთან ბრძოლაში საჭირო გახდა კერძო სექტორების ჩართვაც და სახელმწიფოს რეკომენდაციების საფუძველზე უამრავ სფეროში მოგვიწია ისეთი საშუალებების გამოყენება, რითიც შესაძლოა საფრთხე მიადგეს პირის პერსონალურ მონაცემებს (როგორც პირის ჩვეულებრივ, ასევე განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს). დღესდღეობით ტექნოლოგიების განვითარებასთან ერთად უფრო ხშირდება სხვადასხვა სახის კიბერდანაშაულები, ამის გათვალისწინებით ის ფაქტორი, რომ პანდემიის პირობებში იძულებულები გავხდით გამოგვეყენებინა სხვადასხვა სახის ელექტრონული მოწყობილობა და გზები, ასევე კერძო თუ საჯარო სექტორის უმეტესობას მოუწია დისტანციურ რეჟიმზე გადასვლა, დიდ საფრთხეს წარმოადგენს პერსონალური მონაცემებისათვის და შესაბამისად მათი დაცვის გარანტირებისთვისაც მეტი ძალისხმევაა საჭირო.

საყურადღებოა რომ მაღალი საჯარო ინტერესიდან გამომდინარე,ხდება საზოგადოების ინფორმირება დაავადებულთა შესახებ, ასევე წყაროების კვლევა, თუმცა ამ დროს შეიძლება ზიანი მიადგეს მონაცემთა სუბიექტის ინტერესსაც და პრაქტიკიდან როგორც ჩანს,დისკრიმინაციის ობიექტიც კი გახდეს. ამიტომ მნიშვნელოვანია დავიცვათ ბალანსი საჯარო ინტერესსა და სუბიექტის უფლებებს შორის. ასე რომ, საჭიროა ვიმსჯელოთ არა პერსონალური მონაცემების დამუშავების დასაშვებობაზე, არამედ იმაზე თუ როგორ უნდა განხორციელდეს აღნიშნული ქმედებები, როგორც სახელმწიფოს, ასევე ორგანიზაციებისა და კომპანიების მხრიდან.

კვლევის მიზანია დავადგინოთ თუ პრაქტიკაში რა საშუალებები გამოიყენება კოვიდ-19-თან ბრძოლისათვის, რაც ყველაზე მნიშვნელოვანია რა გავლენა აქვს ამ უკანასკნელს პირის პერსონალური მონაცემების უსაფრთხოებაზე,რამდენად გამჭირვალეა მონაცემთა სუბიექტისთვის თავისი მონაცემების დამუშავების შესახებ ინფორმაცია. გამოვიკვლიოთ თუ რა პრაქტიკა გვაქვს პანდემიის პერიოდში მონაცემთა დაცვასთან დაკავშირებით და რა გამოწვევების წინაშე მოგვიწევს დადგომა მის შემდეგ.

საკვანძო სიტყვები: კოვიდ-19, პანდემია, პერსონალური მონაცემები, მონაცემთა დაცვის უსაფრთხოება.

Abstract

The large-scale explosion of Covid-19 in 2020 required radical changes-many challenges were faced by the health systems of all countries, mass restrictions on fundamental human rights and freedoms. States use measures that would normally be prohibited and would be considered unacceptable interference with fundamental rights. Georgian, as well as international law, permits such interference for legitimate purposes such as public and state security. Statesneeded to respond quickly to prevent the virus from spreading further, for which the public had to make many „compromises “.

In the fight against the pandemic, it became necessary to involve the private sector, and based on the recommendations of the government, we had to use methods that could endanger a person's personal data (both ordinary and special categories of personal data) in many areas.

With the development of technology, various types of cybercrime are becoming more frequent, taking into account the fact that in the pandemic we were forced to use different types of electronic devices, furthermore most private or public sector had to switch to distance mode of working, hence more effort is needed for protecting data privacy.

It is noteworthy that due to the high public interest, the public is informed about the patients, but that may be detrimental to the interest of the data subject and in practice he/she may even become an object of discrimination. It is therefore important to maintain a balance between the public interest and the rights of the subject.

During pandemic it’s crucial to consider not the permissibility of personal data processing, but how the actions in honor of protecting humans‘ lives should be carried out by the state, as well as by organizations and companies. The aim of the study is to determine what tools are used to cope with Covid-19 in practice, most importantly what impact the latter has on the data privacy and security, also about transpearecy of these whole process for data subjects. Analyze data privacy and protection issues during the pandemic and the aftermath when Covid-19 is over.

Key words: covid-19, pandemic, personal data, data privacy and security.

შესავალი

ადამიანის პერსონალური მონაცემების დაცვა მისი ერთ-ერთი უმნიშვნელოვანესი უფლებაა. სამართლის აღნიშნული დარგი დრო და დრო უფრო მეტ პოპულარობას ჰპოვებს და განსაკუთრებით აქტუალური ხდება ბოლო პერიოდში განვითარებული მოვლენების ფონზე.2020 წელს მსოფლიოს თავს დაატყდა ახალი გამოწვევა Sars–Cov-2-ის[1] სახით. აღნიშნული ვირუსი უჩვეულო სისწრაფით მოედო ქვეყნების დიდ ნაწილს, რასაც შესაბამისი დროული რეაგირება მოჰყვა ჯანდაცვის საერთაშორისო ორგანიზაციისა და მათი მხრიდან.

პანდემიამ დიდი გავლენა იქონია სახელმწიფოების ჯანდაცვის სისტემაზე, სოციალურ სფეროსა და ეკონომიკურ სტაბილურობაზე. აღმოჩნდა, რომ სულ რამდენიმე თვის შემდეგ ჩამოყალიბდა ახალი დღის წესრიგი, რომლის ფარგლებშიც მთავარ მიზანს წარმოადგენდა მოსახლეობის ჯანმრთელობისა და სიცოცხლის დაცვა. იმისათვის, რომ რაც შეიძლება სწრაფად შეეჩერებინათ Covid-19-ის შემდგომი გავრცელება და ასევე დაემარცხებინათ იგი,საჭირო გახდა პანდემიასთან ბრძოლის პროგრამის ფარგლებში ბევრი ისეთი ზომის მიღება,რითიც შეიზღუდებოდა ადამიანის ძირითადი უფლებები და თავისუფლებები. ჩვეულებრივ მდგომარეობაში სახელმწიფოს მხრიდან მსგავსი ქმედებების განხორციელება ან უფლებებში ამგვარი ჩარევა

[1] მსოფლიოში ცნობილი, როგორც კოვიდ-19.

იქნებოდა დაუშვებელი და წარმოუდგენელიც კი დემოკრატიულ საზოგადოებაში. პანდემიის შესაკავებლად ბევრი ისეთი მეთოდოლოგია და ტექნოლოგიის გამოყენება გახდა საჭირო, რომლის მეშვეობითაც თითოეული ჩვენგანის პერსონალური მონაცემების დამუშავება ხდება, შესაბამისად ყოველივე ეს დიდ გავლენას იქონიებს პირის პერსონალური მონაცემების უსაფრთხოებაზე.

კვლევის მიზანია ვნახოთ თუ რა მდგომარეობა გვაქვს პერსონალურ მონაცემთა დაცვასთან მიმართებით Covid-19-ის პირობებში, ამისათვის გამოვიკვლიეთ თუ რა გზით ებრძვის მსოფლიო ვირუსს და რა გავლენა აქვს ამ ყველაფერს ინდივიდთა მონაცემების უსაფრთხოებაზე ამ პერიოდში, არის თუ არა დასაშვები ჩვენი მონაცემების დამუშავება ჩვენი თანხმობის გარეშე, რის საფუძველზე. ასევე პანდემიის პირობებში მონაცემთა დამუშავებისას, როგორ შეიძლება იყოს უზრუნველყოფილი მათი უსაფრთხოება და რაც არანაკლებ მნიშვნელოვანია რა გავლენა შეიძლება იქონიოს ამ დონის მასშტაბურმა მონაცემთა დამუშავებამ პანდემიის შემდგომ პერიოდზე.

1.პერსონალური მონაცემი და Covid-19-ის პირობებში მათი დამუშავება.

ადამიანის პერსონალური მონაცემები არ არის აბსოლუტური უფლება და შესაბამისად როგორც საერთაშორისო აქტები, ისეთი როგორიცაა ევროპის საბჭოს 108-ე კონვენცია[2], GDPR[3], ასევე საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, ითვალისწინებენ შემთხვევებს, როდესაც დასაშვებია კანონიერი საფუძვლის არსებობისას პირის ამ უფლებების გარკვეულწილად შეზღუდვა. თუმცა გასათვალისწინებელი, რომ მონაცემები უნდა დამუშავდეს ამ სფეროში დამკვიდრებული პრინციპების დაცვით.

სანამ უშუალოდ გადავიდოდით იმ გზების განხილვაზე, რომელიც სხვადასხვა სახელმწიფოებმა გამოიყენეს ვირუსთან საბრძოლველად და ასევე რა გავლენა იქონიეს მათ მონაცემთა უსაფრთხოებაზე, ჩემი აზრით, მნიშვნელოვანია პირველ რიგში განვიხილოთ, თუ რის საფუძველზე შეიძლება პანდემიის პირობებში ჩვენი პერსონალური მონაცემების დამუშავება (რაც რაღა თქმა უნდა ყოველთვის გარკვეულ საფრთხეს წარმოადგენს ჩვენი აღნიშნული უფლებისათვის).

პირველ რიგში, განვსაზღვროთ რა არის ადამიანის პერსონალური მონაცემი-„ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით“ [4]შესაბამისად ჩვენი კანონმდებლობით იმისათვის, რომ ინფორმაცია ჩაითვალოს პერსონალურ მონაცემად, საკმარისია აღნიშნული ინფორმაცია რაიმე სახით პირდაპირ თუ არაპირდაპირ მისი იდენტიფიცირების, ინდივიდუალიზაციის შესაძლებლობას გვაძლევდეს. ეს არ უნდა მოითხოვდეს არაგონივრულ დროს,რესურსებსა და ძალისხმევას, რაც ყოველ კონკრეტულ შემთხვევაში ინდივიდუალურად უნდა შეფასდეს.

---

[2] European Treaty Series-No.108.Convention for the Protection of Individuals with regard to Automatic.Processing of Personal Data.Strasbourg,28.I.1981.

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,and repealing Directive 95/46/EC (General Data Protection Regulation).

[4] მუხლი 2 ა, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ.28/12/2011

„მხედველობაში უნდა იქნეს მიღებული ყველა ობიექტური ფაქტორი, როგორიცაა იდენტიფიცირებისათვის საჭირო ხარჯები და დრო, მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიები და ტექნოლოგიის განვითარება.“[5] შესაბამისად მონაცემთა დაცვას არ ექვემდებარება ანონიმური მონაცემი, რომლის მეშვეობითაც პირის ამოცნობა ზემოთ აღნიშნული არაგონივრული ძალისხმევისა და რესურსების გარეშე შეუძლებელი იქნება, თუმცა ექვემდებარება ფსევდონიმიზირებული ინფორმაცია, რომელიც შეიძლება სხვა მონაცემთა ერთობლიობაში საშუალებას გვაძლევდეს პირის იდეტიფიცირებისათვის.

საქართველოს კანონმდებლობა განარჩევს „ჩვეულებრივ“ პერსონალურ მონაცემებს და განსაკუთრებული კატეგორიის მონაცემებს. ასეთია-„მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული ორგანიზაციის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან ან ნასამართლობასთან, ასევე ბიომეტრული მონაცემი, რომლითაც შესაძლებელია პირის იდენტიფიცირება ზემოაღნიშნული ნიშნებით“

ზემოთ აღნიშნული „ერსონალური მონაცემები, რომლებიც მათი ბუნებიდან გამომდინარე, განსაკუთრებულად მგრძნობიარეა ფუნდამენტურ უფლებებთან და თავისუფლებებთან მიმართებაში, საჭიროებს განსაკუთრებულ დაცვას,რადგან მათი დამუშავების კონტექსტი შეიძლება მნიშვნელოვანი რისკის ქვეშ აყენებდეს ფუნდამენტურ უფლებებსა და თავისუფლებებს.“[6]

სწორედ მონაცემთა „სენსიტიურობიდან“ გამომდინარე მათი დამუშავების საფუძვლებიც განსხვავებულია.მონაცემთა დამუშავების საფუძვლები მოცემულია საქართველოს პერსონალურ მონაცემთა დაცვის შესახებ კანონის მეხუთე და მეექვსე მუხლებში.

დღევანდელობაში ჯანმრთელობისა და სიცოცხლის მიმართ არსებული გადამეტებული საფრთხიდან გამომდინარე მსოფლიოს მასშტაბით მუშავდება ორივე კატეგორიის მონაცემები, თუმცა ძირითადი საფრთხე, ვფიქრობ, მაინც განსაკუთრებული კატეგორიის მონაცემებს ადგება, სწორედ, მათი ბუნებიდან გამომდინარე.

პანდემიის პირობებში მონაცემთა დამუშავება შეიძლება გამომდინარეობდეს პირის თანხმობიდან ან არსებობდეს შესაბამისი კანონიერი საფუძველი, როგორიცაა საზოგადოებრივი ჯანმრთელობის დაცვა, სისტემის მართვისა და ფუნქციონირების უზრუნველყოფა. ასევე ჩვეულებრივი პერსონალური მონაცემების დამუშავების საფუძველი შეიძლება იყოს მნიშვნელოვანი საჯარო ინტერესი, მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესი და ა.შ [7]

მიუხედავად კანონიერი საფუძვლის არსებობისა,მნიშვნელოვანია, რომ აღნიშნულ უფლებაში ჩარევა ისეთი მოქმედების განხორციელებით, როგორიცაა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის შეგროვება, გენეტიკური თუ ბიომეტრიული მონაცემების შეგროვება და ა.შ განხორციელდეს ისე, რომ არ მოხდეს პირის ღირსებისა შეურაცხყოფა, ასევე არ დაირღვეს მისი სხვა ფუნდამენტური უფლებები, ამისათვის მნიშვნელოვანია პერსონალური მონაცემების დამუშავებისას ეს ქმედებები იყოს კანონიერი მიზნის შესაბამისი, აუცილებელი და პროპორციული დემოკრატიულ საზოგადოებაში. გარდა ზემოთ აღნიშნულისა, დამმუშავებლის მიერ უზრუნველყოფილი უნდა იყოს პირის პერსონალურ მონაცემთა დამუშავებისას მისი

[5] Recital 26. TheGeneral Data Protection Regulation (EU) 2016/679

[6] Recital 51. The General Data Protection Regulation (EU) 2016/679.

[7] მუხლი 5 საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ.28/12/2011.

უსაფრთხოება,რათა აღნიშნული ინფორმაცია არ იყოს მესამე პირებისათვის ხელმისაწვდომი, არ მოხდეს მისი გავრცელება ან სხვა (თავდაპირველისგან განსხვავებული) მიზნით გამოყენება.

პანდემიის გამოჩენის დღიდან საჯაროდ ვრცელდებოდა ინფორმაცია კოვიდ-პაციენტთა ისეთი მონაცემების შესახებ,როგორიცაა ასაკი, სქესი, მოქალაქეობა, გადაადგილების მარშრუტი, ასევე მათი ეთნიკური კუთვნილების შესახებ. მართალია აღნიშნული ხორციელდება საჯარო ინტერესის დაკმაყოფილების აუცილებლობიდან გამომდინარე, თუმცა როგორც უკვე აღვნიშნე მნიშვნელოვანია, იყოს დაცული მონაცემთა დამუშავების პრინციპები[8] და ნებისმიერ უფლებაში კანონიერი ჩარევისას აუცილებელია არსებობდეს პროპორციულობა. მართალია ჩემს მიერ ზემოთ ჩამოთვლილი ნიშნები ცალკეულად არ გვაძლევს პირის იდენტიფიცირების საშუალებას, თუმცა ერთობლიობაში, მითუმეტეს ისეთ მცირე მასშტაბიან ქვეყანაში, როგორიც საქართველოა ნამდვილად შეგვეძლება პირის იდენტიფიცირება, შესაბამისად უნდა მოხდეს მათი გამჟღავნება მხოლოდ იმ მოცულობით, რაც საჯარო ინტერესისათვისაა აუცილებელი. ასევე ჩემი აზრით პირის ეთნიკური კუთვნილების შესახებ ინფორმაციის გავრცელება[9], შესაძლოა პრობლემური იყოს იმ მხრივ,რომ საფრთხეს უქმნის დისკრიმინაციის აკრძალვას- მაგალითად, 2020 წლის დასაწყისში,გავრცელდა ინფორმაცია, რომ კოვიდ-ინფიცირებული ეთნიკურად აზერბაიჯანელი საქართველოს მოქალაქე იყო, რომელიც ვირუსის გავრცელების ერთ-ერთი წყარო გახდა. ამ ყველაფერმა კი საზოგადოებაზე უარყოფით გავლენა იქონია და ეთნიკური უმცირესობის, მათ შორის, აღნიშნული პირის მიმართ დისკრიმინაციული მიდგომა გააღვივა.

ასეთივე შემთხვევა დაფიქსირდა სამხრეთ კორეაშიც, სადაც ყველაზე მასშტაბურად ვირუსის გავრცელება ერთ-ერთ რელიგიურ სექტას უკავშირდებოდა, რაც მათ მიმართ აგრესიის მიზეზი გახდა. იქიდან გამომდინარე,რომ ამ ქვეყანაში არსებობს არაერთგვაროვანი მიდგომა განსხვავებული ორიენტაციის მქონე პირების მიმართ და ამასთან ერთად Covid-19 ის პირობებში რთული ხდება პირის პერსონალური მონაცემების უსაფრთხოების უზრუნველყოფა,ის პირები რომლებსაც კავშირი ჰქონდათ მეორე მასშტაბური კოვიდ-აფეთქებასთან,თავს არიდებდნენ სახელმწიფო უწყებებთან გამოჩენას,იქიდან გამომდინარე,არსებობდა საფრთხე მათი განსაკუთრებული კატეგორიის მონაცემის გამჟღავნებისა,ეს კი გამოიწვევდა მათ მიმართ აგრესიას,დისკრიმინაციულ მიდგომას,როგორც საზოგადოების,ასევე მათი ოჯახის წევრების მხრიდანაც.[10]

მართალია პანდემიის პირობებში პირის პერსონალურ მონაცემთა დაცვა იზღუდება, ჯანმრთელობის უსაფრთხოებიდან, ასევე მაღალი საჯარო ინტერესიდან გამომდინარე, თუმცა არანაკლებ მნიშვნელოვანია, რომ არ მოხდეს ამ და სხვა უფლების არაპროპორციულად შეზღუდვა, იმაზე მეტი მოცულობით ვიდრე ეს ლეგიტიმური მიზნის მიღწევისთვისაა საჭირო.ყოველთვის უნდა გვახსოვდეს,რომ მართალია მონაცემები არ შიძლება იყოს სიცოცხლის დაცვის ხელისშემშლელი, თუმცა მათი უსაფრთხოება გარანტირებული უნდა იყოს,

[8] მუხლი 4 საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ.28/12/2011.

[9]მუხლი2,გ,საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ. 28/12/2011 „განსაკუთრებული კატეგორიის მონაცემი – მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან“.

[10] Kanga Kong and Jihye Lee „ Korea's Virus Strategy is Tested by Outbreak at Nightclubs „ Bloomberg May 11,2020 https://www.bloomberg.com/news/articles/2020-05-11/gay-club-outbreak-poses-challenge-to-korea-s-open-virus-strategy [უ.გ.12 /05/2020].

მიუხედავად არსებული რთული სიტუაციისა, დაცული უნდა იყოს ძირითადი პრინციპები და ზემოთ აღნიშნულ ინტერესთა შორის ბალანსი.[11]

2. Covid-19-თან ბრძოლის მექანიზმები და მათი გავლენა მონაცემთა უსაფრთხოებაზე.

პანდემიის სპეციფიკური გარემოებების პირობებში პერსონალურ მონაცემთა დამუშავება სასიცოცხლოდ მნიშვნელოვანია, რათა შევაჩეროთ ვირუსის შემდგომი გავრცელება და ამასთან ერთად შევამსუბუქოთ მისი გავლენა. პირველ რიგში, ზოგიერთი ტიპის პერსონალური მონაცემების დამუშავება (როგორიცაა სახელი, მისამართი, სამუშაო ადგილი, მოგზაურობის შესახებ ინფორმაცია) შეიძლება გამოსადეგი იყოს რათა გავიგოთ სტუმრობდა თუ არა „ვირუსის კერას“ ან ჰქონდა თუ არა კოვიდ ინფიცირებულთან კავშირი პირს. მეორე შემთხვევაში, სპეციალური კატეგორიის მონაცემების (ჯანმრთელობის მდგომარეობის შესახებ მონაცემები, როგორიცაა მათ შორის ტესტის შედეგების დიაგნოსტიკა) დამუშავება კრიტიკულად მნიშვნელოვანია იმის გასაგებად აქვს თუ არა ინდივიდს კოვიდ-19-ისათვის დამახასიათებელი სიმპტომები.[12]

როგორც უკვე აღვნიშნე ახალმა ვირუსმა დააწესა ახალი დღის წესრიგი (New “normal”)-დისტანციურ მუშაობაზე გადავიდა როგორც საჯარო, ასევე კერძო დაწესებულებები, დისტანციურად მიმდინარეობს სწავლა მთელი მსოფლიოს გარშემო, როგორც უნივერსიტეტებში, ასევე სკოლებშიც რისთვისაც გამოიყენება თანამედროვე ტექნოლოგიები. პანდემიასთან ბრძოლის საუკეთესო საშუალება გახდა კონტაქტების ძიება (Contact Tracing), რაშიც დიდი წვლილი მიუძღვის ციფრულ ტექნოლოგიებს გარდა საჯარო დაწესებულებებისა, ასევე დამსაქმებლებს ხელი მიუწვდებათ დასაქმებულთა ისეთ პირად ინფორმაციაზე, რაც მას ჩვეულებრივ მდგომარეობაში ამ პირის უფლებების დარღვევად ჩაითვლებოდა (მაგ: მისი მოგზაურობის შესახებ ინფორმაცია, ასევე მისი ჯანმრთელობის შესახებ ინფორმაცია, რაც სამუშაო ადგილზე ვირუსის გავრცელების პრევენციისთვისაა საჭირო).

ჯერ კიდევ 2003 წელს SARS-ის შემთხვევების დაფიქსირებისას გამოიყენებოდა ინფორმაციებისა და საკომუნიკაციო ტექნოლოგიების (ისტ) ხელსაწყოები, რათა უსწრაფესად მომხდარიყო ინფექციის წყაროების, კლასტერების და გადაცემის გზების აღმოჩენა. კოვიდ-19-ის პანდემიის დროს კვლავ საჭირო გახდა ამ მექანიზმების ამოქმედება და ტექნოლოგიების სფეროს დიდი წვლილი შეიტანა ვირუსთან ბრძოლაში.[13]

3. ლოკაციის მონაცემების გამოყენება და COVID აპლიკაციები.; მონაცემთა უსაფრთხოების უზრუნველყოფა და კიბერუსაფრთხოება.

კოვიდ-19-ის ერთ-ერთი დამახასიათებელი თვისებაა, რომ როგორც რესპირატორული დაავადება ვრცელდება მცირე წვეთებით ცხვირიდან ან პირიდან, რომლებიც შეიძლება პირდაპირ შეისუნთქოს სხვა პირმა ან თუ ინფიცირებულ ზედაპირთან აქვს კონტაქტი, აქედან გამომდინარე ვირუსის თავიდან ასაცილებლად მნიშვნელოვანია დაცული იყოს სოციალური დისტანციის ზომები. სწორედ ამ მიზნისთვის ბევრმა ქვეყანამ მსოფლიოს გარშემო მიმართა ლოკაციის მიკვლევისათვის მობილური მოწყობილობების გამოყენებას.ეს გულისხმობს პირის/პირთა ადგილმდებარეობისა თუ გადაადგილების მონაცემების მოპოვებას და დამუშავებას სხვადასხვა ისეთი რესურსებიდან,როგორებიცაა ტელეკომუნიკაციის კომპანიები,

[11] A. Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe Strasbourg , Joint Statement on „ the right to data protection in the context of the COVID-19 pandemic” 30 March 2020- pg.2.

[12] E. Ventrella, Privacy in emergency circumstances: data protection and the COVID-19 pandemic.ERA Forum 21,379–393 (2020).– pg.3 .

[13] D. Shu Wei Ting, L. Carin, V. Dzau, et al. Digital technology and COVID-19. NatMed 26,459–461 (2020).

ასევე საძიებო სისტემის მეშვეობით და გარდა ამისა პირდაპირ მობილურზე დარეგისტრირებული აპლიკაციებიდან (Google, Facebook, Uber აქტიურად მონაწილეობდნენ ამ პროცესებში)[14], რომელსაც ჩვენივე თანხმობით წვდომა აქვს ჩვენს გეო-ლოკაციაზე. ლოკაციის მიკვლევა შესაძლებელია როგორც ფართო მასშტაბით, მთლიან მოსახლეობაზე დაკვირვებით-დიდი თავშეყრის ადგილების აღმოსაჩენად, ასევე ინდივიდუალურად-პიროვნების გადაადგილების მონიტორინგისათვის, რათა მოხდეს რისკის ქვეშ მყოფ პირთა იდენტიფიცირება.

ამ მეთოდებს ეფექტურად იყენებენ აზიის ქვეყნებში (სამხრეთ კორეა, ჩინეთი, სინგაპური) სადაც არამხოლოდ იკვლევდნენ, არამედ მესამე პირებისთვის ხელმისაწვდომი ხდებოდა დაინფიცირებულ პირთა გადაადგილების შესახებ ინფორმაცია[15], თუმცა ევროპის ქვეყნებში, კანონმდებლობის სპეციფიკიდან გამომდინარე განსხვავებული მიდგომებია. ლოკაციის ინფორმაცია სახელმწიფო ორგანოებს შესაძლებელია გადაეცეს მხოლოდ ანონიმური (დეპერსონალიზირებული) ფორმით, რაზეც უნდა იზრუნოს უშუალოდ მისმა მიმწოდებელმა. რაც შეეხება ისეთი ინფორმაცია ადგილმდებარეობის შესახებ, რომელიც უშუალოდ მოწყობილობიდანაა აღებული შეიძლება გადაეცეს მათ უშუალოდ მონაცემთა სუბიექტის თანხმობით ან თუ ამის აუცილებლობა მისივე მოთხოვნიდან გამომდინარეობს. თუმცა როგორც ზემოთ არაერთხელ აღვნიშნეთ პერსონალური მონაცემების დაცვა არ არის აბსოლუტური უფლება და დასაშვებია მასში ჩარევა საჭირო, მისაღები, პროპორციული ზომებით, რომლებიც დემოკრატიული საზოგადოებისთვისაა დამახასიათებელი. ყოველ ზემოთ აღნიშნულ შემთხვევაში, იმისათვის, რომ უზრუნველყოფილი იყოს მონაცემთა უსაფრთხოება, რათა იგი შემდგომში არ იყოს ხელმისაწვდომი მესამე პირებისათვის საჭიროა მოხდეს ამ მონაცემთა დეპერსონალიზაცია, რომლის შედეგადაც მათი დაკავშირება კონკრეტულ პირთან, ე.ი პირის იდენტიფიცირება შეუძლებელი იქნება.

მონაცემთა უსაფრთოხების უზრუნველყოფის ისეთი მნიშვნელოვანი სახეები როგორიცაა მისი დეპერსონალიზაცია და ფსევდონიმიზაცია არ უნდა იქნეს გაიგივებული, ვინაიდან ეს უკანასკნელი ანონიმური მონაცემებისგან განსხვავებით ისევ რჩება პერსონალურ მონაცემთა დაცვის სამართლის გავლენის ქვეშ.ანონიმურმა მონაცემმა უნდა გაიაროს „გონივრულობის“ ტესტი,რომლის შესახებაც მაღლაც გვქონდა საუბარი.

აღსანიშნავია,რომ საფრთხე მონაცემების ახლიდან იდენტიფიცირებადად გადაქცევისათვის, პირის ადგილმდებარეობის, მისი გადაადგილების განსაკუთრებულობიდან გამომდინარე, მაინც არსებობს, და კვლევებმა აჩვენა,რომ ის რაც ანონიმურად ითვლება შეიძლება მართლაც ასე არ იყოს[16]. მნიშვნელოვანია დეპერსონალიზაციის პროცესი ზედმიწევნით წარიმართოს და გამოყენებული იყოს ყველა საჭირო და აუცილებელი ზომა, გარდა ამისა ეს მეთოდები გამჭირვალე უნდა იყოს სუბიექტისთვისაც.

რაც შეეხება აპლიკაციებს აქაც კანონმდებლობიდან გამომდინარე მსოფლიოს მასშტაბით განსხვავებული მიდგომა არსებობს. ევროსაბჭოს გზამკვლევში კოვიდ აპლიკაციების შესახებ[17]

[14] C. Dumbrava "Tracking mobile devices to fight coronavirus*" European Parliamentary Research* Service,PE 649.384 – April 2020.

[15] The New York Times. As Coronavirus Surveillance Escalates, Personal Privacy Plummets ",2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html[უ.გ.17.04.2020 წ].

[16] de Montjoye et al "Unique in the Crowd: The privacy bounds of human mobility" (2013) and (Pyrgelis et al.,2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

[17] European commission communication from the commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01).

აღნიშნულია, რომ მონაცემთა სენსიტიურობიდან გამომდინარე, მნიშვნელოვანია რომ პერსონალურ მონაცემთან წვდომა ჰქონდეს ჯანდაცვის ორგანიზაციას და უშუალოდ მის მიერ ხდებოდეს ამ ინფორმაციის დამუშავება.

განსხვავებით ჩინეთისგან, სადაც აპლიკაციის ჩამოტვირთვა სავალდებულოა ყველასთვის, ზემოთ აღნიშნული გზამკვლევი მოიცავს რეკომენდაციას მის ნებაყოფლობითობის შესახებ. გარდა ამისა სუბიექტს უნდა ჰქონდეს „კონტროლი“ მის პერსონალურ მონაცემებზე, ინფექციის დადასტურების შემთხვევაში კი მის კონტაქტს ინფორმაცია ანონიმური ფორმით გადაეცემა. მნიშვნელოვანია ისიც, რომ რათა არ მოხდეს არასწორი ინფორმაციის გავრცელება, მხოლოდ ინფორმაციის შესაბამისი დაზუსტების შემდეგ ენიჭება მომხმარებელს „ინფიცირებულის“ სტატუსი. ამასთან ერთად აპლიკაცია უნდა მოქმედებდეს იმ შემთხვევაში, თუ საზოგადოების მხრიდან მათი პრაქტიკაში მოხმარება დაფიქსირდება, რასაც ჩამოტვირთვებზე დაკვირვებით ადგენენ. იმ შემთხვევაში, თუ აპლიკაციაზე პრაქტიკულად არ არსებობს მოთხოვნა, მისი მიზნები ვერ მიიღწევა, იგი უნდა ავტომატურად განადგურდეს. გარდა ზემოთ აღნიშნულისა მნიშვნელოვანია ის ფაქტიც, რომ პანდემიის სიტუაციის დასრულების შემდეგ აპლიკაციის და შესაბამისად დამუშავებული მონაცემების განადგურება არ უნდა იყოს სუბიექტის ნებაზე დამოკიდებული, არამედ უშუალოდ ვირუსის დამარცხების მომენტიდანვე უნდა განხორციელდეს მმართველი ორგანოების მხრიდან. მონაცემთა დამუშავებისას ინფორმაცია უნდა იყოს ხელმისაწვდომი მისი სუბიექტისთვის, ის უნდა მოიპოვებოდეს მხოლოდ იმ კონკრეტული, ლეგიტიმური მიზნებისთვის, რისთვისაც თავდაპირველად გახდა დასაშვები მისი დამუშავება (მაგ-კარანტინის ზომების დაცვის, სოციალური დისტანცირება, ინფიცირებულთა წყაროს მოკვლევი, ტელემედიცინის და ა.შ). აუცილებელია დამუშავდეს მხოლოდ იმ მოცულობის მონაცემები და იმ დროით, რაც მიზნის მიღწევისთვისაა საჭირო. ეს ყველაფერი წარმოადგენს მონაცემთა დამუშავების პრინციპებს, რაც ყველა შემთხვევაში გამოიყენება.

აპლიკაციის შექმნისას ამ პრინციპების დაცვამ შეიძლება არამხოლოდ მონაცემთა უსაფრთხოებას შეუქმნას საფრთხე, არამედ ინდივიდთა სხვა უფლებებსაც. მაგალითად მოსკოვის კოვიდ-აპლიკაციის არასწორი ფუნქციონირების გამო, რაც იმაზე მეტი ინფორმაციის მოპოვებასთან არის დაკავშირებული, რომელიც მიზნის-კარანტინის წესების დაცვას ემსახურებოდა ასობით ადამიანი დაჯარიმდა.[18]

აპლიკაციის შექმნისას გარანტირებული უნდა იყოს სუბიექტთა მონაცემთა უსაფრთხოება, ამისათვის პირის პერსონალური მონაცემები განთავსებული უნდა იყოს არა ცენტრალურ სერვერზე, არამედ ადგილობრივ, ინდივიდის ტერმინალურ მოწყობილობაზე, ფსევდონიმიზირებული ფორმატით, დაშიფრულ მდგომარეობაში, შესაბამისი ტექნიკის (state-of-the art cryptographic) გამოყენებით. იმისათვის, რომ მესამე პირების მიერ მიკვლევა მონაცემებისა გამორიცხული იყოს, აპლიკაციისთვის Bluetooth აქტივაცია, სხვა ლოკაციის სერვისების გარეშე უნდა ხდებოდეს. ასევე „სიახლოვის მონაცემების“ (proximity data) BLE[19]-ის მეშვეობით შეგროვებისას უმჯობესია არ გამოიყენებოდეს უშუალოდ მოწყობილობის ID,არამედ რეგულარულად იქმნებოდეს დროებითი, ახალი საიდენტიფიკაციო კოდი. აღნიშნული უზრუნველყოფს ჰაკერების მიერ თვალთვალისა და მიყურადებისგან დაცვას, ამასთან ერთად კიდევ უფრო ართულებს პირის იდენტიფიცირებას. დამატებით, რათა დაცული იყოს მონაცემები, ნებისმიერი ინფორმაცია, რომელიც პირის მოწყობილობიდან გადაეცემა

[18]„Russia: Intrusive Tracking App Wrongly Fines Muscovites“*Human rights watch, May21,2020* https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites [უ.გ.21.05.2020].

[19] Bluetooth low energy.

ჯანდაცვის ორგანოებს, უნდა იყოს დაშიფრული. ხოლო იმ ქვეყნებში, სადაც მოპოვებული პერსონალური მონაცემების გამოყენება შეიძლება გამოიყენებოდეს სამეცნიერო კვლევის მიზნებისათვის, მონაცემთა უსაფრთხოების უზრუნველყოფისათვის მათ ფსევდონიმიზაციას უნდა მიმართონ.[20]

როგორც სტატიის დასაწყისში აღვნიშნე კოვიდ-19-ის შედეგად ჩამოყალიბდა ახალი დღის წესრიგი, რომლის ფარგლებშიც თითქმის ყველაფერი დამოკიდებული გახდა ციფრულ ტექნოლოგიებზე. ჩვენი პერსონალური მონაცემების მასშტაბური დამუშავება საზოგადოებრივი ჯანდაცვის უსაფრთხოების უზრუნველყოფისთვის კიდევ უფრო დაუცველს ხდის მათ. იზრდება საშიშროება იმისა, რომ ჩვენი მონაცემები ხელმისაწვდომი გახდება მესამე პირებისთვის, გარდა ამისა,დიდია კიბერშეტევების საფრთხეც, რაც კვლევების თანახმად სხვა ტრადიციულ დანაშაულებს ჩაანაცვლებს მათი მასშტაბებისა და ხარჯების მხრივ[21] აღსანიშნავია, რომ 2020 წლის მარტის მონაცემებით კიბერდანაშაულის შემთხვევები 600% ით იყო გაზრდილი.[22] აღნიშნული დაკავშირებული არის იმასთანაც, რომ ვირუსის პერიოდში მოსახლეობა მთლიანად დამოკიდებული გახდა ელექტრონულ სერვისებზე. აქედან გამომდინარე ხშირად ხდებიან ე.წ „ფიშინგის“ მსხვერპლი, რომლის შედეგადაც გასცემენ საკუთარ პერსონალურ მონაცემებს. შეიქმნა ცრუ საიტები, რომელიც დაკავშირებული იყო კოვიდ-19 თან, ასევე თითქოსდა მმართველი ორგანოების მიერ შექმნილი ვებ-გვერდები უზიარებდნენ ვებ-ლინკებს, სადაც სუბიექტებს შეჰყავდათ თავიანთი პერსონალური მონაცემები და ამით ხდებოდნენ ფინანსური თაღლითობის მსხვერპლნი. დამნაშავეებმა დრო იხელთეს და მათი მთავარი სამიზნე გახდა სამედიცინო, კვლევითი დაწესებულებები და სხვადასხვა ორგანიზაციები. ისინი „მძევლად იყვანდნენ“ სუბიექტთა პერსონალურ მონაცემებს და მხოლოდ შესაბამისი თანხის მიღების შემდეგ უბრუნებდნენ მათ უკან. ასეთი შემთხვევები გვაქვს იტალიასა და კანადაში-ცრუ-კოვიდ აპლიკაციის შექმნით.2020 წლის 1 სექტემბერს კიბერშეტევა განხორციელდა საქართველოს ჯანდაცვის სამინისტროს[23] კომპიუტერულ სისტემაზე, რომლის შედეგადაც დაავადებათა კონტროლისა და ლუგარის კვლევითი ცენტრის მონაცემთა ბაზებში დაცული სამედიცინო ხასიათის დოკუმენტაციას დაეუფლნენ და ეს მონაცემები აიტვირთა ერთ-ერთ უცხოურ ვებ-გვერდზე, სადაც ხელმისაწვდომი გახდა მასობრივი მომხმარებლებისთვის.[24]

სწორედ გაზრდილი საფრთხიდან გამომდინარე, ვფიქრობ, მნიშვნელოვანია პანდემიის პირობებში გავითვალისწინოთ სახელმწიფო ინსპექტორის სამსახურის მიერ გავრცელებული რეკომენდაციები „COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავების“ შესახებ.

[20] EUROPEAN COMMISSION Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01) – 3. ELEMENTS FOR A TRUSTFUL AND ACCOUNTABLE USE OF APPS,3.8. Ensuring the security of the data.

[21] Cybersecurity Ventures: 2019, official annual cybercrime report (2019). https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ [უ.გ26.03.2020].

[22]F. Shi: „Threat spotlight: coronavirus-related phishing Barracuda, March26,2020. https://blog.barracuda.com /2020/03/26/threat-spotlight-coronavirus-related-phishing/ [უ.გ.26.05.2020].

[23] საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო.

[24] „კიბერშეტევა ჯანდაცვის სამინისტროზე და რუსული კვალი“ ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 3 სექტემბერი 2020 https://idfi.ge/ge/strategy_of_russian_cyber_operations [უ.გ.3.09.2020]

დასკვნა

კოვიდ-19-მა კიდევ ერთხელ დაგვანახა თუ რა მნიშვნელოვანი როლი აქვს პირის პერსონალურ მონაცემებს მის ცხოვრებაში. მართალია ამ უფლების დაცვა უმნიშვნელოვანესია, როგორც სხვა ფუნდამენტური უფლებებისა, თუმცა პერსონალური მონაცემების დაცვის სამართალი არ აღუდგება წინ ისეთი ზომების გატარებას, რომელიც სახალხო ჯანდაცვის ეფექტურობას, პანდემიის დამარცხებას უზრუნველყოფს. პერსონალური მონაცემების დაცვა არ წარმოადგენს პირის აბსოლუტურ უფლებას, რომელიც გადაწონის ყველა სხვა ღირებულებებს, მათ შორის სხვა უფლებებსა და თავისუფლებებს. არ შეიძლება მაშინ, როდესაც არსებობს ადამიანთა სიცოცხლის საფრთხე, პერსონალურ მონაცემებს უპირატესობა მივანიჭოთ, თუმცა არ უნდა დაგვავიწყდეს, რომ ადამიანის უფლებაში ნებისმიერი ლეგიტიმური ჩარევისას აუცილებელია დაცული იყოს შესაბამისი ზომები,ეს ჩარევა იყოს პროპორციული და მიზნის შესაბამისი, აუცილებელი დემოკრატიულ საზოგადოებაში. ყოველ შემთხვევაში დაცული უნდა იყოს ბალანსი უფლებებს შორის.იქიდან გამომდინარე, რომ პერსონალური მონაცემები პანდემიის პირობებში უფრო დაუცველი ხდება ვიდრე ჩვეულებრივ მდგომარეობაში, მნიშვნელოვანია უზრუნველყოფილი იყოს მისი უსაფრთხოება მონაცემთა დამუშავებისას, ამისათვის კი დამმუშავებელთა მიერ უპირობოდ დაცული უნდა იყოს პერსონალურ მონაცემთა სამართლის პრინციპები. გარდა ამისა უზრუნველყოფილი უნდა იყოს დამატებით უსაფრთხოების ზომებიც, რაზეც ზემოთ გვქონდა საუბარი. ვფიქრობ ჩემს მიერ მოყვანილი მაგალითები კოვიდ-19-ის პირობებში მონაცემთა დამუშავებისა, ნათელს ხდის თუ რა გავლენა იქონია პანდემიამ პერსონალურ მონაცემთა უსაფრთხოებაზე. ჩემი აზრით, არანაკლებ მნიშვნელოვანი პროცესები გველის წინ პანდემიის დასრულების შემდგომ, როდესაც ამ მასშტაბების მონაცემთა დამუშავება დაუშვებელი გახდება და დამმუშავებლები ვალდებულები იქნებიან გაანადგურონ ეს მონაცემები ან მოახდინონ მათი დეპერსონალიზაცია. ასე,რომ კოვიდ-19-ის გავლენა მონაცემთა უსაფრთხოებაზე არამხოლოდ პანდემიის პერიოდში, არამედ მისი დასრულების შემდეგაც ისევ დიდი იქნება.

ბიბლიოგრაფია

1. ევროპის საბჭოს ხელშეკრულებების სერია-ნ.108 კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ. სტრასბურგი, 28 იანვარი,1981 წ;
2. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ,რომელიც აუქმებს 95/46/EC დირექტივას (მონაცემთა დაცვის ზოგადი რეგულაცია);
3. ევროკომისიის შეტყობინება კომისიიდან, სახელმძღვანელო, კოვიდ-19 პანდემიის წინააღმდეგ ბრძოლისათვის გამოყენებული აპლიკაციების პერსონალურ მონაცემთა დაცვასთან მიმართებით (2020/C 124 I/01);
4. ევროპის პერსონალურ მონაცემთა დაცვის კომიტეტი 03/2020-ის სახელმძღვანელო კოვიდ-19 ის აფეთქებასთან დაკავშირებით სამეცნიერო მიზნით ჯანმრთელობის შესახებ მონაცემთა დამუშავებაზე. დამუშავებული 21 აპრილს,2020 წ;
5. ევროპის პერსონალურ მონაცემთა დაცვის კომიტეტი, 04/2020-ის სახელმძღვანელო კოვიდ-19 პანდემიის აფეთქებასთან დაკავშირებით ადგილმდებარეობის შესახებ მონაცემების და კონტაქტების კვლევის ხელსაწყოების გამოყენება;
6. ევროპის პერსონალურ მონაცემთა დაცვის კომიტეტის განცხადება, კოვიდ-19-ის აფეთქებისას პესონალურ მონაცემთა დამუშვების შესახებ. დამუშავებული19 მარტი, 2020 წ;
7. ევროპის კავშირის საბჭოს დასკვნები, ჯანმრთელობასთან დაკავშირებით კოვიდ-19-ის შედეგად მიღებული გამოცდილება. (2020/C 450/01), 28.12.2020;
8. კოვიდ-19-თან საბრძოლველად პრობლემის გადაჭრის ციფრული გზები.ევროპის საბჭოს 2020 წლის ანგარიში პერსონალურ მონცემთა დაცვასთან დაკავშირებით.2020 წლის ოქტომბერი;
9. კანგა კონგი და ჯიჰიე ლი „ კორეის ვირუსთან ბრძოლის სტრატეგიის გამოცდა „ღამის კლუბის“ აფეთქების სახით“ ბლუმბერგი, 11 მაისი, 2020 წელი https://www.bloomberg.com/news/articles/2020-05-11/gay-club-outbreak-poses-challenge-to-korea-s-open-virus-strategy (უკანასკნელად გადამოწმდა 12.05.2020);
10. ალესანდრა პიერუჩი, 108-ე კონვენციის კომიტეტის ხელმძღვანელი, ჯინ-ფილიპ ვოლტერი პერსონალურ მონაცემთა დაცვის კომისარი ევროპის საბჭოში,საერთო განცხადება, კოვიდ-19 პანდემიის კონტექსტში მონაცემთა დაცვის უფლების შესახებ 30 მარტი, 2020 წ;
11. ემანუელე ვეტერელა, პრივატულობა საგანგებო შემთხვევებში: პერსონალურ მონაცემთა დაცვა და კოვიდ-19-ის პანდემია, ERA-ს ფორუმი ნ.21,379-393 (2020;
12. დანიელ შუ ვეი ცინ, ლორენს კარინი, ვიქტორ ძაუ, ტიენ ი ვონგ, ციფრული ტექნოლოგიები და კოვიდ-19.ნაც-მედ 26,459-461 გ(2020);
13. დე მონტიოიე „უნიკალურობა ბრბოში: ადმიანების გადაადგილების პრივატულობის საზღვრები“ 2013 წ. და „კაკუ-კაკუ, ვინ არის მანდ? აგრეგატული ადილმდებარეობის მონაცემებში ჩარევა“ 2017 წ;
14. The New York Times „კორონავირურის მეთვალყურეობის გაზრდის შედეგად, პერსონალური მონაცემების პრივატულობა იკლებს“;

15. 3 მარტი 2020 წ. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html [უკანასკნელად გადამოწმდა17.04.2020];
16. Cybersecurity Ventures 2019 „ყოველწლიური კიბერუსაფრთხოების აგარიში“ 2019წ. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ [უკანასკნელად გადამოწმდა 26.03.2020];
17. ფლემინ ში, „საყურადღებო საფრთხე: კოროავირუსთან დაკავშირებლი ფიშინგი“ Barracuda,26/03/2020წ.https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ [უკანასკნელად გადამოწმდა 26.03.2020];
18. „კიბერშეტევა ჯანდაცვის სამინისტროზე და რუსული კვალი“ ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 3 სექტემბერი 2020. https://idfi.ge/ge/strategy_of_russian_cyber_operations [უკანასკნელად გადამოწმდა 3.09.2020];
19. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ.28/12/2011;
20. „მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო“ ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018.

Bibliography

1. European Treaty Series-No.108.Convention for the Protection of Individuals with regard to Automatic.Processing of Personal Data.Strasbourg,28. I.1981;
2. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
3. EUROPEAN COMMISSION COMMUNICATION FROM THE COMMISSION, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01);
4. European Data Protection Board, „Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak”. Adopted on 21 April 2020;
5. European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020;
6. European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adoptedon 19 March 2020;
7. NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES COUNCIL Council conclusions on COVID-19 lessons learned in health 2020/C 450/01 28.12.2020;
8. “DIGITAL SOLUTIONS TO FIGHT COVID-19“ 2020 DATA PROTECTION REPORT, Council of Europe, October 2020;
9. Kanga Kong and Jihye Lee „Korea’s Virus Strategy is Tested by Outbreak at Nightclubs„ Bloomberg May 11,2020 https://www.bloomberg.com/news/articles/2020-05-11/gay-club-outbreak-poses-challenge-to-korea-s-open-virus-strategy [Last seen 12/05/2020];

10. Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe Strasbourg , Joint Statement on „ the right to data protection in the context of the COVID-19 pandemic „.30 March 2020;
11. Emanuele Ventrella, Privacy in emergency circumstances: data protection and the COVID-19 pandemic.ERA Forum 21,379–393 (2020);
12. Daniel Shu Wei Ting, Lawrence Carin, Victor Dzau, Tien Y Wong. et al. Digital technology and COVID-19. NatMed 26,459– 461 (2020);
13. de Montjoye et al, „Unique in the Crowd: The privacy bounds of human mobility" (2013) and (Pyrgelis et al.,2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data";
14. Russia: Intrusive Tracking App Wrongly Fines Muscovites „ Human rights watch, May 21,2020. https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites [Last seen 21.05.2020.];
15. Costica Dumbrava "Tracking mobile devices to fight coronavirus" European Parliamentary Research Service, PE 649.384 – April 2020;
16. The New York Times. „As Coronavirus Surveillance Escalates,Personal Privacy Plummets", 2020/03/23. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html [Last seen 17.04. 2020];
17. Cybersecurity Ventures: 2019, official annual cybercrime report (2019). https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ [Last seen 17.04. 2020];
18. Shi Fleming.: „Threat spotlight: coronavirus-related phishing". Barracuda,March 26,2020. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ [Last seen 26.03.2020];
19. Cyberattack on the Ministry of Health and Russian Trace" – Institute for development of freedom of information,3 September 2020. https://idfi.ge/ge/strategy_of_russian_cyber_operations [Last seen 3.09. 2020];
20. „Law of Georgia on Personal Data Protection" 28/12/2011;
21. „Handbook on European data protection law" Luxemburg : Publications Office of the EU.2018 edition.

COVID- 19 ის გავლენა მონაცემთა უსაფრთხოებაზე

ელენე სულაბერიძე,
ილიას სახელმწიფო უნივერსიტეტი

აბსტრაქტი

ტექნოლოგიის განვითარებასთან ერთად უფრო მეტი პროდუქტი ხდება ჩვენთვის ხელმისაწვდომი ინტერნეტის საშუალებით. COVID-19 პანდემიიდან გამომდინარე სხვადასხვა კომპანიები და ორგანიზაციები უფრო მეტად არიან დამოკიდებული ინტერნეტ მომსახურებაზე, ვიდრე ოდესმე. გაიზარდა დისტანციური მომსახურების მოთხოვნილება, რაც ადამიანებს ეხმარება იმაში რომ მარტივად და სახლიდან გაუსვლელად მიიღონ სასურველი მომსახურება და განახორციელონ საჭირო მოქმედებები, თუმცა, ამას თან ახლავს გარკვეული რისკები, რამაც შესაძლოა უარყოფითი გავლენა მოახდინოს მონაცემთა უსაფრთხოებაზე.

წინამდებარე ნაშრომი მიზნად ისახავს წარმოაჩინოს ის რისკები, რომლებიც პანდემიის პერიოდში სულ უფრო მეტად იჩენს თავს და დაუცველს ხდის სხვადასხვა სახის მონაცემთა უსაფრთხოებას, რაც შესაძლოა გამოწვეული იყოს ადამიანების მიერ ინტერნეტში განხორციელებული ნებისმიერი მოქმედების შედეგად.

ნაშრომი ასევე მოიცავს სხვადასხვა სახის მონაცემთა განმარტებას და ინფორმაციას იმის შესახებ, თუ რა მნიშვნელობა აქვს თითოეული მათგანის დაცვას ადამიანის უსაფრთხოებისათვის და რა სახის მონაცემებია განსაკუთრებით საფრთხის ქვეშ, ასევე, რა მიზნით შეიძლება იქნეს გამოყენებული ესა თუ ის მონაცემი.

გამოკვლეულია სხვადასხვა ქვეყნებში გატარებული ღონისძიებები COVID-19-ის გავლენის შესაჩერებლად მონაცემთა უსაფრთხოებაზე, რომლებიც ემსახურებიან პერსონალურ მონაცემთა სუბიექტის დაცვას, ვინაიდან ზოგიერთ სახელმწიფოში განხორციელებული იყო გარკვეული ზომები პანდემიასთან საბრძოლველად, რომლებიც შესაძლოა ეფექტური აღმოჩნდა ვირუსის პრევენციის მიზნით, თუმცა, ამან უარყოფითი გავლენა მოახდინა მოქალაქეთა პერსონალურ მონაცემებზე. მიმოიხილავს არა მარტო უცხოურ, არამედ ქართულ რელობაში არსებულ რისკებს, რომლებიც განსაკუთრებით გახშირდა პანდემიის პერიოდში და გავლენა მოახდინა ადამიანების პერსონალურ მონაცემებზე და ასევე, რა სახის ღონისძიებები იქნა გატარებული მის შესაჩერებლად.

ნაშრომში ასევე წარმოდგენილია ის რეკომენდაციები და რჩევები, რომლის გათვალისწინებითაც შევძლებთ იმ რისკების პრევენციას, რომლებიც შეიძლება მოყვეს ჩვენს მიერ ინტერნეტში განხორციელებულ მოქმედებებს. რას უნდა მივაქციოთ ყურადღება და როგორ უნდა გამოვიცნოთ რომ კონკრეტული ვებ-გვერდი არ არის სანდო, რა მოქმედებები უნდა განვახორციელოთ იმისათვის რომ თავიდან ავირიდოთ ჩვენი მონაცემეების გასაჯაროვება და რაიმე მიზნით გამოყენება.

და ბოლოს, ნაშრომში გამოკვლეულია საქართველოში პერსონალურ მონაცემთა დაცვის ინსპექტორის როლი განსაკუთრებით პანდემიის პირობებში დაუცველი მონაცემების უსაფრთხოებისათვის, წარმოდგენილია ქართული კანონმდებლობით დაწესებული

პასუხისმგებლობა, როდესაც უკვე დარღვეულია მოქალაქის პერსონალური მონაცემების უსაფრთხოება.

საკვანძო სიტყვები: პერსონალური მონაცემები, covidsafe- აპლიკაციები, კეთილდღეობის სერვისები, კონფიდენციალურობა.

Abstract

With the development of technology more products are made through the internet. Since the COVID-19 pandemic, various companies and organizations have become more dependent on Internet services than ever before. The need for remote services has increased, which helps people to easily get the desired service and perform the necessary actions without leaving home, although this has some risks that can have a negative impact on data security.

The purpose of this paper is to highlight the risks that are becoming increasingly apparent during the pandemic period, and that various types of data security will become vulnerable to any human-induced Internet activity.

Measures have been taken in various countries to reduce the impact of COVID-19 on data security, which serves to protect the subject of personal data, as some countries have implemented measures to combat pandemics that may be effective in preventing the virus, adversely affecting citizens' personal data. It reviews not only foreign but also Georgian realities, which have become particularly frequent during the pandemic and affect people's personal data, as well as what measures have been taken to stop it.

The paper also provides recommendations and tips to help us avoid the risks that may arise from our actions on the Internet. What to look out for and how to guess that a particular website is unreliable, what actions we need to take to prevent our data from being disclosed and used for any purpose.

Finally, the paper examines the role of the Personal Data Protection Inspector in Georgia, especially for data security in a pandemic, and presents responsibilities under Georgian law when the security of a citizen's personal data has already been compromised.

Keywords: personal data, covidsafe-applications, welfare services, privacy.

შესავალი

დღესდღეობით ჩვენ ვცხოვრობთ ტექნოლოგიურ ეპოქაში, სადაც ინტერნეტი გლობალურ საკომუნიკაციო და საინფორმაციო საშუალებად იქცა. მისი საშუალებით შეგვიძლია განვახორციელოთ ელექტრონული შესყიდვები, მივიღოთ სხვადასხვა სახის მომსახურება, ეს იქნება სახელმწიფო თუ საბანკო სერვისები, ონლაინ ვაჭრობა და სხვ. ინტერნეტმომსახურებაზე დამოკიდებულება განსაკუთრებით გაიზარდა covid-19 პანდემიის პერიოდში, როდესაც თითქმის ყველა კომპანია თუ ორგანიზაცია იძულებულია განახორციელოს ონლაინ მომსახურება და ფაქტობრივად მოქალაქეების ყოველდღიური აქტივობა გახდა დამოკიდებული ინტერნეტ სივრცეზე, ეს ეხება საბანკო მომსახურებას, ონლაინ მაღაზიებს, სასწავლო პლატფორმას და სხვ. რაც პანდემიის პირობებში უზრუნველყოფს იმას, რომ მოქალაქეებმა უსაფრთხოდ, სახლიდან გაუსვლელად და ვირუსისგან დაცულად მიიღონ სასურველი მომსახურება და განახორციელონ საჭირო მოქმედებები, რაც, ცალსახად, ნამდვილად კომფორტულია, თუმცა, ასეთი კომუნიკაციის

მამოძრავებელი ძალა მონაცემებია, რომლებიც დიდი ოდენობით გროვდება ინტერნეტში, მათი არასათანადოდ დაცვა კი საფრთხის ქვეშ აყენებს მომხმარებელთა პერსონალურ მონაცემებს.

ნაშრომის მიზანიც სწორედ ის არის რომ მომოიხილოს თუ ზოგადად რა გავლენა მოახდინა პანდემიამ მონაცემთა უსაფრთხოებაზე, რადგან ამ პერიოდში განსაკუთრებით გაძლიერდა მონაცემთა ხელმისაწვდომობის შესაძლებლობა, საზოგადოების ყურადღება სულ უფრო მეტადაა მიმართული მათ ჯანმრთელობაზე და ყოველდღიურ ინფორმაციაზე ვირუსის შესახებ, აქედან გამომდინარე ისინი ნაკლებ ყურადღებას აქცევენ საკუთარი მონაცემების დაცვას.

ნაშრომში ყურადღება გამახვილებულია იმ მონაცემების დაცვაზე, რომელთა უსაფრთხოებაზეც პანდემიამ განსაკუთრებული გავლენა მოახდინა, ასეთია, მაგალითად, პირის ჯანმრთელობის შესახებ ინფორმაცია, რომლის დაცვაც პანდემიის პერიოდში განსაკუთრებით მნიშვნელოვანია და რომელთა გამჟღავნებამაც შესაძლოა კონკრეტულ პიროვნებას დაბრკოლება შეუქმნას გარესამყაროსთან ურთიერთობის კუთხით.

ნაშრომში ასევე მოცემულია სხვადასხვა ქვეყნებში გატარებული ღონისძიებები COVID- 19 ის გავლენის შესაჩერებლად მონაცემთა უსაფრთხოებაზე, მექანიზმები რომელთა საშუალებითაც ისინი ცდილობენ დაიცვან თავიანთი ქვეყნის მოსახლეობა მონაცემთა არაკანონიერად დამუშავებისაგან.

ნაშრომის მიზანია მიმოიხილოს COVID -19 ის პერიოდში პერსონალური მონაცემების დაცვის მდგომარეობა საქართველოში, კერძოდ, რა გავლენა მოახდინა პანდემიამ მოსახლეობის მონაცემებზე საქართველოს.

ნაშრომში წარმოდგენილია ის რეკომენდაციები და რჩევები, რომელთა გათვალისწინებითაც შევძლებთ იმ რისკების პრევენციას, რომლებიც თან ახლავს პანდემიის პირობებში მონაცემთა უსაფრთხოებას

1. პერსონალური მონაცემები

მონაცემები არის ნებისმიერი სახის ინფორმაცია, რომელიც ეხება იდენტიფიცირებად ან იდენტიფიცირებულ ფიზიკურ პირს, მაგალითად ეს შეიძლება იყოს პირადი ნომერი, საბანკო ანგარიშები, სახელი და გვარი, ელექტრონული ფოსტის მისამართი, ინფორმაცია სამუშაო ადგილისა და ოჯახური მდგომარეობის შესახებ, ინფორმაცის ჯანმრთელობის მდგომარეობის შესახებ და სხვ. არსებობს ე.წ ,,მგრძნობიარე'' მონაცემები, რომლებიც გამოხატავენ პოლიტიკურ მოსაზრებებს რელიგიურ, ფილოსოფიურ მრწამსს, მასში შედის ასევე ეთნიკური ან რასობრივი წარმოშობის ამსახველი მონაცემები. ასევე ჯანმრთელობის მდგომარეობის და გენეტიკური ინფორმაციის შესახებ. პირად მონაცემებს განეკუთვნება, ასევე, ინფორმაცია სექსუალური ცხოვრების შესახებ, პროფესიული კავშირის წევრობის, ნასამართლეობის და ადმინისტრაციული პატიმრობის შესახებ.

ინტერნეტ სივრცეში არაინფორმირებული პირის გაუაზრებელმა ქმედებამ შესაძლოა საფრთხე შეუქმნას მომხმარებლის პირადი ცხოვრების ხელშეუხებლობას, შესაძლოა ითქვას რომ COVID- 19 მა განსაკუთრებული გავლენა მოახდინა ისეთ სფეროებზე როგორიცაა: ჯანდაცვა, კერძოდ ჯანმრთელობასთან დაკავშირებულ მონაცემებზე, ასევე ონლაინ მომსახურებაზე, კერძოდ, ონლაინ შესყიდვების და საბანკო მომსახურების დროს მომხმარებლები გასცემენ ისეთ ინფორმაციას, როგორიცაა ელექტრონული ფოსტა, პირადი ნომერი, სახელი და გვარი,

საბანკო ანგარიშები, ბარათის ნომერი, ტელეფონის ნომერი. პანდემიამ ასევე გავლენა მოახდინა საგანმანათლებლო დაწესებულებაში პერსონალური მონაცემების დაცვაზე და ზოგადად ინტერნეტ სივრცეში არსებულ მონაცემებზე.

1.1. ჯანმრთელობასთან დაკავშირებული მონაცემები

პანდემიის პერიოდში შესაძლოა მოხდეს პაციენტის მონაცემების გასაჯაროება, მაგალითად მონტენეგროში პირველი კოვიდინფიცირებული პაციენტების მონაცემები სოციალურ ქსელში გაასაჯაროვეს, კერძოდ, მათი ვინაობა და ფოტოსურათები, რასაც შედეგად მოჰყვა მათი ოჯახის წევრების დევნა საზოგადოების მიერ.

ბევრ ქვეყანაში მთავრობის წარმომადგენლებმა და კერძო პირებმა გამოაქვეყნეს ჯანმრთელობის მონაცემები, რითაც შეეცადნენ საზოგადოების ინფორმირებას ჰქონდათ თუ არა მათ კონტაქტი ინფიცირებულ ინდივიდთან. მათ შეძლეს ინფიცირებული პირებისა და მათი ოჯახების იდენტიფიცირება. ინფორმაციის გამოქვეყნებამ საფრთხე შეუქმნა საზოგადოებრივ წესრიგს და უსაფრთხოებას, გამოიწვია მათი დისკრიმინაცია.

კოვიდ 19 პანდემიის დროს, ინფექციის დიაგნოზის სირთულის გამო შეიმუშავეს ტექნოლოგიური ინიციატივები, რათა შესაძლებელი ყოფილიყო მოქალაქეთა სიმპტომების, გადაადგილებისა და კონტაქტების კონტროლი, რაც ინფექციის მეთვალყურეობისთვის აუცილებელი ელემენტს წარმოადგენდა. მაგალითად, დიდ ბრიტანეთში სამთავრობო სააგენტოები თანამშრომლობდნენ ტექნოლოგიურ კომპანიებთან, რათა შეექმნათ კოვიდ 19 ის საცავი, რომელიც ინახავდა პაციენტის მონაცემებს. აღნიშნული კომპანიები დაიქირავა ჯანმრთელობის ეროვნულმა სამსახურმა(NHS), რათა ერთობლივად შეემუშავებინათ პროგნოზირების მოდელები. ინიციატივამ გაამართლა იმ თვალსაზრისით, რომ მისი საშუალებით ხდებოდა საჭიროებისამებრ, დროულად ინფორმაციის მიწოდება, ჯანდაცვის მომსახურების, ჰოსპიტალიზაციის მონაცემებისა და ინტენსიური თერაპიის ხელმისაწვდომობის შესახებ. მიუხედავად მნიშვნელობისა, ინიციატივამ საზოგადოებაში უკმაყოფილება გამოიწვია, მოქალაქეთა პირადი ინფორმაციის, კონფიდენციალურობისა და მონაცემთა დაცვის თვალსაზრისით. თუმცა, ჯანმრთელობის ეროვნულმა სამსახურმა (NHS), განაცხადა, რომ საცავში არსებული მონაცემები კონფიდენციალურია, ანონიმურია, ინახება მთავრობის მონაცემთა ბაზაში და ექვემდებარება მკაცრ კონტროლს მონაცემთა დაცვის კანონმდებლობით.[1]

მიუხედავად იმისა, რომ ჯანმრთელობის დაცვისა და ელექტრონული ჯანდაცვის გამოყენებამ, შესაძლოა, ჯანდაცვის სფეროს უკეთ მუშაობას და ვირუსთან ეფექტურად ბრძოლას შეუწყოს ხელი, მაგრამ ასეთ დროს შესაძლოა საფრთხე შეექმნას მოქალაქის პირად მონაცემებს.

1.2 თანამშრომელთა მონაცემების დაცვა

COVID-19 მა განსაკუთრებული გავლენა მოახდინა, ასევე, დამსაქმებლების მიერ თანამშრომლების მონაცემების დაცვაზე, კერძოდ, კითხვის ნიშნის ქვეშ დადგა საკითხი თუ რა

[1]ს.ა.აარონსონი, პ.ლებლონდი, "Your personal data is being used to fight COVID-19, but the data market needs transparency". 2020 წლის 20 აპრილი https://thehill.com/opinion/cybersecurity/493628-your-personal-data-used-to-fight-covid-19-data-market-transparency [უ.გ. 05.01.2021].

პერსონალური ინფორმაცია სჭირდებათ დამქირავებლებს თანამშრომლების შესახებ, ვირუსის გავრცელების შეზღუდვის მიზნით.

დამსაქმებლებმა პირველ რიგში უნდა განასხვაონ პირადი მონაცემებისა და ჯანმრთელობის მონაცემების კონცეფციები, რადგან თანამშრომლების ჯანმრთელობის მონაცემების დამუშავების შემთხვევაში უნდა მიიღონ დამატებითი და უფრო მკაცრი ზომები. მონაცემთა დაცვის ზოგადი რეგულაციის(GDPR)-ის თანახმად პირადი მონაცემები მოიცავს ნებისმიერ ინფორმაციას, რომელიც შესაძლოა პირდაპირ ან არაპირდაპირ დაუკავშირდეს თანამშრომელს, ხოლო ჯანმრთელობასთან დაკავშირებული მონაცემები ნიშნავს პერსონალურ მონაცემებს, რომლებიც დაკავშირებულია პირის ფიზიკურ ან ფსიქიკურ ჯანმრთელობასთან.

მიზანშეწონილია ვივარაუდოთ, რომ თანამშრომლების მონაცემების შეგროვება COVID- 19 ის აფეთქების დროს უნდა შეესაბამებოდეს თანამშრომელთა ინდივიდულაურ ინტერესებს, მათი კეთილდღეობის თავლსაზრისით. დამსაქმებლებს შეუძლიათ დაამუშავონ თანამშრომლების ჯანმრთელობის მონაცემები მხოლოდ გამონაკლის შემთხვევებში, ვინაიდან ეს მონაცემები მიეკუთვნება პერსონალური მონაცემის სპეციალურ კატეგორიას და მოითხოვს სპეციფიკურ დაცვას. [2]

COVID- 19 ის ვითარებით განსაკუთრებით ისარგებლეს ჰაკერებმა, მათ გზა გაეხსნათ თავიანთი მიზნების განსახორციელებლად. ასეთ ვითარებაში კომპანიებმა განსაკუთრებული ყურადღება უნდა მიაქციონ ახალ თანამშრომლებს ან მათ ვისაც არ აქვს დისტანციური მუშაობის გამოცდილება. ჰაკერები იყენებენ ხალხის შიშსა და გაურკვევლობას, რომელიც ვირუსის პერიოდს თან ახლავს, მათ შესაძლოა გამოგზავნონ ცრუ ინფორმაცია, ვირუსის შესახებ საზოგადოების ყურადღების მისაქცევად, რომელიც რეალურად შესაძლოა საფრთხის შემცველი იყოს, ამ მეთოდით ისინი წვდომას ახდენენ მოწყობილობებზე, რათა შეძლონ ფინანსური ინფორმაციის მოპარვა.

1.3 მონაცემების დაცვა განათლების სფეროში

ვირუსმა ასევე გავლენა მოახდინა განათლების სფეროზე, როგორც საყოველთაოდ ცნობილია COVID-19 ის პერიოდში უნივერსიტეტებმა და სკოლებმა საგანმანათლებლო დაწესებულებებში შეაჩერეს მუშაობა და გადავიდნენ ონლაინ პლატფორმებზე, სადაც ასევე ხდება პერსონალური მონაცემების დამუშავება, მათ შორის, სტუდენტებისა და პროფესორების ფოტოსურათების, ელექტრონული ფოსტის, სახელებისა და გვარების. ასეთ შემთხვევაში მნიშვნელოვანია მონაცემთა დამუშავების სათანადო იურიდიული საფუძვლების არჩევა, განსაკუთრებით მაშინ, როდესაც ასეთ პროცესში ბავშვები არიან ჩართული.

1.4 მონაცემების დასაცავად გატარებული ღონისძიებები

COVID- 19 ის პერიოდში სხვადასხვა ქვეყნებმა მისი გავლენის შესაჩერებლად გაატარეს ღონისძიებები, რომლების ვირუსის პრევენციის მიზნით შესაძლოა ეფექტური აღმოჩნდა, თუმცა, უარყოფითი გავლენა მოახდინა მონაცემთა უსაფრთხოებაზე, მაგალითად, ირანის

[2]ს.სუდერ,"Processing employees' personal data during the Covid-19 pandemic",2020 წლის 16 დეკემბერი, https://journals.sagepub.com/doi/full/10.1177/2031952520978994 [უ. გ. 05.01.2021].

მოქალაქეებს შესთავაზეს, რომ გადმოეწერათ აპი, რომლის საშუალებითაც გაიგებდნენ დაინფიცირებული იყვნენ თუ არა კორონავირუსით, მისი ჩამოტვირთვა შეეძლოთ ირანული აპლიკაციის მაღაზიიდან café Bazaar. რა თქმა უნდა, აპლიკაციამ, რელურად, ვერ უთხრა მოსახლეობას იყვნენ თუ არა ინფიცირებული, მაგრამ მოხდინა გავლენა მათ პერსონალურ მონაცემებზე, მათ შორის მათ მისამართებზე, დაბადების თარიღებზე, სახელებსა და გვარებზე და შეძლო მოქალაქეების ადგილმდებარეობაზე თვალყურის დევნებაც კი.[3]

ასეთი შემთხვევისგან განსხვავებით ავსტრალიის კომისრის ოფისი(OAIC)-ი აქვეყნებს ინფორმაციას CovidSafe აპლიკაციის შესახებ, რომელიც ახდენს ინფიცირებული ადამიანების იდენტიფიცირებას, თუმცა აპი ნებაყოფლობითია. კონფიდენციალურობის შესახებ კანონის თანახმად დანაშაულია ნებისმიერი პირის, ორგანიზაციის ან სამთავრობო სააგენტოს მიერ აპის ჩამოტვირთვის მოთხოვნა. აპლიკაცია ინახავს მონაცემებს 21 დღის განმავლობაში, შემდეგ კი ავტომატურად წაშლის მას. აპი არ აგროვებს პირის პერსონალურ ინფორმაციას, მისი კონფიდენციალურობის დაცვას კი ახორციელებს ავსტრალიის კომისრის ოფისი(OAIC), რომელსაც აქვს დამოუკიდებელი სამეთვალყურეო ფუნქცია კონფიდენციალურობის შესახებ კანონის შესაბამისად, აქტიურად არეგულირებს კონიდენციალურობის აქტის დაცვას CovidSafe აპთან დაკავშირებით. [4]

ციფრულ საზოგადოებაში სადაც სულ უფრო მეტი ადამიანი ზრუნავს მონაცემების კონფიდენციალურობის დაცვაზე და სადაც უფრო მეტი ციფრული მომსახურება და პირადი ინფორმაცია წარმოადგენს მნიშვნელოვან ელემენტებს ყოველდღიურ ცხოვრებაში. მისი დაცვის საიმედო მექანიზმია ე.წ. eHealth მექანიზმი და კეთილდღეობის სერვისები, რომლებიც დაფუძნებულია კონფიდენციალურობის მიხედვით ტექნოლოგიებზე და Blockchain ქსელებზე, რომლებიც გამოიყენება მომხმარებლის პირადი მონაცემების კონტროლის უზრუნველსაყოფად.[5]

მსოფლიოს სხვადასხვა რეგიონებმა და სამთავრობო დაწესებულებებმა ხელი შეუწყვეს სხვადასხვა რეგულაციების მიღებას, მათ შორის ევროკომისიის მიერ შექმნილმა მონაცემთა დაცვის ზოგადმა რეგულაციამ(GDPR) განსაზღვრა მონაცემთა დაცვის ზოგადი მახასიათებლები ციფრული სერვისებისთვის, კერძოდ, 1. გამჭვირვალობა- კეთილდღეობის ყველა სერვისმა პერსონალური მონაცემები უნდა დაამუშავოს მონაცემთა მფლობელების მიმართ გამჭვირვალედ. 2.დანიშნულების შეზღუდვა- პერსონალურ მონაცემებზე წვდომა და დამუშავება შესაძლებელია მხოლოდ ლეგიტიმური და შემზღუდველი მიზნებისთვის რომელიც მკაფიოდ ავტორიზებულია მომხმარებლების მიერ. 3. მონაცემთა მინიმიზაცია- დამუშავებული პირადი მონაცემები არ უნდა იყოს გადაჭარბებული კეთილდღეობის სერვისების მიზნებისათვის. 4. სიზუსტე- კეთილდღეობის სერვისებმა უნდა უზრუნველყონ პერსონალურ მონაცემთა სიზუსტით დამუსავება და შედეგის განახლება თუ ეს შესაძლებელი. 5. შენახვის შეზღუდვა- ოპერსონალური მონაცემები არ უნდა იყოს შენახული იმაზე დიდხანს ვიდრე ეს მომსახურების მიზნის მისაღწევადაა საჭირო. 6. მთლიანობა და

[3] დ. გილბერტი, „Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People", 2020 წლის 14 მარტი, https://www.idp.al/wp-content/uploads/2020/06/Guidelines_on_the_processing_of_personal_data_in_specific_sectors_in_the_context_of_measures_against_COVID-19. pdf. [უ. გ. 03.01.2021].

[4] "COVID-19 advice and guidance", https://journals.sagepub.com/doi/full/10.1177/1550147720912110 [უ. გ. 09.01.2021].

[5] თ. რობლესი, "Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design", 2020 წლის 5 მაისი, https://journals.sagepub.com/doi/full/10.1177/1550147720912110 [უ. გ. 09.01.2021].

კონფიდენციალურობა- პერსონალური მონაცემები ყოველთვის უნდა იყოს უსაფრთხოდ დამუშავებული, გადაცემული და შენახული.

1.5 პერსონალური მონაცემების დაცვა საქართველოში

საქართველოში პერსონალურ მონაცემთა დაცვას არეგულირებს ,,პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი'' , რომელიც 2012 წლის 1-ლი მაისიდან შევიდა ძალაში. კანონის მე-4 მუხლში მოცემულია მონაცემთა დამუშავების პრინციპები, რომლის მიხედვითაც მონაცემები უნდა დამუშავდეს სამართლიანად, კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად, მხოლოდ მკაფიოდ განსაზღვრული კანონიერი მიზნებისთვის, დაუშვებელია მონაცემთა შემდგომ დამუშავება სხვა თავდაპირველ მიზანთან შეუთავსებლად. ასევე, მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. კანონში ასევე გათვალისწინებულია ადმინისტრაციული პასუხისმგებლობა იმ შემთხვევაში თუ დარღვეული იქნება კანონით გათვალისწინებული საფუძვლების გარეშე მონაცემთა დამუშავება, რაც იწვევს გაფრთხილებას ან დაჯარიმებას 500 ლარის ოდენობით.[6] ასევე მონაცემთა დამუშავების პრინციპების დარღვევა გამოიწვევს გაფრთხილებას ან დაჯარიმებას 500 ლარის ოდენობით. რაც შეეხება განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას კანონით გათვალისწინებული საფუძვლების გარეშე გამოიწვევს დაჯარიმებას 1000 ლარის ოდენობით.

ასევე, პერსონალური მონაცემების უკანონოდ გამჟღავნებისას ზიანის ანაზღაურების წესს იცნობს საქართველოს სისხლის სამართლის საპროცესო კოდექსი, პირი რომელსაც ზიანი მიადგება მისი პირადი ცხოვრების შესახებ პერსონალური მონაცემების უკანონოდ გამჟღავნებით აქვს საქართველოს კანონმდებლობით დადგენილი წესით ზიანის სრულად ანაზღაურების უფლება.[7]

ზემოთ აღნიშნული ქვეყნებისგან განსხვავებით, საქართველოში COVID- 19-ს მოსახლეობის პირად ცხოვრებაზე, ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის უფლებების არსებითი შეზღუდვა არ მომხდარა. თუმცა, როდესაც სულ უფრო მეტად ხდება პერსონალური მონაცემების დამუშავება, საჭირო ხდება მისი დაცვა და საზოგადოების ინფორმირება, ამას კი საქართველოში ახორციელებს სახელმწიფო ინსპექტორის სამსახური, რომლის ერთ-ერთი ძირითადი ფუნქციაა საქართველოში პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულებაზე ზედამხედველობა და მონაცემთა დამუშავების კანონიერებაზე კონტროლი. მისი საშუალებით ხორციელდება საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების კანონიერების შემოწმება (ინსპექტირება); მონაცემთა დაცვასთან დაკავშირებით მოქალაქეთა განცხადებების განხილვა; საჯარო და კერძო დაწესებულებებისათვის, აგრეთვე ფიზიკური პირებისათვის მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციის გაწევა.

25. რეკომენდაციები

იმისათვის, რომ არ მოხდეს პერსონალური ინფორმაციის არაკანონიერად დამუშავება, ინტერნეტმომხმარებლებმა უნდა გაითვალისწინონ რამდენიმე რეკომენდაცია:

[6] მუხლი 45, ,,საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ''. 28 დეკემბერი, 2011.
[7] მუხლი 7, ნაწილი 3, ,,საქართველოს სისხლის სამართლის საპროცესო კოდექსი''. 9 ოქტომბერი, 2009.

- სასურველია, რომ მონაცემების დაცვის მიზნით მომხმარებელმა გამოიყენოს უნიკალური და რთული პაროლი, რომელიც შედგება მრავალფეროვანი სიმბოლოებისგან.
- არ გამოიყენოს ერთი და იგივე მომხმარებლის სახელი და პაროლი სხვადასხვა ინტერნეტრესურსით სარგებლობისას, ასეთ შემთხვევაში თუ ერთი ანგარიში დადგება საფრთხის ქვეშ იგივე ემუქრება მის სხვა ანგარიშებსაც.
- პერსონალურ მონაცემთა შეგროვება ხდება მომხმარებლის თანხმობის საფუძველზეც, როდესაც ვებგვერდზე რეგისტრაციისას მომხმარებელი მონიშნავს სპეციალურ ველს, რომელშიც მოცემულია ინფორმაცია პერსონალურ მონაცემთა გამოყენების წესების შესახებ, ასეთ დროს მნიშვნელოვანია რომ მომხმარებელი თანხმობამდე გაეცნოს მონაცემთა დამუშავების წესებს რომელიც მოცემულია კომფიდენციალურობის შესახებ განაცხადში(privacy police).
- მომხმარებელს უფლება აქვს მოითხოვოს თავისი მონაცემების წაშლა თუ ისინი არასწორია ან მათი გამოყენების მიზანი აღარ არსებობს, ასევე ისეთ შემთხვევაში თუ მომხმარებელი ჩათვლის, რომ ამუშავებენ მცდარ, მოძველებულ ან არაზუსტ ინფორმაციას აქვს უფლება, რომ მოითხოვოს ამ ინფორმაციის წაშლა, დამატება, შეცვლა ან განადგურება.[8]

დასკვნა

ნაშრომში, კვლევის შედეგად დგინდება, რომ COVID-19 ის პერიოდში ინტერნეტი გლობალურ საკომუნიკაციო და საინფორმაციო საშუალებად იქცა, ამ პერიოდში უამრავი ადამიანი ახორციელებს კომუნიკაციას, ელექტრონულ შესყიდვებს, იღებს სხვადასხვა სახის მომსახურებას და იხდის გადასახადებს. ასეთ ვითარებაში COVID- 19-მა განსაკუთრებული გავლენა მოახდინა მონაცემთა უსაფრთხოებაზე.

ნაშრომში ჩანს, რომ პანდემიამ გავლენა მოახდინა განსაკუთრებით ჯანმრთელობის მონაცემებზე, რადგან ვირუსის დროს ადამიანების ექიმთან ვიზიტი გახშირდა, ჯანმრთელობის მონაცემების გავრცელებამ კი ზოგიერთ ქვეყანაში გამოიწვია ადამიანების დისკრიმინაცია, რადგან როგორც ვიცით კორონა ვირუსი გადამდები დაავადებაა რაც ცალსახად საზოგადოებაში შიშს იწვევს. ნაშრომიდან დგინდება, რომ ვირუსის პრევენციის მიზნით ქვეყნებმა შეიმუშავეს ტექნოლოგიური ინიციატივები, რათა შესაძლებელი ყოფილიყო მოქალაქეთა სიმპტომების, გადაადგილებისა და კონტაქტების კონტროლი, რაც ინფექციის მეთვალყურეობისთვის აუცილებელი ელემენტს წარმოადგენდა.

საბოლოოდ შეიძლება ითქვას, რომ მონაცემთა უსაფრთხოებასთან დაკავშირებული პრობლემა განსაკუთრებით გაიზარდა COVID-19 ის პერიოდში, მისი პრევენციის ერთადერთი საშუალებაა საზოგადოების ინფორმირება ამ საკითხთან დაკავშირებით, მაგალითად, მუდმივი ტრენინგების საშუალებით. საზოგადოებას უფრო მეტი ინფორმაცია უნდა ჰქონდეს საკუთარი პერსონალური მონაცემების დაცვის შესახებ, იცოდნენ თუ რისი უფლება აქვთ მათ.

[8] „რეკომენდაციები ინტერნეტსივრცეში პერსონალურ მონაცემთა დაცვის შესახებ", https://personaldata.ge/cdn/2018/12/Online-Privacy-Rec-for-Users-.pdf [უ.გ.12.01.2021].

ბიბლიოგრაფია

1. Personal Data Protection Act. https://www.riigiteataja.ee/en/eli/512112013011/consolide [უკანასკნელად გადამოწმდა 03.01.2021];
2. Montenegrin Coronavirus Patients' Identities Exposed Online. https://balkaninsight.com/2020/03/18/montenegrin-coronavirus-patients-identities-exposed-online/ [უკანასკნელად გადამოწმდა 07.01.2021];
3. https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf [უკანასკნელად გადამოწმდა 29.12.2020];
4. Your personal data is being used to fight COVID-19, but the data market needs transparency. https://thehill.com/opinion/cybersecurity/493628-your-personal-data-used-to-fight-covid-19-data-market-transparency [უკანასკნელად გადამოწმდა 05.01.2021];
5. Processing employees' personal data during the Covid-19 pandemic. https://journals.sagepub.com/doi/full/10.1177/2031952520978994 [უკანასკნელად გადამოწმდა 05.01.2021];
6. How to stay safe online during the COVID-19 crisis. https://www.amnesty.org/en/latest/news/2020/04/stay-safe-online-during-the-covid-19-crisis/ [უკანასკნელად გადამოწმდა 03.01.2021];
7. https://www.idp.al/wpcontent/uploads/2020/06/Guidelines_on_the_processing_of_personal_data_in_specific_sectors_in_the_context_of_measures_against_COVID-19.pdf. [უკანასკნელად გადამოწმდა 03.01.2021];
8. Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People. https://www.vice.com/en/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people [უკანასკნელად გადამოწმდა 07.01.2021];
9. https://www.vice.com/en/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people [უკანასკნელად გადამოწმდა 02.01.2021];
10. COVID-19 advice and guidance. https://www.oaic.gov.au/updates/news-and-media/covid-19/ [უკანასკნელად გადამოწმდა 06.01.2021];
11. Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design. https://journals.sagepub.com/doi/full/10.1177/1550147720912110 [უკანასკნელად გადამოწმდა 09.01.2021];
12. Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. https://journals.sagepub.com/doi/full/10.1177/2053951720976680 [უკანასკნელად გადამოწმდა 09.01.2021];
13. https://personaldata.ge/ka/organization [უკანასკნელად გადამოწმდა 10.01.2021];
14. https://personaldata.ge/cdn/2018/12/Online-Privacy-Rec-for-Users-.pdf [უკანასკნელად გადამოწმდა 12.01.2021];
15. https://matsne.gov.ge/ka/document/view/1561437?publication=22 [უკანასკნელად გადამოწმდა 12.01.2021].

Bibliography

1. Personal Data Protection Act. https://www.riigiteataja.ee/en/eli/512112013011/consolide [Last seen 03.01.2021];
2. Montenegrin Coronavirus Patients' Identities Exposed Online. https://balkaninsight.com/2020/03/18/montenegrin-coronavirus-patients-identities-exposed-online/ [Last seen 07.01.2021];
3. https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf [Last seen 29.12.2020];
4. Your personal data is being used to fight COVID-19, but the data market needs transparency. https://thehill.com/opinion/cybersecurity/493628-your-personal-data-used-to-fight-covid-19-data-market-transparency [Last seen 05.01.2021];
5. Processing employees' personal data during the Covid-19 pandemic. https://journals.sagepub.com/doi/full/10.1177/2031952520978994 [Last seen 05.01.2021];
6. How to stay safe online during the COVID-19 crisis. https://www.amnesty.org/en/latest/news/2020/04/stay-safe-online-during-the-covid-19-crisis/ [Last seen 03.01.2021];
7. https://www.idp.al/wp-content/uploads/2020/06/Guidelines_on_the_processing_of_personal_data_in_specific_sectors_in_the_context_of_measures_against_COVID-19.pdf. [Last seen 03.01.2021];
8. Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People. https://www.vice.com/en/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people [Last seen 07.01.2021];
9. https://www.vice.com/en/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people [Last seen 02.01.2021];
10. COVID-19 advice and guidance. https://www.oaic.gov.au/updates/news-and-media/covid-19/ [Last seen 06.01.2021];
11. Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design. https://journals.sagepub.com/doi/full/10.1177/1550147720912110 [Last seen 09.01.2021];
12. Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. https://journals.sagepub.com/doi/full/10.1177/2053951720976680 [Last seen 09.01.2021];
13. https://personaldata.ge/ka/organization [Last seen 10.01.2021];
14. https://personaldata.ge/cdn/2018/12/Online-Privacy-Rec-for-Users-.pdf [Last seen 12.01.2021];
15. https://matsne.gov.ge/ka/document/view/1561437?publication=22 [Last seen 12.01.2021].

დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა

ლიკა აბესაძე,
თბილისის სახელმწიფო უნივერსიტეტი

აბსტრაქტი

ესე ,,დისტანციური სწავლების დროს სკოლის მოსწავლეების პერსონალური მონაცემების დაცვა“ შეისწავლის დისტანციურ სწავლებასთან დაკავშირებულ პრობლემატურ საკითხებს მოსწავლეთა პერსონალური მონაცემების უსაფრთხოების თვალსაზრისით, რადგან ონლაინ სწავლების პირობებში უფრო და უფრო იმატებს არაკანონიერი გზით პერსონალური მონაცემების მოპოვების რისკი. ტერმინი ,,პერსონალური მონაცემი“ განმარტებულია ,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში, როგორც ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს[1]. საქართველოს საკონსტიტუციო სასამართლომ კი განმარტა, რომ ,,პერსონალურ მონაცემთა ხელშეუხებლობა არის ინდივიდის ავტონომიურობის, დამოუკიდებელი განვითარების, მისი ღირსების დაცვის წინაპირობა“.[2]

პერსონალურ მონაცემთა დაცვის საკითხი განსაკუთრებით აქტუალურია პანდემიის პირობებში, როდესაც სკოლის მოსწავლეებს აქტიურად უწევთ ტექნოლოგიების გამოყენება გაკვეთილებზე დასწრების მიზნით. სამწუხაროდ, ხშირად სოციალურ ქსელებში ვრცელდება ონლაინ სასწავლო პროცესის ამსახველი ფოტო-ვიდეო მასალა, რომელიც წარმოადგენს პირის პერსონალურ მონაცემებს, ეს კი უნდა იქნეს გათვალისწინებული მათი გასაჯაროებისას. არასრულწლოვნის მონაცემების ინტერნეტში ყველასთვის ხელმისაწვდომი ფორმით გასაჯაროებამ შესაძლოა არასასურველი ზეგავლენა მოახდინოს არასრულწლოვანზე.[3] უნდა გავითვალისწინოთ ისიც, რომ არასრულწლოვნების შემთხვევაში პერსონალურ მონაცემთა დაცვის საკითხი უდიდესი მნიშვნელობის მატარებელია, რადგან სკოლის მოსწავლეებს არ აქვთ გაცნობიერებული პერსონალური მონაცემების მნიშვნელობა და ის, თუ როგორ უნდა დაიცვან თავი პერსონალური მონაცემების გამჟღავნების საფრთხისაგან. ამიტომ მათ ამ სფეროში სპეციფიკური დაცვა ესაჭიროებათ.[4]

მოცემულ ესეში მიმოხილულია პერსონალური მონაცემების დაცვის მნიშვნელობა და მოცემულია მისი ანალიზი. ასევე აშშ-სა და ევროკავშირის მაგალითზე განხილულია, თუ როგორია ბავშვთა პერსონალურ მონაცემთა უსაფრთხოების საკანონმდებლო რეგულირება საზღვარგარეთის ქვეყნებში, მათი გამოყენება პრაქტიკაში. უცხო ქვეყნების პრაქტიკა კი შედარებული იქნება საქართველოს მაგალითთან და დეტალურად იქნება გაანალიზებული სახელმწიფო ინსპექტორის სამსახურის როლი მოსწავლეთა პერსონალური მონაცემების დაცვის საკითხში..

[1] ,,პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი“ <matsne.gov.ge> [20.12.2020].
[2] საქართველოს საკონსტიტუციო სასამართლოს 2009 წლის 10 ივნისის N1/2/458 განჩინება საქმეზე, ,,საქართველოს მოქალაქეები - დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ“.
[3] სახელმწიფო ინსპექტორის სამსახური https://personaldata.ge [უ.გ.9.01.2021].
[4] S. Livingstone, Children: a special case for privacy? http://eprints.lse.ac.uk/ [უ.გ.19.12.2020].

ასევე, ესეში პასუხი გაეცემა შემდეგ კითხვებს:

1. რამდენად ეფექტიანად ხდება 13 წლამდე ბავშვთა პერსონალური მონაცემების დაცვა COPPA[5]-ს მიხედვით? და საჭიროებს თუ არა დამატებით რეგულირებას 13-18 წლის მოსწავლეთა პერსონალური მონაცემების დაცვა?
2. რა ვითარებაა საქართველოში სკოლის მოსწავლეთა პერსონალურ მონაცემთა დაცვის კუთხით და როგორ უნდა უზრუნველყოთ ბავშვთა დაცვა პერსონალური მონაცემების გამჟღავნებისგან ?

დაბოლოს, ესეში მოცემულ პრობლემებისა და საფრთხეების ანალიზის შედეგად, კონკრეტულ მაგალითებზე დაყრდნობით შევეცდები განვსაზღვრო პრობლემის გადაჭრის ჩემეული გზები და ის ნაბიჯები, რომლებიც, სასურველია, გადაიდგას სკოლის მოსწავლეთა პერსონალური მონაცემების დაცვის თვალსაზრისით.

საკვანძო სიტყვები: პერსონალური მონაცემები, დისტანციური სწავლება, სახელმწიფო ინსპექტორის სამსახური.

Abstract

The essay "Protecting the Personal Data of Schoolchildren during Distance Learning" deals with issues related to distance learning in terms of the security of students' personal data, as the risk of obtaining personal data illegally nowadays increases. The term "personal data" is defined in the Personal Data Protection Act as any information relating to an identified or identifiable person. The Constitutional Court of Georgia clarified that "the inviolability of personal data is a precondition for the autonomy of independent development of the individual and protection of his dignity."

The issue of personal data protection is especially relevant during pandemic, when school children are actively using technology to attend classes. Unfortunately, the photo-video material of the online learning process is often spread on social networks. Disclosure of personal data on the Internet in an accessible form may have an adverse effect on the child. Personal data protection is of paramount significance, as school children do not realize the importance of personal data and how to protect themselves from the dangers of disclosing personal data. Therefore, they need specific protection in this area.

This essay reviews the importance of personal data protection and analyzes it. The example of the US and the EU also shows the legal regulation of the personal data security of children in foreign countries, their application in practice. The practice of foreign countries will be compared with the example of Georgia and the role of the State Inspector's Office will be analyzed.

The essay will also answer the following questions:

1. How effective is the protection of personal data of children under 13 according to COPPA? And does it require additional regulation to protect the personal data of 13-18 years old students?

[5] Children's Online Privacy Protection Rule, https://www.ftc.gov/ [უ.გ.19.12.2020].

2. What is the situation regarding the protection of personal data of schoolchildren in Georgia and how should we ensure the protection of children from the disclosure of personal data?

Finally, as a result of the analysis of the problems and threats presented in the essay, based on specific examples, I will try to identify my own ways of solving the problem and the steps that should be taken in terms of protecting the personal data of school children.

Keywords: personal data, distance learning, State Inspector Service.

შესავალი

დღევანდელ დღეს, პანდემიის პირობებში, განსაკუთრებით აქტუალური გახდა მოსწავლეთა პერსონალური მონაცემების დაცვის საკითხი. 160-ზე მეტ სახელმწიფოში სკოლები დაიხურა და მსოფლიოს მოსწავლეთა 87% განათლებას დისტანციურად იღებს. განათლების მისაღებად ტექნოლოგიების აქტიურად გამოყენების საჭიროება წარმოშობს მთავრობებისა და სკოლების ვალდებულებას, რომ ზომები მიიღონ მოსწავლეთა პერსონალური მონაცემების უკანონო დამუშავებისგან დაცვის მიზნით.[6]

მოსწავლეების განათლებასთან დაკავშირებით მონაცემები ნაკლებად დაცულია, ვიდრე მათ ჯანმრთელობასთან დაკავშირებით ცნობები. ბევრ სახელმწიფოს აქვს რეგულაციები, რათა არ მოხდეს ჯანმრთელობასთან დაკავშირებული ისეთი მონაცემის გამჟღავნება, რომელიც უზრუნველყოფს პიროვნების იდენტიფიცირებას[7]. თუმცა განათლებასთან დაკავშირებული მონაცემები ბევრად უფრო დაუცველია, რადგან სახელი და გვარი, სახლის მისამართი, გამოსახულება და სხვა პირადი დეტალები შეიძლება ადვილად გამჟღავნდეს ონალინ სივრცეში და, შესაბამისად, ავნოს ბავშვებსა და მათ ოჯახებს, ვინაიდან ბევრ სახელმწიფოს არ აქვს ბავშვთა პერსონალური მონაცემების დაცვის შესახებ კანონმდებლობა.

აქედან გამომდინარე, დღევანდელი რეალობიდან გამომდინარე, მნიშვნელოვანია გავაანალიზოთ, თუ რა გამოწვევებთან არის დაკავშირებული მოსწავლეთა პერსონალური მონაცემების დაცვა ონლაინ სივრცეში, რა პრევენციული ღონისძიებების გატარებაა შესაძლებელი და რა საკანონმდებლო ცვლილებები უნდა განხორციელდეს არასრულწლოვანთა საუკეთესო ინტერესების დაცვის მიზნით.

1. სკოლის მოსწავლეთა პერსონალური მონაცემების დაცვასთან დაკავშირებული პრობლემები

COVID-19-ის შედეგად, სკოლის მოსწავლეები იძულებულნი გახდნენ, რომ განათლების მიღება სახლიდან გაეგრძელებინათ. რის შედეგადაც გაიზარდა ბავშვთა პერსონალური მონაცემების გავრცელების რისკი.

მოსწავლის პერსონალური მონაცემი შეიძლება იყოს ნებისმიერი ინფორმაცია მისი ოჯახური მდგომარეობის, აკადემიური მოსწრების შესახებ და ა.შ. აღნიშნული მონაცემების ხელყოფა მარტივადაა შესაძლებელი დისტანციური სწავლების პირობებში, ვინაიდან არსებობს მაგალითად, მოსწავლის ქულების სხვა პირთათვის ხელმისაწვდომობისა თუ ვიდეო

[6] Hye Jung Han, „As Schools Close Over Coronavirus, Protect Kids' Privacy in Online Learning ", https://www.hrw.org/news [უ.გ.9.01.2021].
[7] „Preliminary Opinion 8/2020 on the European Health Data Space", https://edps.europa.eu/ [უ.გ. 9.01.2021].

ჩანაწერების გავრცელების შესაძლებლობა. ფიზიკური პირის ვიდეო გამოსახულება წარმოადგენს გამოსახულებათა თანმიმდევრობის ჩანაწერს, რომელიც შეიძლება შეიქმნას ვიდეოთვალთვალის, ვიდეოკამერის, სმარტფონის ან სხვა ელექტრონული მოწყობილობის დახმარებით.[8] ონლაინ გაკვეთილები სხვადასხვა ონლაინ პლათფორმის(ZOOM, Teams და ა.შ.) საშუალებით მიმდინარეობს და, როგორც უკვე ზემოთ აღინიშნა, შესაძლებელია განხორციელდეს მოსწავლეთა გამოსახულების შემცველი ჩანაწერის შექმნა. აღნიშნული ჩანაწერის ინტერნეტ სივრცეში გავრცელება საზიანოა მოსწავლეებისთვის, რადგან შეიძლება ისინი შესაძლოა გახდნენ ბულინგის მსხვერპლნი, ან სხვა არასასურველი მოპყრობის ობიექტები.[9]

სახელმწიფო ინსპექტორის სამსახურის 2019 წლის ანგარიშში მითითებულია, რომ ამ ორგანოს მიერ შესწავლილ იქნა არასრულწლოვანთა პერსონალური მონაცემების დამუშავების 13 შემთხვევა როგორც კერძო, ისე საჯარო სექტორში და გამოვლინდა ადმინისტრაციული დარღვევების ფაქტები. დარღვევების უმეტესობა დაფიქსირდა სკოლაში, სადაც არასრულწლოვანთა დიდი რაოდენობით პერსონალური ინფორმაცია გროვდება.[10] აღნიშნულიდან გამომდინარე, რიგ შემთხვევაში სკოლამ შეიძლება ვერ უზრუნველყოს მოსწავლის პერსონალური მონაცემების დაცვა, რაც ასევე გამოწვევად რჩება დისტრანციური სწავლების დროს.

აღნიშნული პრობლემების აღმოსაფხვრელად უნდა განისაზღვროს, თუ რა ქმედითი ნაბიჯები უნდა გადაიდგას სახელმწიფოსა და მშობლების, ასევე სასწავლო დაწესებულებების მიერ, რადგან არასრულწლოვანთა პერსონალური მონაცემების დაცვის თვალსაზრისით, მნიშვნელოვანი პასუხისმგებლობა ეკისრებათ იმ დაწესებულებებსა და ორგანიზაციებს, სადაც თავს იყრის დიდი მოცულობისა და განსაკუთრებით სენსიტიური მონაცემები მათ შესახებ. უპირველესად, ესაა სკოლები (კერძო თუ საჯარო), სადაც არასრულწლოვანთა დიდი რაოდენობით პერსონალური ინფორმაცია გროვდება.[11] ხოლო იმისათვის, რომ მათ უზრუნველყონ მოსწავლეების დაცვა პერსონალური მონაცემების გამჟღავნებისა და ამით გამოწვეული ნეგატიური ზეგავლენისგან. ამისათვის, საჭიროა საზღვარგარეთის ქვეყნების პრაქტიკის გათვალისიწინება და, შესაბამისად, კვლევის შედარებითი მეთოდის გამოყენება.

2. პერსონალური მონაცემების დაცვა ევროკავშირის კანონმდებლობის მიხედვით

ბავშვთა საუკეთესო ინტერესების დაცვას დიდი მნიშვნელობა ენიჭება ევროკავშირის კანონმდებლობაში. მაგალითად, ევროკავშირის შესახებ ხელშეკრულების მესამე მუხლის მესამე პუნქტი შეეხება ბავშვთა უფლებების დაცვის მნიშვნელობას ევროკავშირის წევრი სახელმწიფოებისთვის.[12]

რაც შეეხება უშუალოდ ბავშვთა პერსონალურ მონაცემთა დაცვის კანონმდებლობასა და პრაქტიკას. ევროკავშირში არსებობს მონაცემთა დაცვის ზოგადი რეგულაცია(GDPR),

[8] პერსონალური მონაცემების ანბანი http://portal.personaldata.ge/ [უ.გ.9.01.2021].

[9] სახელმწიფო ინსპექტორის სამსახურის რეკომენდაცია COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით https://personaldata.ge/ [უ.გ.09.01.2021].

[10] ,,სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, სახელმწიფო ინსპექტორის სამსახური, 2019წ. გვ66.

[11] ,,სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, სახელმწიფო ინსპექტორის სამსახური, 2019წ. გვ68.

[12] მუხლი3(3), The Treaty on European Union, 1992.

რომელიც იცავს პერსონალურ მონაცემებს მიუხედავად იმისა, თუ რომელი ტექნოლოგიაა გამოყენებული მონაცემთა დამუშავებისათვის. არ აქვს მნიშვნელობა თუ სად არის მონაცემები შენახული: IT სისტემაში, ვიდეო მეთვალყურეობით, თუ ფურცელზე. ყველა შემთხვევაში, პერსონალური მონაცემი ექცევა GDPR-ის დაცვის ქვეშ.[13]

ამ დოკუმენტში ხაზგასმულია, რომ არასრულწლოვნები საჭიროებენ განსაკუთრებულ დაცვას, რადგან ისინი შესაძლოა არ ფლობდნენ საკმარის ინფორმაციას იმ უფლებების, რისკებისა და შედეგების შესახებ, რაც დაკავშირებულია მათი მონაცემების დამუშავებასთან.[14] GDPR-ის მეორე თავის მერვე მუხლის მიხედვით, ბავშვთა პერსონალური მომაცემების დამუშავება კანონიერია მაშინ, როდესაც 16 წლამდე არასრულწლოვნის კანონიერი წარმომადგენელი თანახმაა, ხოლო 16 წელს მიღწეული ბავშვის შემთვხვევაში, თავად ბავშვი გამოხატავს თანხმობას პერსონალური მონაცემების დამუშავებაზე.

პანდემიის პირობებში ევროპულმა კომისიამ შეიმუშავა ციფრული სტრატეგია, რომელიც მოიცავს შემდეგ სფეროებს:

- კორონავირუსის გავრცელებაზე მონიტორინგი
- დიაგნოზის, მკურნალობისა და ვაქცინების გამოკვლევა და განვითარება
- ევროპელების დაცულობის უზრუნველყოფა ონლაინ სივრცეში.[15]

მაშინ, როდესაც ევროკავშირის სახელმწიფოებში, სოციალურმა და ეკონომიკურმა აქტივობებმა ციფრულ სფეროში გადაინაცვლა, მოქალაქეები და ბიზნესები ინტერნეტზე გახდნენ დამოკიდებულნი. შესაბამისად, პანდემიამ ონლაინ სერვისების ფართო გამოყენებამდე მიგვიყვანა. ადამიანები მეტ დროს ხარჯავენ და დამოკიდებულნი არიან ციფრულ კომუნიკაციაზე. ამგვარი გაზრდილი ონლაინ აქტივობა ზრდის პერსონალური მონაცემების ბოროტად გამოყენების საშიშროებას. ეს საფრთხე ბავშვებსაც ეხებათ, რომლებიც ახლა მეტ დროს ატარებენ ონლაინ(შესაძლოა მეთვალყურეობის გარეშე). ეს განაპირობა დისტანციური სწავლების სპეციფიკამ, ვინაიდან საჭიროა ონალინ სივრცის გამოყენება განათლების მისაღებად და თანატოლებთან კავშირისათვის. თუმცა არ უნდა დაგვავიწყდეს, რომ ონლაინ სწავლება რისკებთანაა დაკავშირებული. ამ რისკების საპასუხოდ, EUROPOL-მა საერთაშორისო პარტნიორებთან ერთად შეიმუშავა ,,ონლაინ უსაფრთხოებასთან დაკავშირებული რჩევები მშობლებისა და მზრუნველებისთვის“[16], რათა დაეხმაროს ბავშვებს, რომ დაცულად გრძნობდნენ თავს დისტანციური სწავლების პირობებში.[17]

აღნიშნული რეკომენდაცია მნიშვნელოვანია სკოლის მოსწავლეთა პერსონალური მონაცემების დაცვის თვალსაზრისით, ვინაიდან მოუწოდებს მშობლებს, რომ მეტად იყვნენ ჩართულნი ბავშვის ციფრულ სამყაროში, ასწავლონ კონფინდენციალურობის დაცვის მნიშვნელობა, რეგულარული შეამოწმონ, ხომ არ არსებობს არასრულწლოვანის პერსონალური ინფორმაციის გამჟღავნების საფრთხე, მათ შორის უსაფრთხოებისა და კონფიდენციალურობის პარამეტრების დაყენებით, ასევე იმის შემოწმებით, რომ მოსწავლის ელექტრონულ

[13] European Data Protection https://ec.europa.eu/ [უ.გ.9.01.2021].
[14] თავი II, მუხლი 8, General Data Protection Regulation, 2016.
[15] Digital Solutions During Pandemic https://ec.europa.eu/ [უ.გ.9.01.2021].
[16] EUROPOL „Online Safety Advice for Parents and Carers”, 2020.
[17] Stay Safe Online https://ec.europa.eu/ [უ.გ.9.01.2021].

მოწყობილობაში არსებული თამაშები და აპლიკაციები სარგებლობენ კონფიდენციალურობის მკაცრი დაცვით და ა.შ[18]

აქედან გამომდინარე, ევროკავშირის სახელმწიფოებში პერსონალური მონაცემების ზოგად დაცვას GDPR უზრუნველყოფს, თუმცა ევროკომისიის ციფრული სტრატეგია პანდემიის პირობებში შექმნილი რეალობიდან გამომდინარე ეფექტიან ზომებს იღებს ონლაინ უსაფრთხოებისათვის. უშუალოდ სკოლის მოსწავლეების პერსონალური მონაცემების დაცულობისთვის კი EUROPOL-ის რეკომენდაცია მშობლებისთვის უდიდესი მნიშვნელობის მატარებელია.

3. პერსონალურ მონაცემთა დაცვა ამერიკის შეერთებული შტატების კანონმდებლობის მიხედვით

როდესაც საუბარია ონლაინ სივრცეში ბავშვთა პერსონალურ მონაცემთა დაცვაზე, მნიშვნელოვანია აღინიშნოს Children's Online Privacy Protection Rule[19]. COPPA 1998 წელს მიიღო კონგრესმა და მის მიზანს წარმოადგენს ის, რომ მშობლები ინფორმირებულნი იყვნენ, თუ რა სახის ინფორმაცია შეიძლება იყოს შეგროვებული ბავშვებიდან ონლაინ. აღნიშნული დოკუმენტი შემუშავებულია, რათა დაცული იყოს 13 წლამდე ბავშვების უსაფრთხოება ინტერნეტის გამოყენებისას, რათა კომერციულმა ვებსაიტებმა თუ სხვადასხვა ინტერნეტ სერვისებმა არ შეაგროვონ, გამოიყენონ ან გაამჟღავნონ ინფორმაცია .

მნიშვნელოვანი საკითხია ის, თუ რატომ ვრცელდება COPPA-ს მოქმედება მხოლოდ 13 წლამდე ბავშვებზე, და რატომ არ ვრცელდება იგი 13-18 წლის პირებზე. კონგრესმა COPPA-ს მიღებისას გაითვალისწინა ის, რომ 13 წლამდე პირები განსაკუთრებით დაუცველნი არიან და შეიძლება ვერ გააანალიზონ უსაფრთხოებასა და კონფიდენციალურობასთან დაკავშირებული პრობლემები. თუმცა, ეს ყველაფერი არ ნიშნავს იმას, რომ თინეიჯერები დაუცველები არიან.[20] ფედერალური სავაჭრო კომისია (FTC) იცავს 13-18 წლის ასაკის ბავშვებს სხვადასხვა რეკომენდაციის გაცემით მშობლებისა და ბავშვებისათვის.[21]

დისტანციური სწავლების პერიოდში, სკოლის მოსწავლეთა დაცულობას COPPA უზრუნველყოფს, რომელიც 13 წლამდე პირების შემთხვევაში პერსონალური ინფორმაციის შეგროვებისას მშობლების თანხმობას ითხოვს. სკოლების მიერ ონლაინ სწავლების მეთოდის გამოყენების შემთხვევაში, მოსწავლის პერსონალური მონაცემები შეიძლება გამოყენებული იყოს მხოლოდ საგანმანათლებლო, და არავითარ შემთხვევაში კომერციული მიზნებისთვის.

ასევე, მნიშვნელოვანია FERPA and Virtual Learning During COVID-19. რომელიც შეეხება FERPA-ს[22] გამოყენებას პანდემიის პირობებში და პერსონალური მონაცემების დაცვას. აღნიშნული დოკუმენტის მიხედვით, მოსწავლეთა კონფიდენციალურობის პოლიტიკის ოფისი პასუხისმგებელია FERPA-ს იმპლემენტაციისთვის, რაც გულისხმობს FERPA-სთან დაკავშირებული საჩივრების განხილვას. ზოგადად, FERPA არის ოჯახის საგანმანათლებლო

[18] EUROPOL „Online Safety Advice for Parents and Carers", 2020, p5.
[19] Federal Trade Commission, Children's Online Privacy Protection Rule", 1998.
[20] Complying With COPPA: Frequently Asked Questions, www.ftc.gov [უ.გ.9.01.2021].
[21] Online Security, www.OnguardOnline.gov. [უ.გ.9.01.2021].
[22] Family Educational Rights and Privacy Act, 1974.

უფლებებისა და კონფინდენციალურობის აქტი, რომელიც უზრუნველყოფს მშობლებისა და მოსწავლეების შემდეგი უფლებების დაცვას ისეთ საკითხებთან დაკავშირებით, როგორებიცაა:

- განათლებასთან დაკავშირებულ მონაცემებზე წვდომა;
- თანხმობის საჭიროება მოსწავლის პერსონალური ინფორმაციის გამჟღავნების შემთხვევაში;
- FERPA-ში გათვალისწინებული უფლების დარღვევის შემთხვევაში გასაჩივრების შესაძლებლობა.

ონლაინ სწავლებისას FERPA and Virtual Learning During COVID-19-ს მიხედვით, FERPA- როლი განსაკუთრებით გაიზარდა დისტანციური სწავლების დროს, როდესაც საქმე ეხება მოსწავლეების საგანმანათლებლო მონაცემებს/ჩანაწერებს, მათთან წვდომას, ასევე მოსწავლის გამოსახულების შემცველ ვიდეოებზე, ან სხვა სახის პერსონალურ მონაცემებზე, მაგალითად ელექტრონულ ფოსტაზე ხელმწისაწვდომობას და ა.შ. შესაბამისად, FERPA უზრუნველყოფს აშშ-ში მოსაწავლეთა პერსონალური მონაცემების დაცულობას.

აქედან გამომდინარე, როდესაც საუბარია მოსწავლეთა პერსონალური მონაცემების დაცვაზე, მნიშვნელოვანია ფედერალური კანონმდებლობა კონფიდენციალურობის შესახებ, კერძოდ, COPPA და FERPA.

4. სკოლის მოსწავლეთა პერსონალური მონაცემების დაცვა ქართული კანონმდებლობის მიხედვით

საქართველოში პერსონალურ მონაცემთა ზოგად დაცვას უზრუნველყოფს პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, რომელშიც მოცემულია მონაცემების დამუშავების საფუძვლები, კერძოდ: არსებობს მონაცემთა სუბიექტის თანხმობა; მონაცემთა დამუშავება გათვალისწინებულია კანონით; მონაცემთა დამუშავება საჭიროა მონაცემთა დამმუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად; მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად; მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის აღმატებული ინტერესი[23] და ა.შ. აღნიშნული კანონში არ ვხვდებით დებულებებს არასრულწლოვნების პერსონალური მონაცემების დაცვის შესახებ, განსხვავებით GDPR-გან, რაც, ვფიქრობ, საჭიროებს დამატებით საკანონმდებლო ცვლილებას, რადგან არასრულწლოვნების შემთხვევა სპეციფიკური ხასიათისაა და სკოლის მოსწავლეები დაუცველები არიან, როდესაც საქმე ეხება მათი მონაცემების დამუშავებას.

არასრულწლოვანის პერსონალურ მონაცემებზე უშუალოდ საუბარია ,,ზოგადი განათლების შესახებ“ კანონის დებულებებში. კერძოდ, მათში მითითებულია, რომ მოსწავლის, მშობლის და მასწავლებლის პირადი ცხოვრება ხელშეუხებელია. მათ არ შეიძლება მოეთხოვოთ, გაამჟღავნონ ინფორმაცია თავიანთ პირად ცხოვრებაზე. ასევე, მოცემულია სკოლის ვალდებულება, რომ მოსწავლის, მშობლის და მასწავლებლის პერსონალური მონაცემების შეგროვებისას და შენახვისას იხელმძღვანელოს ზოგადი განათლების შესახებ კანონისა და საქართველოს ზოგადი ადმინისტრაციული კოდექსის მოთხოვნებით. გარდა ამისა,

[23] მუხლი 5, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი. 2012წ.

მოსწავლის აკადემიური მოსწრების შესახებ ინფორმაცია დისციპლინური მონაცემებისგან განცალკევებით უნდა ინახებოდეს და სხვ.[24] ვფიქრობ, რომ აღნიშნული დებულებები მნიშვნელოვანია მოსწავლეთა პერსონალურ მონაცემთა დაცვის თვალსაზრისით, თუმცა დისტანციური სწავლების პირობებში საჭიროა დამატებითი რეგულაციების არსებობა, რადგან საკლასო ოთახში და ონლაინ სივრცეში ჩატარებული გაკვეთილები ერთმანეთისგან განსხვავდება იმ თვალსაზრისით, რომ მოსწავლის მონაცემის გავრცელება გაცილებით მარტივია ელექტრონული მოწყობილების გაკვეთილზე აქტიურად გამოყენების მეშვეობით, ვინაიდან არსებობს სოციალური ქსელებსა თუ ვებსაიტებზე ვიდეო ჩანაწერებისა და ფოტოების გავრცელების საშიშროება. ამიტომ, მნიშვნელოვანია, რომ ქვეყნის კანონმდებლობა მოერგოს დღევანდელ რეალობას და ონლაინ გაკვეთილების შემთხვევებს. ასევე, შესაძლებელია ახალი კანონის მიღება ონლაინ სივრცეში არასრულწლოვანის პერსონალური მონაცემების დაცვის შესახებ, რაც COPPA-ს მაგალითზე დაყრდნობით შეგვიძლია ვთქვათ, რომ ეფექტიანი იქნება.

როდესაც ვსაუბრობთ პერსონალური მონაცემების დაცვაზე, მნიშვნელოვანია ვახსენოთ სახელმწიფო ინსპექტორის სამსახურის როლი. იგი წარმაოდგენს დამოუკიდებელ ორგანოს, რომელიც 2019 წლიდან ამოქმედდა და მისი საქმიანობის მიმართულებებს წარმოადგენს პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი; ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი[25] და ა.შ. თუმცა, მოცემული ნაშრომის მიზნებისთვის, ყურადღება უნდა გავამახვილოთ სახელმწიფო ინსპექტორის სამსახურის როლზე არასრულწლოვანთა პერსონალური მონაცემების დამუშავების კუთხით. როგორც ზემოთ აღინიშნა, სახელმწიფო ინსპექტორის სამსახურის 2019 წლის ანგარიშში მოცემული იყო ინფორმაცია არასრულწლოვანის პერსონალური მონაცემების დამუშავების შესახებ. ასევე, 2020 წლის 20 მარტს სახელმწიფო ინსპექტორის სამსახურმა გამოაქვეყნა რეკომენდაციები კორონავირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით, რომელში განხილულ საკითხებს შორის ერთ-ერთია დისტანციური შეხვედრებისა და სწავლების პროცესში პერსონალური მონაცემების დამუშავება. აღნიშნული რეკომენდაციის თანახმად, საგანმანათლებლო დაწესებულებები, ამ დაწესებულებებში დასაქმებული პირები, ასევე, არასრულწლოვანი პირების მშობლები და ოჯახის წევრები, მეტი პასუხისმგებლობით უნდა მოეკიდონ ბავშვების მონაცემების გასაჯაროებას და იმოქმედონ არასრულწლოვნის საუკეთესო ინტერესების გათვალისწინებით.[26]აქედან გამომდინარე, სახელმწიფო ინსპექტორის სამსახურს დიდი წვლილი მიუძღვის სკოლის მოსწავლეთა პერსონალური მონაცემების დამუშავების შესახებ არსებული დარღვევების გამოვლენასა და არასრულწლოვანთა პერსონალური მონაცემების დაცვაში, თუმცა მიმაჩნია, რომ ესეში გადმოცემული პრობლემების პრევენციისა და აღმოფხვრისათვის საჭიროა დამატებითი ღონისძიებების მიღება, რომელზეც დასკვნით ნაწილში იქნება საუბარი.

[24] მუხლი 17, ,,ზოგადი განათლების შესახებ კანონი“, 2005წ.

[25] https://personaldata.ge/ [უ.გ.8.01.2021].

[26] სახელმწიფო ინსპექტორის სამსახური, ,,სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები, COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავება“, 2020წ. გვ4.

დასკვნა

პერსონალურ მონაცემთა ,,ხელშეუხებლობა არის ინდივიდის ავტონომიურობის, დამოუკიდებელი განვითარების, მისი ღირსების დაცვის წინაპირობა[27]. სწორედ ამიტომ, არასრულწლოვანთა პერსონალური მონაცემების დაცვა განსაკუთრებული მნიშვნელობის მატარებელია.

საზღვარგარეთის ქვეყნების კანონმდებლობის ანალიზმა გვიჩვენა, რომ როგორც ევროკავშირის, ისე აშშ-ს ფედერალურ კანონმდებლობაში დიდი მნიშვნელობა ენიჭება ბავშვთა პერსონალური მონაცემების დაცვას, მათ შორის კიბერ სივრცეში, რადგან არასრულწლოვნებს კარგად არ აქვთ გააზრებული პერსონალური მონაცემების დაცვის მნიშვნელობა და ამიტომაც განსაკუთრებულ დაცვას საჭიროებენ.

ხოლო რაც შეეხება საქართველოში არსებულ ვითარებას. აუცილებელია, რომ სკოლის მოსწავლეების მშობლებმა, ასევე სასწავლო დაწესებულებებმა და სახელმწიფომ ერთობლივად განახორციელონ ქმედებები მოსწავლეთა პერსონალურო მონაცემების დაცვისათვის.

პირველ რიგში, უნდა მოხდეს მშობლების ინფორმირება და საზოგადოების ცნობიერების ამაღლება პერსონალური მონაცემების დაცვის შესახებ. მშობლებისათვის შესაძლებელია ტრენინგების ჩატარება, ასევე სპეციალური სახელმძღვანელოების შექმნა, რომელშიც დეტალურად იქნება ახსნილი მოსწავლის პერსონალური მონაცემების გამჟღავნების საფრთხეების შესახებ, განსაკუთრებით დისტანციური სწავლების პირობებში. ეს ყველაფერი მშობლებს მისცემს საშუალებას, რომ დაიცვან ბავშვები აღნიშნული საფრთხეებისგან, მიაწოდონ ინფორმაცია პერსონალური მონაცემების შესახებ მათთვის გასაგებ ენაზე და ამ გზით მოახდინონ მოსწავლეთა პერსონალური მონაცემების გავცელების პრევენცია.

გარდა ამისა, ტრენიგნები უნდა ჩაუტარდეთ სასწავლო დაწესებულებების ადმინისტრაციას, პედაგოგებს, რადგან სკოლის მოსწავლის პერსონალურ მონაცემთა უმეტესობა სწორედ სკოლაში იყრის თავს. მასწავლებლებს უნდა ჰქონდეთ ინფორმაცია იმის შესახებ, თუ როგორ აირიდონ თავიდან მოსწავლეთა მონაცემების გასაჯაროვება, მოახდინონ მოსწავლის აკადემიური მოსწრების, გამოსახულების ამსახველი და სხვა ინფორმაციის საჯარო სივრცეში გავრცელების პრევენცია არასრულწლოვანისა და მისი მშობლის თანხმობის გარეშე.

რაც შეეხება სახელმწიფოს. უნდა მოხდეს სახელმძღვანელო პრინციპების შემუშავება სკოლის მოსწავლეთა პერსონალური მონაცემების გამჟღავნების პრევენციის მიზნით, მნიშვნელოვანია ასევე სახელმწიფო ინსპექტორის სამსახურის თანამშრომლების გადამზადება და თანამედროვე ტექნოლოგიების გამოყენება იმისათვის, რომ რაც შეიძლება სწრაფად გამოვლინდეს მოსწავლის პერსონალური ინფორმაციის გავრცელების შემთხვევა და თავიდან იქნეს აცილებული მოსწავლის ბულინგი ან სხვაგვარი ნეგატიური ფსიქოლოგიური ზეწოლა. ასევე, როგორც უკვე აღვნიშნე, მიზანშეწონილია ცვლილებები განხორციელდეს კანონმდებლობაში. როგორც უკვე აღვნიშნეთ, ,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი ზოგადი ხასიათისაა და სასურველია დაემატოს დებულებები არასრულწლოვანთა დაცვის შესახებ. რაც შეეხება ,,ზოგადი განათლების შესახებ კანონს“, საჭიროა იგი მეტად მოერგოს დისტანციური სწავლების შემთხვევას და გათვალისწინებული იყოს დღევანდელი

[27] მუხლი 2. დადგენილება N180 ,,პერსონალურ მონაცემთა დავის ინსპექტორის საქმიანობისა და მისი უფლებამოსილების განხორციელების წესის შესახებ დებულების დამტკიცების თაობაზე“.

რეალობა. ეს ყველაფერი აუცილებელია, რათა კანონები მოერგოს დღევანდელ მდგომარეობას და დისტანციური სწავლების პირობებში შესაძლებელი გახდეს მოსწავლეთა პერსონალური მონაცემების ეფექტიანად დაცვა.

ბიბლიოგრაფია

1. ,,პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი“ <matsne.gov.ge> https://www.ftc.gov/ [უკანასკნელად გადამოწმდა 18.01.2021];
2. The Treaty on European Union, 1992;
3. General Data Protection Regulation, 2016 ;
4. EUROPOL „Online Safety Advice for Parents and Carers”, 2020;
5. Family Educational Rights and Privacy Act, 1974 ;
6. დადგენილება N180 ,,პერსონალურ მონაცემთა დავის ინსპექტორის საქმიანობისა და მისი უფლებამოსილების განხორციელების წესის შესახებ დებულების დამტკიცების თაობაზე“;
7. ,,ზოგადი განათლების შესახებ კანონი“, 2005წ;
8. Children's Online Privacy Protection Rule, https://www.ftc.gov/ [უკანასკნელად გადამოწმდა 18.01.2021];
9. Hye Jung Han, ,,As Schools Close Over Coronavirus, Protect Kids’ Privacy in Online Learning“, https://www.hrw.org/news [უკანასკნელად გადამოწმდა 18.01.2021];
10. Sonia Livingstone, Children: a special case for privacy? http://eprints.lse.ac.uk/;
11. სახელმწიფო ინსპექტორის სამსახური, https://personaldata.ge [უკანასკნელად გადამოწმდა 13.01.2021];
12. სახელმწიფო ინსპექტორის სამსახურის რეკომენდაცია COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით https://personaldata.ge/_[უკანასკნელად გადამოწმდა 18.01.2021];
13. ,,სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, სახელმწიფო ინსპექტორის სამსახური, 2019წ;
14. European Data Protection https://ec.europa.eu/ [უკანასკნელად გადამოწმდა 16.01.2021];
15. Digital Solutions During Pandemic https://ec.europa.eu/_[უკანასკნელად გადამოწმდა 15.01.2021];
16. EUROPOL „Online Safety Advice for Parents and Carers”, 2020;
17. Stay Safe Online https://ec.europa.eu/_[უკანასკნელად გადამოწმდა 13.01.2021];
18. Complying With COPPA: Frequently Asked Questions, www.ftc.gov [უკანასკნელად გადამოწმდა 12.01.2021];
19. Online Security, www.OnguardOnline.gov. [უკანასკნელად გადამოწმდა 12.01.2021];
20. საქართველოს საკონსტიტუციო სასამართლოს 2009 წლის 10 ივნისის N1/2/458 განჩინება საქმეზე, ,,საქართველოს მოქალაქეები - დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ“.

Bibliography

1. Law of Georgia on Personal Data Protection <matsne.gov.ge> [Last checked 18.01.2021];
2. The Treaty on European Union, 1992;
3. General Data Protection Regulation, 2016;
4. EUROPOL, ,, Online Safety Advice for Parents and Carers ", 2020;
5. Family Educational Rights and Privacy Act, 1974;
6. Resolution N180 "On Approval of the Regulation on the Activities of the Personal Data Dispute Inspector and the Rules of Exercise of His Powers";
7. Law on General Education, 2005;
8. Children's Online Privacy Protection Rule, https://www.ftc.gov/ [Last checked 18.01.2021];
9. Hye Jung Han, ,, As Schools Close Over Coronavirus, Protect Kids 'Privacy in Online Learning", https://www.hrw.org/news [Last checked 16.01.2021];
10. Sonia Livingstone, Children: a special case for privacy? http://eprints.lse.ac.uk/ [Last checked 18.01.2021];
11. State Inspector Service, https://personaldata.ge [Last checked 18.01.2021];
12. Recommendation of the State Inspector's Office regarding the processing of personal data in the process of combating COVID-19 https://personaldata.ge/ [Last checked 13.01.2021];
13. "Activity Report of the State Inspector Service", State Inspector Service, 2019;
14. European Data Protection https://ec.europa.eu/ [Last checked 18.01.2021];
15. Digital Solutions During Pandemic https://ec.europa.eu/ [Last checked 16.01.2021];
16. EUROPOL, Online Safety Advice for Parents and Carers, 2020;
17. Stay Safe Online https://ec.europa.eu/ [Last checked 18.01.2021];
18. Complying With COPPA: Frequently Asked Questions, www.ftc.gov [Last checked 13.01.2021];
19. Online Security, www.OnguardOnline.gov. [Last checked 12.01.2021];
20. Judgment N1 / 2/458 of the Constitutional Court of Georgia of 10 June 2009 on the case "Citizens of Georgia - Davit Sartania and Aleksandre Macharashvili v. Parliament of Georgia and Ministry of Justice of Georgia".

COVID-19 პანდემიის პირობებში ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვა

მზექალა რომანაძე,
თავისუფალი უნივერსიტეტი

აბსტრაქტი

COVID-19 პანდემიის პირობებში მთელი მსოფლიოს მასშტაბით ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის რისკი საგრძნობლად გაიზარდა. თითოეული სახელმწიფო, მათ შორის საქართველი, უდიდესი გამოწვევის წინაშე დგას და COVID-19-ის წინააღმდეგ ბრძოლის პროცესში აქტიურად არის ჩართული.

მცირე დროის მონაკვეთში კორონავირუსის სწრაფ გავრცელებასთან ერთად, გაიზარდა საზოგადოებრივი ინტერესი თითოეული ადამიანის ჯანმრთელობის მდგომარეობის მიმართ, რამაც ჯანმრთელობის შესახებ პერსონალური მონაცემების გასაჯაროებისაგან დაცვის საკითხი საფრთხის წინაშე დააყენა. კერძოდ, პაციენტთა ჯანმრთელობის შესახებ დეტალური მონაცემების გასაჯაროების თაობაზე მუდმივად არსებობს მედიის/საზოგადოების მოთხოვნები.

სტატისტიკური მონაცემები, რომლებიც ასახავს კორონავირუსით ინფიცირებულების, გარდაცვლილების ან მისგან გამოჯანმრთელებულების შესახებ ინფორმაციას, წარმოადგენს პერსონალური მონაცემების დამუშავების შედეგს, რომელიც როგორც წესი მაქსიმალურად დეპერსონალიზებულია. თუმცა, კონკრეტული შემთხვევების განხილვა ცხადყოფს, რომ პიროვნების ჯანმრთელობის შესახებ პერსონალური ინფორმაცია ისე ხდება მესამე პირებისათვის ხელმისაწვდომი, რომ კონკრეტული პირის იდენტიფიცირება ხშირად შესაძლებელი ხდება. კორონავირუსით ინფიცირების გამჟღავნების შედეგად კი, შესაძლოა ადამიანი დისკრიმინაციული მოპყრობის ობიექტადაც კი იქცეს და მორალური ზიანი მიადგეს, რადგან საზოგადოება მას აღიქვამს, როგორც საფრთხის წყაროს (გამოჯანმრთელების შემდგომაც კი).

ამავდროულად საყურადღებოა, რომ ზოგჯერ კონკრეტული ადამიანის არა მარტო კორონავირუსით ინფიცირების შესახებ ინფორმაციის გამჟღავნება ხდება, არამედ მისთვის დამახასიათებელი სხვა დაავადებების არსებობის თაობაზეც, რის მიმართაც ინფორმაციის გამცემ პირს შესაძლოა არ ჰქონდეს მიღებული პაციენტის თანხმობა (მოცემული კი სავალდებულო წინაპირობაა).

კორონავირუსის პანდემიის პირობებში ნამდვილად არსებობს ჯანმრთელობის შესახებ პერსონალური მონაცემების დამუშავების საჭიროება, თუმცა ეს არ გამორიცხავს პერსონალური მონაცემების კონფიდენციალურობის დაცვის ლეგიტიმურ ინტერესს.

იმის გათვალისწინებით, რომ ჯანმრთელობის მდგომარეობის შემცველი ინფორმაცია წარმოადგენს განსაკუთრებული კატეგორიის მონაცემს და მის მიმართ მოქმედებს დაცვის მაღალი სტანდარტი, COVID-19 პანდემიის პირობებში, ანუ მაშინ, როცა საზოგადოებრივი ინტერესი ჯანმრთელობის მდგომარეობის შესახებ ჩვეულებრივზე საგრძნობლად მაღალია, არსებობს ჯანმრთელობის შესახებ პერსონალურ მონაცემთა კანონის დარღვევით დამუშავებისა და გამჟღავნების მომეტებული საფრთხე.

თუ პანდემიის პირობებში, არ იქნება დაცული პირთა ჯანმრთელობის შესახებ ინფორმაცია და საზოგადოებრივ ინტერესებს მიენიჭება უპირატესობა, ადამიანები თავს შეიკავებენ სათანადო ორგანოებისათვის ინფორმაციის მიწოდებისაგან, რაც ვირუსის შემდგომი გავრცელების პრევენციას ხელს შეუშლის.

საკვანძო სიტყვები: პერსონალური მონაცემი, განსაკუთრებული კატეგორიის პერსონალური მონაცემი, პერსონალურ მონაცემთა დამუშავება, პანდემია, COVID-19, ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის დამუშავება.

Abstract

In the condition of the COVID-19 pandemic, the risk of violations of basic human rights and freedoms has increased significantly worldwide. Every country, including Georgia, is facing many difficult challenges and is actively involved in the fight against COVID-19.

With the rapid spread of the coronavirus in a short period of time, there has been an increase in public interest in the healthrelated information of each individual, which put the issue of protection of personal health data at risk. In particular, there are permanent requirements for the disclosure of detailed patient health data from media / community.

Statistics that show information about coronavirus infection, death, or recovery from it are the result of personal data processing that is typically maximally depersonalized. However, reviewing specific cases reveals that personal information about a person's health becomes so accessible to third parties that it is often possible to identify a specific person. Disclosure of a coronavirus infection may even result in discriminatory treatment and moral damage, as society perceives it as a source of danger (even after recovery).

At the same time, sometimes information is disclosed not only about the coronavirus infection of a particular person, but also about the existence of other diseases and illnesses, for which the person who issue the information may not have the consent of the patient (this is a compulsory prerequisite).

In the conditions of a coronavirus pandemic, the processing of personal health data is necessary, although this does not preclude a legitimate interest in protecting the privacy of personal data.

Health related personal information is a special category of data and is subject to a high standard of protection, in the context of the COVID-19 pandemic, when the public interest in healthrelated information is significantly higher than usual, there is increased risk of illegal data processing.

If, in the condition of the pandemic, information about the health of individuals is not protected and the public interest is given priority, people will refrain from providing information to the appropriate authorities - which eventually will not prevent spread of the virus.

Keywords: Personal data, a special category of personal data, personal data processing, pandemic, COVID-19, processing of healthrelated information.

შესავალი

კორონავირუსის პანდემიამ მოულოდნელად და რადიკალურად შეცვალა მსოფლიოს სურათი. შეცვალა სახელმწიფოები, ადამიანები, ურთიერთობები და ყოველდღიურობის თითქმის ყველა ასპექტი. აღნიშნული პანდემია შეეხო ყველა სფეროს (ეკონომიკას, პოლიტიკას, სამართალს, მედიცინას, განათლებას, სპორტს და ა.შ.), რაც მეტწილად მძიმე შედეგების მომტანი აღმოჩნდა, რადგან ჩვეულებრივი რეალობა ფორსმაჟორულ[1] ვითარებად გარდაიქმნა, რომლის მიმართაც პანდემიამდე არსებული სამართლებრივი წესრიგი არაეფექტური აღმოჩნდა.

არსებული რეალობის პირობებში კი თითოეული სახელმწიფო იძულებული გახდა პანდემიით გამოწვეული უარყოფითი შედეგების თავიდან აცილების მიზნით, მორგებოდა შეცვლილ გარემოებას და შეემუშავებინა საჭიროების შესაბამისი სამართლებრივი რეგულირება. აღნიშნული უმეტესწილად გამოიხატა დროის მოკლე მონაკვეთში მთელი რიგი შეზღუდვებისა და წესების დადგენაში, რამაც ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის რისკი, იმის გათვალისწინებით, რომ COVID-19 პანდემია წარმოადგენს მოულოდნელი და სწრაფი ცვლილებების, არასტაბილურ და იზოლაციის/კარანტინის რეჟიმს, საგრძნობლად გაზარდა.

ამავდროულად, გაიზარდა საზოგადოების ინტერესი მიმდინარე პროცესების მიმართ, რამაც განსაკუთრებით „სასურველი და მოთხოვნადი“ გახადა წვდომა პირთა პერსონალურ მონაცემებზე, კერძოდ ყველაზე აქტუალური გახდა თითოეული ადამიანის ჯანმრთელობის შესახებ მონაცემთა საჯაროობის საკითხი. აღნიშნულის მიზეზი კი კორონავირუსით ინფიცირებულ, შესაძლო ინფიცირებულ ან/და მათთან კონტაქტში მყოფ პირთა ვინაობის იდენტიფიცირების საჭიროება გახდა, რათა თავიდან აეცილებინათ აღნიშნულ ადამიანებთან კონტაქტი და შესაბამისად შეემცირებინათ ვირუსის გავრცელების რისკები.

თუმცა, COVID-19 პანდემიის პირობებში საზოგადოებისათვის კონკრეტულ პირთა ჯანმრთელობის მდგომარეობის შესახებ მონაცემთა გამჟღავნების შემთხვევები გასცდა იმ აუცილებლობის ფარგლებს, რაც ჩვეულებრივ დასაშვებია საჯარო ინტერესებისათვის. მსგავსი შემთხვევები ყველაზე მაღალი ინტენსივობით გამოვლინდა ვირუსის გავრცელების საწყის პერიოდში, როცა ყველაზე მაღალი იყო საზოგადოების ინტერესი ყოველი ახალი შემთხვევის მიმართ. მაგალითად, ყველამ იცოდა თუ ვინ იყო N5 კოვიდ ინფიცირებული საქართველოში, რომელმაც კიდევ რამდენიმე ადამიანი დააინფიცირა. აღნიშნულმა, არცთუ ისე იშვიათმა შემთხვევებმა, არა მარტო საფრთხე შეუქმნა პირთა პერსონალური მონაცემების დაცვას, ასევე კორონავირუსით ინფიცირებულ, შესაძლო ინფიცირებულ, მათთან კონტაქტში მყოფ ან უკვე გამოჯანმრთელებულ პირთა მიმართ ჩამოაყალიბა უარყოფითი და ხშირ შემთხვევაში დისკრიმინაციული დამოკიდებულებები.

პირის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია წარმოადგენს განსაკუთრებული კატეგორიის პერსონალურ მონაცემს,[2] რომლის მიმართ, როგორც საქართველოს[3], ისე

[1] „ფორსმაჟორი - [...] ეპიდემია [...] და სხვა მსგავსი მოვლენები, რომელიც არ ექვემდებარება მხარეთა კონტროლს და რომელთა თავიდან აცილებაც მათ მიერ შეუძლებელია.“ იხ. პირველი მუხლის პირველი პუნქტის „ქ“ ქვეპუნქტი, საქართველოს კანონი „ნავთობისა და გაზის შესახებ“, 16 აპრილი, 1999.

[2] მუხლი 2, ქვეპუნქტი„ბ“, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 28 დეკემბერი, 2011.

[3] იხ. სქოლიო 2, მუხლი 6.

საერთაშორისო კანონმდებლობის[4] საფუძველზე მოქმედებს დაცვის უფრო მაღალი სტანდარტი. განსხვავებული სამართლებრივი რეგულირება განპირობებულია იმით, რომ ჯანმრთელობის მდგომარეობის შესახებ მონაცემები ხშირ შემთხვევაში შეიცავს მეტად ინტიმურ დეტალებს პირის პირადი ცხოვრების, მისი ფსიქიკური და ფიზიკური მდგომარეობის შესახებ, რომლის გამჟღავნებაც შესაძლოა გახდეს პირის ღირსების შელახვის ან დისკრიმინაციის საფუძველი.

პერსონალური მონაცემების დაცვა თავის მხრივ პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზების კომპონენტს წარმოადგენს.[5] რაც იმას ნიშნავს, რომ პერსონალური მონაცემების დაცვას კონსტიტუციური საფუძვლები აქვს. ხოლო, უშუალოდ ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემების დაცვისა და კონფიდენციალურობის უზრუნველყოფის სამართლებრივი მექანიზმები განმტკიცებულია როგორც საქართველოს კონსტიტუციით[6], ასევე სპეციალური კანონებით.[7]

იმის გათვალისწინებით, რომ მცირე დროის მონაკვეთში კორონავირუსის სწრაფ გავრცელებასთან ერთად, გაიზარდა საზოგადოებრივი ინტერესი თითოეული ადამიანის ჯანმრთელობის მდგომარეობის მიმართ, აღნიშნულმა ჯანმრთელობის შესახებ პერსონალურ მონაცემთა გასაჯაროებისაგან დაცვის საკითხი საფრთხის წინაშე დააყენა. განსაკუთრებით, COVID-19 პანდემიის პირობებში აქტუალური და პრობლემატური გახდა ჯანმრთელობის დაცვის დაწესებულებებისა და დამსაქმებლების მიერ ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავების საკითხი.

ამავდროულად, COVID-19 პანდემიის პირობებში პაციენტთა ჯანმრთელობის მდგომარეობის შესახებ დეტალური მონაცემების გასაჯაროების თაობაზე მუდმივად არსებობს მედიის/საზოგადოების მოთხოვნები, რამაც მედია საშუალებების მიერ პერსონალურ მონაცემთა გასაჯაროება რისკის შემცველი გახადა. კერძოდ, კორონავირუსის პანდემიის პირობებში გამოიკვეთა შემდეგი აქტუალური პრობლემები: კორონავირუსით ინფიცირებულ პირთა მარტივად იდენტიფიცირებადობა, კორონავირუსით ინფიცირებასთან ერთად სხვა დაავადებების შესახებ ინფორმაციის გასაჯაროება, საჯარო ინტერესის ფარგლების განსაზღვრა და კორონავირუსით ინფიცირებულის (ან უკვე გამოჯანმრთელებულის) მიმართ უარყოფითი დამოკიდებულება. რის გამოც თითოეული სახელმწიფო, მათ შორის საქართველო, უდიდესი გამოწვევის წინაშე დგას და COVID-19-ის წინააღმდეგ ბრძოლის პროცესში აქტიურად არის ჩართული.

[4] მუხლი 9, Regulation (EU) 2016/679 „General Data Protection Regulation (GDPR)“, 25 მაისი, 2018. ავტორის შენიშვნა: მიუხედავად იმისა, რომ აღნიშნული ევროკავშირის რეგულაციაა და შესაბამისად, საქართველოსთვის არ აქვს სავალდებულო ხასიათი, საქართველოს კანონმდებლობაში პერსონალურ მონაცემთა რეგულირებისას მოცემული წესების გათვალისწინება მნიშვნელოვნად გაზრდის საქართველოში პერსონალურ მონაცემთა დაცვის ხარისხს, რითაც ქართული კანონმდებლობა ევროპულ სტანდარტებს, ხოლო საქართველო ევროკავშირს კიდევ უფრო დაუახლოვდება. <https://bit.ly/2LhnHFV> [უ.გ.05.01.2021].

[5] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაცია, „ჯანმრთელობის დაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ“, გვ. 3.

[6] მუხლი18 პუნქტი3, საქართველოს კონსტიტუცია, 24 აგვისტო, 1995.

[7] „პერსონალურ მონაცემთა დაცვის შესახებ“, „საექიმო საქმიანობის შესახებ“, „პაციენტის უფლებების შესახებ“, „ჯანმრთელობის დაცვის შესახებ“ საქართველოს კანონები და ასევე სხვა კანონქვემდებარე აქტები.

1.ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა დაცვის სამართლებრივი რეგულირება

ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემი[8] არის განსაკუთრებული კატეგორიის მონაცემი[9] და წარმოადგენს პირის ფიზიკურ ან ფსიქიკურ ჯანმრთელობასთან, მათ შორის, სამედიცინო მომსახურების გაწევასთან დაკავშირებულ მონაცემებს, რომლითაც შესაძლებელია პირის ამჟამინდელ, წარსულში არსებულ ან სამომავლო ჯანმრთელობის მდგომარეობასთან დაკავშირებით ინფორმაციის მიღება.[10] მოცემული სახის პერსონალური მონაცემის დამუშავებისა[11] და მისი კონფიდენციალურობის უზრუნველყოფის სამართლებრივი მექანიზმები გათვალისწინებულია როგორც საქართველოს კონსტიტუციით, ასევე სპეციალური კანონებით.

1.1 საქართველოს კონსტიტუცია

„ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, [...] არავისთვის უნდა იყოს ხელმისაწვდომი თვით ამ ადამიანის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის ან სხვათა უფლებების დასაცავად.“[12] აქედან გამომდინარე, კონსტიტუცია პირდაპირ კრძალავს მონაცემთა სუბიექტის[13] თანხმობის[14] გარეშე ჯანმრთელობასთან დაკავშირებული ინფორმაციის გასაჯაროებას ან მესამე პირისათვის[15] გადაცემას. თუმცა ამავდროულად, ამომწურავად განსაზღვრავს საგამონაკლისო შემთხვევებს იმ ლეგიტიმური მიზნების სახით, რომელთა საფუძველზეც დასაშვებია ჯანმრთელობასთან დაკავშირებული ინფორმაციის გამჟღავნება.

საქართველოს საკონსტიტუციო სასამართლომ თავის ერთ-ერთ გადაწყვეტილებაში განმარტა, რომ „საჯარო დაწესებულებაში არსებული და დაცული ნებისმიერი სახის ინფორმაციას და საზოგადოებისათვის მის ხელმისაწვდომობას არ აქვს თანაბარი მნიშვნელობა. საჯარო ინფორმაციის გარკვეული კატეგორიის მიმართ შესაძლოა, არსებობდეს ღიაობის მომეტებული

---

[8] „ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.“ იხ. სქოლიო 2, მუხლი2 „ა“ ქვეპუნქტი.

[9] „მონაცემი, რომელიც დაკავშირებულია პირის [...] ჯანმრთელობის მდგომარეობასთან, [...] აგრეთვე ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა.“ იხ. სქოლიო 2.

[10] იხ. სქოლიო 5, გვ. 4.

[11] „მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, კერძოდ, შეგროვება, ჩაწერა, ფოტოზე აღბეჭდვა, აუდიოჩაწერა, ვიდეოჩაწერა, ორგანიზება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება ან გამჟღავნება მონაცემთა გადაცემის, გავრცელების ან სხვაგვარად ხელმისაწვდომად გახდომის გზით, დაჯგუფება ან კომბინაცია, დაბლოკვა, წაშლა ან განადგურება.“ იხ. სქოლიო 2, მუხლი 2, ქვეპუნქტი „დ“ .

[12] იხ. სქოლიო 6.

[13] „ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემი მუშავდება.“ იხ. სქოლიო 2, მუხლის 2, ქვეპუნქტი„ვ“ .

[14] „მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე ზეპირად, სატელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით გამოხატული ნებაყოფლობითი თანხმობა, რომლითაც შესაძლებელია ნათლად დადგინდეს მონაცემთა სუბიექტის ნება.“ იხ. სქოლიო 2, მუხლი 2, ქვეპუნქტი „ზ“.

[15] „ნებისმიერი ფიზიკური ან იურიდიული პირი, საჯარო დაწესებულება, გარდა მონაცემთა სუბიექტისა, სახელმწიფო ინსპექტორის სამსახურისა, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირისა.“ იხ. სქოლიო 2, მუხლი 2, ქვეპუნქტი „მ“ .

ინტერესი. ამგვარ განსაკუთრებულ ინტერესზე უპირველესად მიუთითებს ინფორმაციის არსი, დანიშნულება და ის სიკეთე, რომლის დაცვასაც უზრუნველყოფს ამგვარი ინფორმაციის საჯაროობა.“[16] შესაბამისად, ყოველ კონკრეტულ შემთხვევაში შესაფასებელია, რამდენად აღემატება ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემის ღიაობის ინტერესი, აღნიშნულ პერსონალურ მონაცემთა კონფიდენციალურობის დაცვის ინტერესს.

საყურადღებოა, რომ საქართველოს კონსტიტუციის ზემოაღნიშნული დებულება „არ მოითხოვს, რომ ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებულია პირის ჯანმრთელობასთან, [...] სრულად დახურული იყოს. პირიქით, ამავე კონსტიტუციურ დებულებაში მითითებულია ამ უფლების შეზღუდვის შესაძლებლობაზე“[17] – კანონით გათვალისწინებულ შემთხვევებში, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის ან სხვათა უფლებების დასაცავად. შესაბამისად, საქართველოს კონსტიტუცია ადგენს ჯანმრთელობის მდგომარეობის შესახებ მონაცემების გაცემის/გამჟღავნების დასაშვებობის გამონაკლის შემთხვევებს, რომელთა კონკრეტიზაცია ხდება კონსტიტუციის გარეთ - სპეციალურ კანონებში.

1.2 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი

კონსტიტუციის შემდეგ, ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვის ცენტრალურ საკანონმდებლო მექანიზმს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი წარმოადგენს, რადგან მასში დეტალურად არის განსაზღვრული ჯანმრთელობის მდგომარეობის შესახებ მონაცემთა დამუშავების კონკრეტული პირობები და ფარგლები. მოცემული კანონის უპირატესობა იმაში მდგომარეობს, რომ მისი მოქმედება ვრცელდება კერძო სექტორზეც, რაც განასხვავებს მას სხვა სპეციალური კანონებისგან.[18][19] შესაბამისად, აღნიშნული კანონის მოქმედება ვრცელდება როგორც ჯანმრთელობის დაცვის დაწესებულების, ასევე დამსაქმებელის მიერ პერსონალურ მონაცემთა, მათ შორის ჯანმრთელობის შესახებ მონაცემთა დამუშავების პროცესზე.

საყურადღებოა, რომ აღნიშნული კანონი ცალკე გამოყოფს განსაკუთრებულ კატეგორიას მიკუთვნებული პერსონალური მონაცემების ცნებას და ადგენს მათი დამუშავების სპეციალურ, მკაცრ რეჟიმს[20]. კერძოდ, მოცემული კანონის მე-6 მუხლის პირველი პუნქტი ზოგადად კრძალავს განსაკუთრებული კატეგორიის პერსონალური მონაცემის დამუშავებას, ხოლო მე-2 პუნქტი ითვალისწინებს დასახელებული მონაცემის დამუშავების შესაძლებლობას

---

[16] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N1/4/693,857 „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“, 2019 წლის 7 ივნისი. პარაგრაფი II-41.

[17] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N3/1/752 „ა(ა)იპ „მწვანე ალტერნატივა“ საქართველოს პარლამენტის წინააღმდეგ“, 2018 წლის 14 დეკემბერი. პარაგრაფი II-10.

[18] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „პერსონალურ მონაცემთა დაცვის შესახებ“, გვ. 2-3.

[19] საყურადღებოა, რომ საქართველოს კანონმდებლობაში პერსონალური მონაცემების დაცვის შესახებ არსებული სხვა დებულებების მოქმედება მხოლოდ საჯარო დაწესებულებებზე ვრცელდება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიღებამ კი, იმის გათვალისწინებით, რომ მნიშვნელოვანი მოცულობის პერსონალური მონაცემები კერძო სექტორში მუშავდება, აღმოფხვრა საჯარო დაწესებულებების გარეთ პერსონალურ მონაცემთა დაუცველობის პრობლემა.

[20] იხ. სქოლიო 16, პარაგრაფი II-14.

მონაცემთა სუბიექტის წერილობითი თანხმობის[21] საფუძველზე. ამავდროულად, აღნიშნულ ნორმაში მოცემულია ამომწურავი ჩამონათვალი იმ საგამონაკლისო შემთხვევებისა, რომლებიც ექცევა კონსტიტუციაში მოცემული ლეგიტიმური მიზნების ფარგლებში[22] და რომელიც (ამავე მუხლის მე-3 პუნქტის საფუძველზე) მოითხოვს მონაცემთა სუბიექტის თანხმობის არსებობას. შესაბამისად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაკუთრებული კატეგორიის მონაცემებთან მიმართებით აწესებს გაცილებით მაღალ სტანდარტს, ვიდრე სხვა პერსონალური მონაცემების დამუშავების მიმართ. კერძოდ, კანონით მკაცრად განსაზღვრულ საგამონაკლისო შემთხვევებშიც კი დაუშვებელია მონაცემთა სუბიექტის თანხმობის გარეშე მონაცემთა გასაჯაროება და მესამე პირისათვის გამჟღავნება.[23] რაც იმას ნიშნავს, რომ ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა დამუშავება დასაშვებია მხოლოდ მონაცემთა სუბიექტის თანხმობის საფუძველზე.

ხაზგასასმელია, რომ ნებისმიერ შემთხვევაში ჯანმრთელობის მდგომარეობის შესახებ მონაცემების დამუშავება უნდა მოხდეს იმ მოცულობით, რაც აუცილებელი, ადეკვატური და პროპორციულია შესაბამისი, მკაფიოდ განსაზღვრული კანონიერი მიზნის მისაღწევად,[24][25] რათა არ მოხდეს მონაცემთა თვითნებური, უკანონო და გაუაზრებელი დამუშავება.

ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გამჟღავნება პერსონალურ მონაცემთა დამუშავების ერთ-ერთი სახეა, რომლის მიმართაც ჯანდაცვის სფეროში სპეციალური რეგულირება არის შემუშავებული.

1.3 „ჯანმრთელობის დაცვის შესახებ“, „საექიმო საქმიანობის შესახებ“ და “პაციენტის უფლებების შესახებ“ საქართველოს კანონები

ცხადია, რომ „ჯანმრთელობის დაცვის შესახებ“, „საექიმო საქმიანობის შესახებ“ და „პაციენტის უფლებების შესახებ“ საქართველოს კანონებში, ჯანმრთელობის შესახებ მონაცემთა კონფიდენციალურობასთან დაკავშირებით, დადგენილი რეგულირება ვრცელდება მხოლოდ საექიმო საქმიანობის სუბიექტსა და პაციენტს შორის არსებულ ურთიერთობაზე. კერძოდ, მოცემული კანონები დეტალურად განსაზღვრავს ჯანმრთელობის დაცვის დაწესებულებების მიერ პაციენტთა პერსონალური მონაცემების კონფიდენციალურობის დაცვის ვალდებულებას.

აღსანიშნავია, რომ პირის ჯანმრთელობის მდგომარეობის შესახებ მონაცემის კონფიდენციალურობის მოთხოვნები პირდაპირ თუ ირიბად აღნიშნული კანონების ყველა მუხლის შინაარსში იკითხება. მათგან შეიძლება გამოვარჩიოთ „საექიმო საქმიანობის შესახებ“ საქართველოს კანონის 48-ე მუხლი, რომელიც განსაზღვრავს საექიმო საქმიანობის სუბიექტის

[21] „მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე გამოხატული ნებაყოფლობითი თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან სხვაგვარად აღნიშნა წერილობით ან მასთან გათანაბრებული ფორმით.“ იხ. სქოლიო 2, მუხლი 2, ქვეპუნქტი „თ“.

[22] „[...] ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებების და ურთიერთობის ხასიათიდან გამომდინარე, [...] ბ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დასაცავად [...] გ) მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, [...] აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის. [...]“ იხ. სქოლიო 2, მუხლი 6, პუნქტი 2.

[23] იხ. სქოლიო 2, მუხლი 6, პუნქტი 3.

[24] იხ. სქოლიო 2, მუხლი 4.

[25] იხ. სქოლიო 18, გვერდი 4.

ვალდებულებას დაიცვას „პაციენტის ჯანმრთელობის მდგომარეობისა და პირადი ცხოვრების შესახებ ინფორმაციის კონფიდენციალობა როგორც საექიმო საქმიანობის განხორციელებისას, ისე მისი შეწყვეტის შემდეგ, როგორც პაციენტის სიცოცხლეში, ისე მისი სიკვდილის შემდეგ.“ თუმცა ამავე მუხლში ჩამოთვლილია ის საგამონაკლისო შემთხვევებიც, როცა დასაშვებია პაციენტის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გამჟღავნება. მოცემულ შემთხვევაშიც უპირველეს პირობას წარმოადგენს პაციენტის თანხმობის არსებობა, თუმცა კანონი ითვალისწინებს სხვა შემთხვევებსაც, კერძოდ როცა: ინფორმაციის გაუმჟღავნებლობა საფრთხეს უქმნის მესამე პირის (რომლის ვინაობაც ცნობილია) ჯანმრთელობას ან/და სიცოცხლეს, თუ არსებობს დასაბუთებული ეჭვი სავალდებულო აღრიცხვას დაქვემდებარებულ დაავადებაზე და ა.შ.[26]

„პაციენტის უფლებების შესახებ“ საქართველოს კანონის 28-ე მუხლის პირველი პუნქტიცა და „ჯანმრთელობის დაცვის შესახებ“ საქართველოს კანონის 42-ე მუხლიც ანალოგიურ მოწესრიგებას ითვალისწინებს. საყურადღებოა, რომ აღნიშნულ ნორმებში მოცემული ყველა საგამონაკლისო შემთხვევა არ მოითხოვს მონაცემთა სუბიექტის თანხმობას. რაც იმას ნიშნავს, რომ რიგ შემთხვევაში შესაძლებელია პაციენტის ჯანმრთელობის შესახებ კონფიდენციალური მონაცემი გამჟღავნებულ იქნეს თვით პაციენტის თანხმობის გარეშე. აქედან გამომდინარე, აღნიშნულ კანონებში არსებული მოწესრიგება გარკვეულწილად ეწინააღმდეგება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის რეგულირებას, რადგან ბოლოხსენებული კანონი ჯანმრთელობის შესახებ მონაცემის ყოველგვარ დამუშავებაზე მოითხოვს მონაცემთა სუბიექტის თანხმობას.

გასათვალისწინებელია, სამართალში მოქმედი პრინციპი: ერთი და იმავე დონის სამართლის ნორმათა კოლიზიის დროს გამოიყენება სპეციალური და უფრო ახალი კანონი. ჯანმრთელობის დაცვის სფეროსათვის უფრო სპეციალურია და უპირატესობა მიენიჭება ზემოაღნიშნულ კანონებს. ხოლო „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის რეგულირება გავრცელდება ყველა სხვა დარჩენილ სფეროზე. თუმცა საყურადღებოა, რომ იმ შემთხვევაში, როდესაც შეუძლებელია პაციენტის თანხმობის მიღება - მეტად წონადი საჯარო ინტერესების არსებობის პირობებში გაუმართლებელია ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა დამუშავების აბსოლუტური აკრძალვა.[27]

ზემოაღნიშნულიდან გამომდინარე, საქართველოში არსებული რეგულირების თანახმად, პირის ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავება, როგორც საჯარო, ისე კერძო სექტორში, დასაშვებია თვითონ ამ პირის თანხმობის საფუძველზე, ვინაიდან აღნიშნული პერსონალური მონაცემი მიეკუთვნება განსაკუთრებულ მონაცემთა კატეგორიას. ხოლო პირის თანხმობის გარეშე ჯანმრთელობის შესახებ პერსონალურ მონაცემთა გამჟღავნება მკაცრად განსაზღვრულ შემთხვევებში დასაშვებია მხოლოდ ჯანდაცვის სფეროში. საყურადღებოა, რომ ისეთი ფორსმაჟორული ვითარება, როგორიც პანდემიაა - არსებული მოწესრიგების პრაქტიკაში ეფექტურად რეალიზებას ხელს არ უშლის, რადგან COVID-19 პანდემიის პირობებში გაზრდილი საზოგადოებრივი ინტერესი (ცალკეულ პირთა

[26] მუხლი 48, პუნქტი 2, საქართველოს კანონი „საექიმო საქმიანობის შესახებ“, 8 ივნისი, 2001.

[27] ამ მხრივ, აღსანიშნავია საქართველოს საკონსტიტუციო სასამართლოს ბოლო პერიოდის პრაქტიკა. კერძოდ, 2019 წლის 7 ივნისის N1/4/693,857 გადაწყვეტილებით, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლით დადგენილი აბსოლუტური აკრძალვა - პერსონალურ მონაცემთა პირის თანხმობის გარეშე დამუშავებაზე - არაკონსტიტუციურად იქნა ცნობილი. კერძოდ, აღნიშნულმა ნორმამ გადაწყვეტილებით დაკარგა აბსოლუტური აკრძალვის ნორმატიული შინაარსი.

ჯანმრთელობის მიმართ) ექცევა იმ საჯარო ინტერესის ფარგლებში, რაც პანდემიამდე მიღებული რეგულირებითაა დადგენილი.

პრინციპულად გაუმართლებელია ჯანმრთელობის შესახებ პერსონალური მონაცემის დაცვის უგულებელყოფის ხარჯზე, მოხდეს მხოლოდ საზოგადოებრივი ინტერესების დაკმაყოფილება, მაშინ როდესაც ამის აუცილებლობა საერთოდ არ არსებობს ან შესაძლებელია ნაკლებად მზღუდავი საშუალებების გამოყენება საჯარო ინტერესების მისაღწევად. ინფორმაცია კონკრეტული პირის ჯანმრთელობის შესახებ, არ უნდა გახდეს მესამე პირთათვის ხელმისაწვდომი, გარდა იმ ცალკეული შემთხვევებისა, როდესაც არსებობს უფრო ძლიერი, მაკონპენსირებელი საჯარო ინტერესი[28] ინფორმაციის გასაჯაროებისთვის.

2. ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა დაცვა პანდემიის პირობებში

COVID-19 პანდემიის პირობებში, მაღალი საზოგადოებრივი ინტერესის ფონზე, ჯანმრთელობის შესახებ პერსონალურ მონაცემთა კანონის დარღვევით დამუშავებისა და გამჟღავნების მომეტებული საფრთხე წარმოიშვა. აღნიშნული განსაკუთრებით გამოვლინდა ჯანდაცვის დაწესებულებებისა და ცალკეულ დამსაქმებელთა მიერ ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავების საჭიროებაში, რაც პანდემიამდე პერიოდში სულაც არ იყო აქტუალური და მათ შორის სავალდებულო.[29] შესაბამისად, კორონავირუსის მიერ შექმნილმა რეალობამ პირთა ჯანმრთელობის შესახებ პერსონალურ მონაცემთა უკანონო გამჟღავნების რისკები გაზარდა.

2.1. ჯანდაცვის დაწესებულებების მიერ პერსონალურ მონაცემთა დამუშავება

ჯანმრთელობის დაცვის დაწესებულებების მიერ პაციენტთა ჯანმრთელობის შესახებ მონაცემთა დამუშავების პროცესი პანდემიით გამოწვეულ სიახლეს არ წარმოადგენს, რადგან სხვადასხვა პერსონალური მონაცემების დამუშავება ჩვეულებრივი მოვლენაა და მათ მიმართ კონფიდენციალურობის ვალდებულება პაციენტის მიღების მომენტიდან წარმოიშობა, ვინაიდან, აუცილებელია ჯანდაცვის სისტემის ეფექტური მართვა-ფუნქციონირებისათვის.

COVID-19 პანდემიის წინააღმდეგ ბრძოლის პროცესში ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავების მიმართ, ჯანმრთელობის დაცვის სფეროში მომეტებული საფრთხე იმიტომ წარმოიშვა, რომ აღნიშნულ დაწესებულებებს უწევთ ჩვეულებრივზე მეტი პერსონალური ინფორმაციის დამუშავება. კერძოდ, მოცემული დაწესებულებები აგროვებენ ინფიცირებულ ან შესაძლო ინფიცირებულ პირთა შესახებ ისეთ ინფორმაციებს, როგორიცაა მაგალითად: ახლო კონტაქტში მყოფი პირების შესახებ, ბოლო დროის მონაკვეთში გადაადგილების შესახებ, სხვა დაავადებების შესახებ ან სხვა ინფორმაციას, რაც მართალია არსებული საჭიროებიდან გამომდინარეობს, თუმცა პარალელურად მაღალი რისკის მატარებელია - კორონავირუსის „ნიღაბს ამოფარებული“ არ მოხდეს აღნიშნული პერსონალური მონაცემების გასაჯაროებაც.

---

[28] ძლიერ მაკონპენსირებელ საჯარო ინტერესად ვერ იქნება მიჩნეული საზოგადოების უბრალო სურვილი იცოდეს მაგალითად კოვიდინფიცირებულთა ვინაობა.

[29] სავალდებულოობა ეხება დამსაქმებელთა მიერ მასთან დასაქმებულ პირთა ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა დამუშავების არასაჭიროებას (მათ შორის უფლების არქონასაც).

ჯანდაცვის დაწესებულებების მიერ ინფიცირებულ, შესაძლო ინფიცირებულ ან ახლო კონტაქტში მყოფ პირთა შესახებ ჩვეულებრივზე მეტი მოცულობის ინფორმაციის დამუშავება თავისთავად ზრდის საზოგადოებისა და მედიის ინტერესს აღნიშნულ პირთა ვინაობის გასაჯაროებასთან დაკავშირებით. თუმცა, ვინაობის გასაჯაროება აუცილებელი არ არის, რადგან საზოგადოებრივი ინტერესის დასაკმაყოფილებლად და ლეგიტიმური მიზნების მისაღწევად, სრულიად საკმარისია არაიდენტიფიცირებადი ინფორმაციის გავრცელება (მაგალითად: მოქალაქეობა, ასაკი, სამუშაო ადგილი, მათი გადაადგილების მარშრუტი და სხვა). რაც იმას ნიშნავს, რომ ზემოაღნიშნულ პირთა შესახებ გასაჯაროებული ინფორმაცია მაქსიმალურად დეპერსონალიზებული[30] უნდა იყოს, რადგან მოცემული წარმოადგენს ყველაზე ნაკლებად მზღუდავ, პროპორციულ და ეფექტურ საშუალებას დაავადების პრევენციის, კონტროლისა და მართვისათვის.

ამავდროულად, გაიზარდა შემთხვევები, როცა ჯანმრთელობის დაცვის დაწესებულებები ისე ამჟღავნებენ პაციენტთა პერსონალურ მონაცემებს, რომ მათგან არ იღებენ შესაბამის თანხმობას. მსგავსი შემთხვევები პანდემიამდე პერიოდშიც არაერთხელ დაფიქსირდა საქართველოში. თუმცა პანდემიით გამოწვეული რეალობა მსგავსი შემთხვევების სიმრავლით უფრო „განებივრებულია“, რადგან არსებულ რეალობაში უფრო მეტად არის მოთხოვნა ჯანრთელობის შესახებ ინფორმაციის გამჟღავნებაზე, ხოლო პაციენტთან კომუნიკაცია უფრო გართულებულია.

2.2. დამსაქმებელთა მიერ დასაქმებულთა ჯანმრთელობის შესახებ მონაცემთა დამუშავება

რაც შეეხება დამსაქმებელთა მიერ დასაქმებულთა ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავება, პანდემიით გამოწვეულ ერთგვარ საჭიროებას წარმოადგენს. არც საქართველოს კანონმდებლობა და არც საერთაშორისო აქტები (მაგალითად, როგორიცაა GDPR) არ ითვალისწინებს დამსაქმებლის ვალდებულებას მოითხოვოს და დაამუშავოს მასთან დასაქმებულის ჯანმრთელობის შესახებ პერსონალური ინფორმაცია.[31] ეს აქტუალური გახდა კორონავირუსის პანდემიის პირობებში, როცა თითოეული ადამიანის ჯანმრთელობის მდგომარეობის შემოწმება აუცილებელი გახდა, სხვათა ჯანმრთელობისა და სიცოცხლისათვის საფრთხის თავიდან აცილებისა და დასაქმებულთათვის უსაფრთხო სამუშაო გარემოს უზრუნველყოფის მიზნით.

საქართველოში არსებული რეგულირების საფუძველზე, დამსაქმებელს უსაფრთხო შრომითი გარემოს უზრუნველყოფის მიზნით შეუძლია დასაქმებულთა დაინფიცირების შესახებ ინფორმაციის შეგროვება, მათი თანხმობის არარსებობის მიუხედავად.[32] თუმცა, COVID-19-ით შეცვლილ გარემოებებში დამსაქმებელი ერთი მხრივ ვალდებულია დაიცვას დასაქმებულის

[30] „მონაცემთა იმგვარი მოდიფიკაცია, რომ შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას , ხარჯებსა და დროს საჭიროებდეს.“ იხ. სქოლიო 2, მუხლი 2, ქვეპუნქტი „რ“.

[31] D. Mikkelsen, H.Soller, M. Strandell-Jansson, How can European companies best prevent measures intended to control the COVID-19 pandemic from also undermining data privacy and security?, <https://mck.co/3bzHmvu> [უ.გ.08.01.2021]

[32] იხ. სქოლიო 2, მუხლი 6, პუნქტის2, ქვეპუნქტები „ა“ და „გ“.

ჯანმრთელობის შესახებ პერსონალური ინფორმაცია გასაჯაროებისგან, მეორე მხრივ კი უზრუნველყოს საზოგადოების ჯანმრთელობა და უსაფრთხოება.[33]

იმის გათვალისწინებით, რომ ვირუსი ძალიან სწრაფად ვრცელდება და მისი გავრცელების მიზეზი შეიძლება სრულიად უსიმპტომო ადამიანიც იყოს[34], ყველა დამსაქმებელმა, რომლებიც არადისტანციურ რეჟიმში მუშაობს, უნდა შეაგროვოს და გააზიაროს იმ მოცულობის ინფორმაცია, რაც საჭიროა ვირუსის გავრცელების პრევენციისა და თანამშრომლებისა და სამუშაო გარემოს უსაფრთხოებისთვის.

დამსაქმებლის მიერ ჯანმრთელობის შესახებ მონაცემთა შეგროვებისას ჩნდება პრობლემატური კითხვები, რომლებიც დეტალურად კანონმდებლობით არ არის მოწესრიგებული, კერძოდ: შეუძლია თუ არა მოსთხოვოს დასაქმებულებს ჯანმრთელობის მდგომარეობის შესახებ სამედიცინო დასკვნის წარდგენა ან შეუძლია თუ არა გაამჟღავნოს იმ პირის ვინაობა, რომელსაც დაუდასტურდა ან შესაძლოა დაუდასტურდეს კორონავირუსი? შესაბამისად, გამოიკვეთა რამდენიმე პრობლემატური შემთხვევა:

I. როცა დასაქმებული თვითონ გაუმჟღავნებს დამსაქმებელს, რომ დაუდასტურდა კორონავირუსი - დამსაქმებელს შეუძლია გაუზიაროს აღნიშნული ინფორმაცია იმ დასაქმებულებს, რომლებსაც კონტაქტი ჰქონდა დაინფიცირებულ თანამშრომელთან, თუმცა ეს არ გულისხმობს ინფიცირებულის ვინაობის გამჟღავნების აუცილებლობას. მოცემულ შემთხვევაში დამსაქმებლის მიერ მხოლოდ კორონავირუსის დადასტურების ფაქტის გაზიარება (დეპერსონალიზებული ინფორმაციის სახით) საკმარისია.

II. დამსაქმებელს შეუძლია აღნიშნული ინფორმაცია მიაწოდოს იმ თანამშრომლებსაც, რომლებთანაც ინფიცირებულს არ ჰქონია კონტაქტი. თუმცა აღნიშნულსაც აქვს კონკრეტული ფარგლები. იმ შემთხვევაში თუ დამსაქმებელს აქვს რამდენიმე ობიექტი და ინფიცირებული თანამშრომელი არასდროს ყოფილა რომელიმე სხვა დაწესებულებაში, ასეთ ობიექტში დასაქმებულების მიმართ ინფორმაციის გამჟღავნების საჭიროება არ არსებობს. დამსაქმებლის მიერ ინფორმაციის გამჟღავნების მსგავსი გადაწყვეტა გამართლებული იქნება როგორც ინფიცირებული, ასევე შესაძლო ინფიცირების შემთვევაში.

საყურადღებოა, რომ დამსაქმებლის მიერ, დაინფიცირებული დასაქმებულის ვინაობის სხვა დასაქმებულებისათვის გამჟღავნება დასაშვებია, თუ ეს აუცილებელია დასაქმებულთან კონტაქტში მყოფი პირების გამოსავლენად და ვირუსის შემდგომი გავრცელების პრევენციისთვის. ხოლო, იმ შემთხვევაში თუ დამსაქმებელს თანამშრომელი თავისი ინიციატივით, მიაწოდებს კორონავირუსით ინფიცირების უარყოფით პასუხთან დაკავშირებით ინფორმაციას, დამსაქმებელმა არ უნდა გაამჟღავნოს აღნიშნული ინფორმაცია, გარდა იმ შემთხვევისა, როცა აღნიშნულ პიროვნებას ჰქონდა სიმპტომები და მისი გამჟღავნება გამართლებულია მასთან კონტაქტში მყოფი დასაქმებულების ინფორმირების საჭიროებით.

III. დამსაქმებელს შეუძლია შეაგროვოს ინფორმაცია: დასაქმებული სტუმრობდა თუ არა ვირუსის გავრცელების მაღალ რისკის შემცველ ადგილებს, აქვს თუ არა დასაქმებულს ვირუსის სიმპტომები, ჰქონდა თუ არა კონტაქტი დაინფიცირებულ პირთან. თუმცა, როცა თანამშრომელი ავლენს კორონავირუსისათვის დამახასიათებელ სიმპტომებს, დამსაქმებელმა

[33] G. Cameron; Shilling, J. Weaver, How does covid-19 impact the privacy of health and personal information? 2020. იხ. <https://bit.ly/35AYXPM> [უ.გ. 08.01.2021].

[34] შესაძლოა თვითონ ამ ადამიანმაც არ იცოდეს, რომ კორონავირუსით ინფიცირებულია.

უპირველესად უნდა უზრუნველყოს აღნიშნული ადამიანის სამუშაო სივრცისგან იზოლირება იმ დროით, სანამ არ დადასტურდება ვირუსის არარსებობა. მსგავს სიტუაციაში, დამსაქმებელს შეუძლია დასაქმებულს მოსთხოვოს კორონავირუსის ტესტის პასუხის წარდგენა. თუმცა, როცა დასაქმებულს არ აღენიშნება რაიმე სიმპტომი, დამსაქმებლის მიერ თანამშრომლის დავალდებულება სამედიცინო დასკვნის წარდგენაზე - გაუმართლებელია.

3. პანდემიის პირობებში მედიის როლი ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა გასაჯაროებაში

პანდემიის პირობებში მედიის მიერ პირთა ჯანმრთელობის შესახებ პერსონალურ მონაცემთა გასაჯაროებამ რიგ შემთხვევაში გასცდა კანონით დადგენილი ლეგიტიმური მიზნების ფარგლებს. მსგავსი შემთხვევები მეტწილად გამოვლინდა ვირუსის გავრცელების საწყის ეტაპზე, როცა მედია საშუალებების მიერ გასაჯაროვდა კორონავირუსით ინფიცირებულთა ვინაობაც, მათთვის დამახასიათებელი სხვა დაავადებებიც და სხვა პერსონალური ინფორმაციებიც, როცა ამისი საჭიროება და აუცილებლობა არ არსებობდა.

„ჟურნალისტმა პატივი უნდა სცეს ადამიანის პირად ცხოვრებას და არ შეიჭრას პირად ცხოვრებაში, თუ არ არსებობს განსაკუთრებული საზოგადოებრივი ინტერესი.“[35] ქვეყანაში დაფიქსირდა თუ არა კორონავირუსის ახალი დადასტურებული შემთხვევა ეს ნამდვილად ექცევა საზოგადოებრივი ინტერესის ფარგლებში, თუმცა კონკრეტულად ვინ არის ეს პიროვნება, სად მუშაობს, ვისი ახლობელია და რამდენი ადამიანის დაინფიცირება გამოიწვია - ამ ინფორმაციის გასაჯაროება არ არის კანონიერი, რადგან აღნიშნული ინფორმაციის გასაჯაროებაც საჭიროებს ცალკე ლეგიტიმურ მიზანს და აღნიშნული პიროვნების თანხმობას.

მედიის მიერ ჯანმრთელობის მდგომარეობის შესახებ პერსონალურ მონაცემთა გასაჯაროება განსაკუთრებით პრობლემატურია ცნობილი ადამიანების, თანამდებობის პირების შემთხვევაში, რადგან ხშირად აღნიშნულ პირთა თანხმობა პერსონალურ მონაცემთა გამჟღავნებაზე არამარტო მედიას, არამედ მედიისთვის მიწოდებულ წყაროსაც არ აქვს.

4.COVID-19 პანდემიის პირობებში - ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული და გამოკვეთილი აქტუალური პრობლემები

სტატისტიკური მონაცემები, რომლებიც ასახავს კორონავირუსით ინფიცირებულების, გარდაცვლილების ან მისგან გამოჯანმრთელებულების შესახებ ინფორმაციას, წარმოადგენს პერსონალური მონაცემების დამუშავების შედეგს, რომელიც როგორც წესი მაქსიმალურად დეპერსონალიზებულია. თუმცა აღნიშნული მონაცემების დამუშავებისას გამოიკვეთა პრობლემატური საკითხები, რომლებმაც ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დაცულობა ეჭვქვეშ დააყენა.

4.1. კორონავირუსით ინფიცირებულ პირთა მარტივად იდენტიფიცირებადობა

კონკრეტული შემთხვევების განხილვამ ცხადყო, რომ ჯანმრთელობის შესახებ პერსონალური ინფორმაცია ისე ხდება მესამე პირებისათვის ხელმისაწვდომი, რომ კონკრეტული პირის იდენტიფიცირება ხშირად შესაძლებელია. კორონავირუსის პანდემიის პირობებში ნამდვილად არსებობს ჯანმრთელობის შესახებ პერსონალური მონაცემების დამუშავების

[35] პრინციპი 10, საქართველოს ჟურნალისტიკური ეთიკის ქარტია.

საჭიროება, თუმცა იმ მოცულობით, რაც აუცილებელია ლეგიტიმური მიზნების მისაღწევად. პრაქტიკაში კი ხშირად ხდება იმაზე მეტი ინფორმაციის გასაჯაროება ჯანდაცვის დაწესებულების ან დამსაქმებლისგან, რაც არ არის აუცილებელი და საჭიროების შესაბამისი. ზედმეტი და არასაჭირო ინფორმაციის გასაჯაროება კი, საბოლოოდ იწვევს ინფიცირებულთა იდენტიფიცირების შესაძლებლობას.

4.2. კორონავირუსით ინფიცირებასთან ერთად სხვა დაავადებების შესახებ ინფორმაციის გასაჯაროება

იმის გათვალისწინებით, რომ კორონავირუსით ინფიცირების დროს ჯანმრთელობის მდგომარეობის შეფასება დამოკიდებულია სხვა დაავადებების არსებობასთან,[36] კორონავირუსის პირობებში მიმდინარეობს პირისათვის დამახასიათებელი სხვა დაავადებების შესახებ ინფორმაციის დამუშავებაც. სწორედ ამიტომ, ზოგჯერ კონკრეტული ადამიანის არა მარტო კორონავირუსით ინფიცირების შესახებ ინფორმაციის გამჟღავნება ხდება, არამედ მისთვის დამახასიათებელი სხვა დაავადებების არსებობის თაობაზეც, რის მიმართაც ინფორმაციის გამცემ პირს შესაძლოა არ ჰქონდეს მიღებული პაციენტის თანხმობა.

4.3. საჯარო/საზოგადოებრივი ინტერესის ფარგლების განსაზღვრა

პანდემიის პირობებში საჯარო/საზოგადოებრივი ინტერესის ფარგლების განსაზღვრა ერთ-ერთი მიშვნელოვანი პრობლემა გახდა, რადგან საზოგადოებრივი ინტერესი იმაზე ფართოდ განიმარტება, ვიდრე ამას არსებული საჭიროებები მოითხოვს. მოცემულ შემთხვევაში ერთმანეთისგან უნდა გაიმიჯნოს საზოგადოების ინტერესების ორი ჯგუფი: ინტერესი, რომელიც ემსახურება ლეგიტიმური მიზნების მიღწევას, და მეორე ე.წ „ცნობისმოყვარე საზოგადოების“ უბრალო ინტერესები. ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემების გასაჯაროება სწორედ პირველი კატეგორიის საჯარო ინტერესების არსებობისას უნდა მოხდეს, რათა მონაცემთა მინიმიზაციის პრინციპი დაცული იქნეს[37] და არასაჭირო მონაცემების გასაჯაროებამ არ გამოიწვიოს პირისათვის მძიმე შედეგები.

4.4. უარყოფითი დამოკიდებულება

პანდემიის პირობებში ყველა ადამიანი ერთმანეთისთვის აღიქმება როგორც საფრთხის წყარო. სწორედ აღნიშნულმა გარემოებამ გამოიწვია საზოგადოებაში კორონავირუსით ინფიცირებულის, შესაძლო ინფიცირებულის, კონტაქტში მყოფის და უკვე გამოჯანმრთელებულის მიმართაც კი უნდობლობა და უარყოფითი დამოკიდებულება. შესაბამისად, კორონავირუსით ინფიცირების გამჟღავნებამ, შესაძლოა პირი დისკრიმინაციული ან სხვაგვარად მტრული მოპყრობის/დამოკიდებულების ობიექტად აქციოს, რასაც შეიძლება შედეგად მორალური ზიანი ან საზოგადოებისაგან მისი იზოლირება მოჰყვეს. ხშირ შემთხვევაში საზოგადოების მიერ აღქმული საფრთხე არარეალურია და ემოციები გადაჭარბებული, რაც ერთმანეთის მიმართ აგრესიაში ვლინდება.

[36] კონკრეტულად, მძიმე თუ სტაბილური მდგომარეობაა.
[37] Managing Employee Privacy in the Face of COVID-19, 19 მარტი, 2020. იხ. https://bit.ly/39uKhTk [უ.გ.10.01.2021]

აღნიშნული განსაკუთრებით, ვირუსის გავრცელების დასაწყისში გამოიხატა, როცა დისკრიმინაციული დამოკიდებულება ჩამოყალიბდა კონკრეტული ეროვნების წარმომადგენლების და ზოგადად უცხოელების მიმართ, როცა აღნიშნული ადამიანების მიმართ შიში ხშირ შემთხვევაში რეალურ საფუძვლებს მოკლებული იყო.

დასკვნა

ყოველივე ზემოაღნიშნულიდან გამომდინარე, კორონავირუსის პანდემიის პირობებში ნამდვილად არსებობს ჯანმრთელობის შესახებ პერსონალური მონაცემების დამუშავების საჭიროება (როგორც ჯანმრთელობის დაცვის სფეროში, ასევე დამსაქმებლების მიერ), თუმცა ეს არ გამორიცხავს პერსონალური მონაცემების კონფიდენციალურობის დაცვის ლეგიტიმურ ინტერესს. სწორედ ამიტომ ყოველ კონკრეტულ შემთხვევაში უნდა შეფასდეს რამდენად აღემატება ჯანმრთელობის მდგომარეობის შესახებ პერსონალური მონაცემის ღიაობის ინტერესი, აღნიშნულ პერსონალურ მონაცემთა კონფიდენციალურობის დაცვის ინტერესს. გაუმართლებელია ყოველგვარი დაფიქრებისა და საფუძვლის გარეშე საზოგადოების ცნობისმოყვარეობისათვის პრივილეგიის მინიჭება და მისი დაკმაყოფილება პერსონალურ მონაცემთა დაცულობის უგულებელყოფის ხარჯზე, რადგან პერსონალურ მონაცემთა (განსაკუთრებით, ჯანმრთელობის შესახებ მონაცემთა) დაცვა არანაკლებ ღირებული და ფასეული ინტერესია.

საქართველოში არსებული პერსონალურ მონაცემთა დაცვის საკანონმდებლო რეგულირება პანდემიის ან სხვა საგანგებო სიტუაციის დროს ხელს არ უშლის აუცილებელი ინფორმაციის გასაჯაროების პროცესს. აქედან გამომდინარე, აუცილებელია ჯანმრთელობის მდგომარეობის (და ასევე სხვა პერსონალურ მონაცემთა) შესახებ ინფორმაციის დამუშავება განხორციელდეს იმ დოზით, რაც აუცილებელია COVID-19 პანდემიის პირობებში ლეგიტიმური მიზნების მისაღწევად. წინააღმდეგ შემთხვევაში, თუ პანდემიის პირობებში, არ იქნება დაცული პირთა ჯანმრთელობის შესახებ ინფორმაცია და საზოგადოებრივ ინტერესებს მიენიჭება უპირატესობა, ადამიანები თავს შეიკავებენ სათანადო ორგანოებისათვის ინფორმაციის მიწოდებისაგან, რაც ვირუსის შემდგომი გავრცელების პრევენციას ხელს შეუშლის.

ბიბლიოგრაფია

1. საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N3/1/752 „ა(ა)იპ „მწვანე ალტერნატივა“ საქართველოს პარლამენტის წინააღმდეგ“, 2018 წლის 14 დეკემბერი;
2. საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N1/4/693,857 „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“, 2019 წლის 7 ივნისი;
3. საქართველოს ჟურნალისტიკური ეთიკის ქარტია;
4. საქართველოს კონსტიტუცია, 24 აგვისტო, 1995;
5. საქართველოს კანონი „ჯანმრთელობის დაცვის შესახებ“, 10 დეკემბერი, 1997;
6. საქართველოს კანონი „საექიმო საქმიანობის შესახებ“, 8 ივნისი, 2001;
7. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 28 დეკემბერი, 2011;
8. საქართველოს კანონი „პაციენტის უფლებების შესახებ“, 5 მაისი, 2000;
9. საქართველოს კანონი „ნავთობისა და გაზის შესახებ“, 16 აპრილი, 1999;
10. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაცია, „ჯანმრთელობის დაცვის სფეროში პერსონალური მონაცემების დამუშავების შესახებ“.
11. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „პერსონალურ მონაცემთა დაცვის შესახებ“;
12. Managing Employee Privacy in the Face of COVID-19, 19 მარტი, 2020. იხ. <https://bit.ly/39uKhTk> [უკანასკნელად გადამოწმდა10.01.2021];
13. Regulation (EU) 2016/679 „General Data Protection Regulation (GDPR)“, 25 მაისი, 2018. იხ. <https://bit.ly/2LhnHFV> [უკანასკნელად გადამოწმდა 05.01.2021];
14. Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson, How can European companies best prevent measures intended to control the COVID-19 pandemic from also undermining data privacy and security?, <https://mck.co/3bzHmvu> [უკანასკნელად გადამოწმდა 08.01.2021];
15. Cameron G. Shilling, John Weaver, How does covid-19 impact the privacy of health and personal information? 2020. იხ. <https://bit.ly/35AYXPM> [უკანასკნელად გადამოწმდა 08.01.2021].

Bibliography

1. Decision of the Constitutional Court of Georgia on the case N3/1/752 "Green Alternative" v. Parliament of Georgia", December 14, 2018;
2. Decision of the Constitutional Court of Georgia on the case N1/4/693,857 "Media Development Fund" and "Freedom of Information Development Institute" v. Parliament of Georgia, June 7, 2019;
3. Charter of Journalistic Ethics of Georgia;
4. Constitution of Georgia, August 24, 1995;
5. Law of Georgia on “Health Care”, December 10, 1997;
6. Law of georgia On “medical practice”, June 8, 2001;
7. Law of Georgia on “Personal Data Protection”, December 28, 2011;
8. Law of Georgia on “Patients' Rights”, May 5, 2000;

9. Law of Georgia on “Oil and Gas”, April 16, 1999;
10. Office of the Personal Data Protection Inspector, Recommendation on "Processing of personal data in the field of health care";
11. Explanatory Card on the Draft Law of Georgia on “Personal Data Protection”;
12. Managing Employee Privacy in the Face of COVID-19, March 19, 2020. <https://bit.ly/39uKhTk> [Last seen 10.01.2021];
13. Regulation (EU) 2016/679 „General Data Protection Regulation (GDPR)“, May 25, 2018. <https://bit.ly/2LhnHFV> [Last seen 05.01.2021];
14. Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson, How can European companies best prevent measures intended to control the COVID-19 pandemic from also undermining data privacy and security? <https://mck.co/3bzHmvu> [Last seen 08.01.2021];
15. Cameron G. Shilling, John Weaver, How does covid-19 impact the privacy of health and personal information? 2020. <https://bit.ly/35AYXPM> [08.01.2021].

დისტანციური სწავლების დროს სტუდენტების პერსონალური მონაცემების დაცვა

ოთარ მურმანიშვილი,
საქართველოს ტექნიკური უნივერსიტეტი

აბსტრაქტი

2020 წლის გაზაფხულის სემესტრიდან დისტანციური სწავლება არა მარტო საქართველოს, არამედ მთელი პლანეტის უმრავლესობას მოევლინა, როგორც ახალი ხილი გამოუვალ, მწარე რეალობაში. აქამდე თუ პირდაპირი სწავლების მეთოდს კონკურენტი არ ყავდა ახლა ზუსტად ამ მწარე რეალობამ მოითხოვა სწავლის მეთოდის მონოპოლიის ჩამოშლა.

დისტანციური სწავლება, როგორც ზემოთ ვახსენეთ ახალი ხილია და შესაბამისად მის ჩამოყალიბებაში ჩვენ შეგვიძლია დავუშვათ ის მომენტი, რომ თავისუფლად შეიძლება დაირღვეს სტუდენტის უფლება. ხშირ შემთხვევაში გაუთვალისწინებელი დაუდევრობით, ხოლო რიგ შემთხვევებში მიზანდასახულად. ასეა თუ ისეა შეცდომის მიზეზი ადამიანია. პერსონალური მონაცემის დაცვის გარანტი შეიძლება დარღვეულ იქნას დისტანციური სწავლების პლატფორმის პროგრამული უზრუნველყოფისას, ელექტრონულ სასწავლო საიტზე, სასწავლებლის სოციალურ გვერდებზე და სხვა პლატფორმებზე წარმოქმნილი ხარვეზების გამო. ასევე პერსონალური უფლებების დარღვევა შეიძლება მოხდეს, როგორც სასწავლებლის ადმინისტრაციისგან ისე აღმზრდელი პირებისაგანაც.

სურათის მარტივად დასანახად საჭიროა შემოვიტანოთ კიბერ უსაფრთხოების (**Cyber Security**), კერძოდ ეთიკური ჰაკერობის (**Ethical Hacking**) 3 ძირითადი მიმართულება და ავაგოთ კლასიფიკაცია 3 ტიპად:

- თეთრი - კომპიუტერის საშუალებით დისტანციური სწავლებისთვის განკუთვნილ საიტზე შესვლის შემდეგ ჩანს პირის პ/ნ: (მაგალითი)0123. ჩვენ ვიმყოფებით ამავე მონიტორის მახლობლად და თავისუფლად ვხედავთ (მაგალითი)0123-ს. შეგვიძლია ამოვიწეროთ ნომერი ჩუმად და დავადგინოთ პირის პერსონალური მონაცემები, მაგრამ მისთვის ზიანის მისაყენებელ არანაირ მოვლენას არ ვასრულებთ. ახლა ჩვენ გვაქვს ინფორმაცია, რომელიც წესით არ უნდა ვიცოდეთ. კანონის წინაშე დამნაშავენი ვერ ვიქნებით თუ ეს ინფორმაცია მივიღეთ ისეთი სისტემიდან, რომელიც თვითონ არ იცავს პერსონალურ მონაცემებს.
- ნაცრისფერი - ჩვენ ვამჩნევთ გარკვეულ დარღვევას სისტემაში და ვაფრთხილებთ სისტემის ხელმძღვანელს დაუყოვნებლივ, როგორც კონკრეტულ დარღვევაზე ისე სუსტი ბარიერის შესახებაც. ჩვენ სუფთად ვერ გამოვძვრებით ამ სიტუაციიდან, რადგან აბსტრაქტულად დავლაქავდით მიღებული ინფორმაციის გაცემით, თუმცა ამ სიტუაციიდან იმ მომენტს გამოვყავართ სუფთად, რომ ჩვენ შევასრულეთ სამოქალაქო მოვალეობა და გარკვეული დარღვევის აღმოჩენისთანავე ვაცნობეთ შესაბამის ორგანოს. მიუხედავად იმისა, რომ ის ინფორმაცია შეიძლება დაგვემახსოვრებინა რაც არ უნდა გვცოდნოდა კანონთან მიმართებაში უდანაშაულოები ვართ.
- შავი - ნაწილობრივ ანტი თეთრი კლასის ამსახველი კლასია. მომენტი, როდესაც (მაგალითი)0123 რიცხვები ამოვიწერეთ/დავიმახსოვრეთ და ბოროტად ვაპირებთ მის გამოყენებას. ამ შემთხვევაში კანონის წინაშე დამნაშავეები ვართ, მიუხედავად

იმისა გამოვჩნდებით თუ არა პოტენციური დაზარალებულის მხედველობის არეალში.

Abstract

From the spring semester of 2020, distance learning has appeared as a new fruit not only in Georgia, but also in the majority of the entire planet, in the bitter reality. Until now, if the method of direct teaching had no competitor, now it is precisely this bitter reality that has demanded the overthrow of the monopoly of the method of teaching.
Distance learning, as we have mentioned above, is a new fruit, and therefore in its formation, we can allow the moment when the student's right can be freely violated. Often in unintentional negligence, and some cases deliberately. One way or another, the cause of the error is human. The guarantee of personal data protection may be violated due to defects in the software of the distance learning platform, the e-learning site, the social pages of the university and other platforms. Both the university administration and educators can also violate personal rights.

To make the picture easier to see, we need to introduce the three main directions of cybersecurity, namely ethical hacking, and build a classification into three types:

- White - After entering the site for distance learning through a computer, you can see the person's ID: (example) 0123. We are near the same monitor and can see (example) 0123 freely. We can delete the number silently and verify the personal data of the person, but we do not take any action to harm him. Now we have information that we usually do not need to know. We will not be guilty before the law if we get this information from a system that does not protect personal data.
- Gray - We notice some breach in the system and warn the system administrator immediately about both a specific breach and a weak threshold. We can't get out of this situation cleanly, because we were abstracted by giving the received information. However, we get out of this situation cleanly from the moment that we have performed our civil duty and notified the relevant authority as soon as a certain violation is discovered. We heard information we should not have known. Nevertheless, we are innocent.
- Black - Partly anti-white reflecting class. The moment when (example) 0123 numbers are written off / memorized, and we are going to abuse person. In this case, we are guilty before the law, regardless of whether we appear in the sight of a potential victim.

შესავალი

ჩვენ დღეს განვიხილავთ 2020 წლის დასაწყისიდან „Covid-19"-ი ვირუსის გავრცელების შედეგად, რომელიც გადაიზარდა პანდემიაში, აღმოცენებულ პრობლემებს, როგორიცაა დისტანციური სწავლების დროს სტუდენტების პერსონალური მონაცემების (პირადი ნომერი, საცხოვრებელი მისამართი, მობილურის ან ტელეფონის ნომრები, სხვადასხვა საიტების პაროლები და ა.შ) დაცვა. ასევე იმ რისკებს თუ რა საფრთხის ქვეშ შეიძლება აღმოვჩნდეთ მონაცემების დაკარგვისას. ვის შეიძლება ჰქონდეს წვდომა ჩვენს პირად ინფორმაციაზე და როგორ შეიძლება ავამაღლოთ საზოგადოებაში განათლებისა და ცოდნიერების ის მიმართულება, რომელიც ასწავლის სტუდენტს მარტივი და საშუალო თავდაცვის ხერხებსა და მეთოდებს.

იქიდან გამომდინარე, რომ დისტანციური სწავლა თუ მუშაობა მოითხოვს კონტაქტს კომპიუტერისა და ინტერნეტის საშუალებით გაიზარდა და საკმაოდ დაიტვირთა ინფორმაციული ნაკადების მოცულობა ინფორმაციულ არხებში. ადამიანს, რომელსაც სურს მოიპოვოს სტუდენტზე ის ინფორმაცია, რომელიც პერსონალურია და დაცულია სახელმწიფოს შესაბამისი კანონმდებლობით მოუწევს მოქმედება ვირტუალურად, ასევე კომპიუტერისა და ინტერნეტის საშუალებით. საბოლოო ჯამში გაიზარდა ასეთი ადამიანების რაოდენობა, მათ კი **„კიბერ ჰაკერებს“ (Cyber Hacker)** ეძახიან. კომპიუტერულ მეცნიერებაში, კიბერ უსაფრთხოების ერთ-ერთი განხრა ეთიკური ჰაკინგი, რომელიც თავისმხრივ შეღწევადობას აღწერს, გვიხასიათებს მსგავს ჰაკერებს სამ ტიპად: თეთრი, ნაცრისფერი და შავი.

1. კიბერ ჰაკერთა კლასიფიკაცია და დეტალიზაცია

1.1 თეთრი ჰაკერი

თეთრი ჰაკერის მთავარი მიზანია მოიპოვოს მონაცემი ისე, რომ ვერც ადამიანმა, ვერც სათვალთვალო კამერამ და ვერც კომპიუტერულმა პროგრამებმა, ეგრედწოდებულმა „თაგვის ხაფანგებმა“, ვერ დააფიქსიროს მისი არსებობა. უნივერსიტეტში ახალწვეული სტუდენტის დარეგისტრირებისას სტუდენტის ინფორმაცია გადაეცემა დეპარტამენტიდან დეპარტამენტს და რამდენიმე ათეული ადამიანი მაინც კითხულობს ჩვენს პერსონალურ მონაცემს. ეს განსაკუთრებულად საშიშია ამ მომენტში, რადგან მსგავსი ინფორმაცია შესაძლოა მოძრაობდეს ახლა არა ხელიდან ხელში, არამედ ინტერნეტის საშუალებით და ეს უფრო საშიშია, მაშინ როდესაც ვიმყოფებით რუსეთის რეგიონთან, რომელსაც კიბერჰაკერთა ყველაზე ძლიერი კონტიგენტი ჰყავს. საბოლოოდ კი ეს ინფორმაცია ჩაეშვება კომპიუტერულ ქსელში. შეინახება ან შიდა უინტერნეტო სასერვერო ბაზაზე ან მაღალი დაცვის გარანტიის მქონე საიტზე. შესაძლოა ინფორმაციამ ამდენ მოძრაობაში გაჟონოს, ან უარესს შემთხვევაში ვინმეს ზედმეტად დავაინტერესდეთ. სტუდენტს ელემენტარული პირობების დასაკმაყოფილებლად უნდა შევუქმნათ შესაბამისი მომხმარებლის ანგარიში და პაროლი, რომელსაც სტუდენტი გამოიყენებს არა მარტო თავისი ნიშნების სანახავად, არამედ დისტანციური სწავლების პლატფორმაზე დასაშვებად და ბიბლიოთეკის მონაცემებზე წვდომისათვის. ძირითად შემთხვევაში ანგარიშის სახელი და პაროლი სტუდენტის პირადი ნომერია. რა შეგვიძლია დავადგინოთ სტუდენტის პირადი ნომრის გამოყენებით? ცესკო-ს საარჩევნო სიიდან შევძლებთ სტუდენტის ფაქტობრივი ან იურიდიული მისამართების დადგენას, პირადობის ნომერზე დატანილი ფოტოსურათის ნახვას, დაბადების თარიღის გაგებას (ზოგიერთი ადამიანი სუსტად დაცულ საიტებზე 21-ე საუკუნეში დღესაც კი თავის დაბადების წელს იყენებს პაროლად), მამის სახელს, რომელ საარჩევნო უბანზე შეუძლია ხმის მიცემა არჩევნების დროს და ასევე ამ მისამართებზე ჩაწერილი სხვა ადამიანებზე მწირე ინფორმაციას. გუგლის საძიებო სისტემაში შეგვიძლია გავიგოთ რას საქმიანობს ეს ადამიანი. მაგალითად: მონაწილეობას იღებს თუ არა ტენდერებში, იყენებს თუ არა საჯარო ან კერძო აუქციონის სისტემას, რომელიც საერთოდ არც კი მალავს ადამიანის პირად მონაცემს, როგორიცაა პირადი ნომერი, საჯარო რეესტრში არსებული მონაცემების შემთხვევაში რა სახის ქონებას ფლობს. საბოლოოდ კი ჩვენ უკვე ვიცით ადამიანის, კონკრეტულ შემთხვევაში კი სტუდენტის

საშუალო შემოსავალი, როგორც დღიური ისე თვიური, კვარტალური ან თუნდაც წლიური. ასევე შესაძლოა აღმოვაჩინოთ სტუდენტის სამსახურეობრივი ანკეტა, ე.წ. “CV”, რომელსაც მსოფლიო მასშტაბით მსგავსი საიტების ნახევარი პირდაპირ საჯაროდ დებს და არ საჭიროებს მისი ნახვა რამდენიმე საიტის გავლას, პირდაპირ ერთ კონკრეტულ მისამართზევე იხსნება. ასეთ წონიან ინფორმაციაზე დაყრდნობით შეგვიძლია ავაგოთ დაკვირვების ობიექტის სრული ანკეტა დაბადებიდან დღემდე. საბოლოოდ კი, როგორ გამოვიყენებთ ამ ინფორმაციას, თუ ვის გადავცემთ დამოკიდებულია ჩვენზე. პერსონალური ინფორმაციის მოპოვების მომენტში ჩვენ არსად გამოვჩენილვართ, ამიტომ აღვიწერებით როგორც თეთრნი.

1.2 ნაცრისფერი ჰაკერი

ნაცრისფერი ჰაკერი, როგორც ზემოთ ვახსენეთ, კანონმორჩილი და ძლიერი სამოქალაქო ვალდებულების გრძნობის მქონე პიროვნების შთაბეჭდილებას ტოვებს. ერთის მხრივ ის მუშაობს, ისევე სუფთად, როგორც თეთრი ჰაკერი, თუმცა ისეთივე უნარებითა და შესაძლებლობებით, როგორც შავ ჰაკერს ახასიათებს. ის დაინტერესებულია ნებისმიერი სახის სისტემის დაბალი ღობით, ე.წ. სისტემური ბზარებით და მისი აღმოჩენის შემთხვევაში სისტემის ადმინისტრატორს ან უშუალოდ მფლობელს ატყობინებს ქსელში ნაპრალის არსებობის შესახებ. ნაცრისფერი ჰაკერი არამარტო მაძებარი ძაღლივითაა, რომელიც საშველად ეძებს ადამიანს, არამედ სხვა ფუნქციებითაც შეიძლება გამოირჩეოდეს. ეს ფუნქციებია დარღვევის აღმოჩენის შემდეგ მფლობელისთვის შესაბამისი რეკომენდაციების გაცემა, დაკვალიანება, მცირე ტრენინგ-კურსის გავლა, უკეთეს შემთხვევაში კი ნაცრისფერი ჰაკერი თვითონვე ეხმარება მფლობელს პრობლემის აღმოფხვრაში. როდესაც დისტანციური სწავლების პლატფორმაზე ახალ დამზადებულ საიტთან გვაქვს შეხება, ხშირად ეს საიტი არ არის რომელიმე კონკრეტული ინსტრუქტაჟის ქვეშ დაგეგმილ-აწყობილი, არამედ დაკოპირებულია სხვა საიტების პროგრამული სკრიპტებისა თუ კოდების ბაზებიდან. ასეთი საიტი ვერასდროს ვერ დააკმაყოფილებს თითოეული მონაცემისთვის იდეალურ დაცვასა თუ მოვლას. მაგალითად შესაძლოა ყველასთვის თვალსაჩინოდ ჩანდეს, როგორც სტუდენტის, ისე ლექტორებისა თუ ადმინისტრაციის იმ თანამშრომლების პირადი ნომრები, რომლებიც უშუალოდ მუშაობენ დისტანციური სწავლების ამ პლატფორმაზე. ნაცრისფერი ჰაკერისთვის ეს ყველაზე ელემენტარული დავალებაა, როცა მას არ უწევს თვითონ რომელიმე საიტის გატეხვა სასურველი ინფორმაციაზე გზის გასაკვალად. მისთვის საჭირო ინფორმაცია პირდაპირ მის თვალწინ დევს. ჩვენ შეგვიძლია დავინახოთ სტუდენტის მიერ შესრულებული დავალებები ან საგამოცდო ნაშრომები. შესაძლოა საქმე გვქონდეს ისეთ გარღვევასთანაც, როდესაც საიტი გვაძლევს მასზე სრული კონტროლის აღების უფლებას. გამოდის, რომ მთელი უნივერსიტეტის არამარტო პერსონალურ, არამედ ყველა შესაძლო ელექტრონულ ინფორმაციაზე ვიღებთ წვდომას. ნებისმიერ შემთხვევაში, ჩვენი, როგორც ნაცრისფერი ჰაკერის, მოვალეობაა ამ ინფორმაციის დაცვა და მფლობელის ელემენტარულად საქმის კურსში ჩაყენება. ზუსტად ამიტომ გვქვია ნაცრისფერ ჰაკერებს ნაცრისფერები, რადგან ვიწყებთ მუშაობას, როგორც თეთრები და ჩვენს შესახებ ინფორმაცია არავის აქვს, ვიყენებთ შავი ჰაკერის უნარებს, რომ შევაღწიოთ იქ სადაც შესაბამისი ნებართვა არ გაგვაჩნია და ჩვენთვითონვე ვილაქავებთ ჩვენ თავს.

1.3 შავი ჰაკერი

შავი ჰაკერი გამოირჩევა თანამედროვე კომპიუტერული მეცნიერების უმაღლესი კატეგორიისა და ჯერ კიდევ შეუსწავლელი მეთოდების ცოდნით. მას არ სჭირდება მფლობელისა თუ ადმინისტრატორის ოფიციალური ნებართვა ნებისმიერი სახის ინფორმაციის მოსაპოვებლად. მისთვის არ არსებობს ბარიერი, რომელსაც ვერ გადალახავს. შავი ჰაკერი კიბერდანაშაულის ყველაზე დიდი პოპულარობით სარგებლობს. როგორ შეიძლება მოიპოვოს მან წვდომა იმ ინფორმაციაზე, რომლის შეფასების რანგსაც სენსიტიური ეწოდება? დისტანციურად კომპიუტერიდან კომპიუტერში შეღწევა ერთი შეხედვით საკმაოდ რთულია, თუმცა როგორც შუასაუკუნეების ანდაზა გვამცნობს „ციხე შიგნიდან ტყდება“. რას ნიშნავს ყოველივე ეს? შავი ჰაკერი შეეცდება ინფორმაციის ულუფა შემოგვთავაზოს, რომლის გააქტიურებაც უშუალოდ მისი გახსნის მომენტიდან იწყება. დიდი კომპანიებისა თუ ინსტიტუტების უმრავლესობა ყველა თავის თანამშრომელსა და მომხმარებელს აფრთხილებს, რომ არ მიაქციოს ყურადღება უცხო მეილებს, საეჭვო ინფორმაციას, საიტების ლინკებს, სხვადასხვა ფორმატის ფაილებს და არავითარ შემთხვევაში არ გახსნან ისინი. რატომ გვეშინია საეჭვო წყაროდან საეჭვო ინფორმაციის მიღების? შავი ჰაკერების უმრავლესობა გამოირჩევა ორმაგი სტანდარტის ტროას ვირუსის გამოყენებით. ეს შეიძლება იყოს როგორც ფაილის გადაგზავნით, რომელშიც იმყოფება არა მხოლოდ კონკრეტული ქვეფაილი, არამედ კიდევ დამალული ფაილიც. ამ დამალული ფაილისა თუ ფაილების შინაარსი იმაში მდგომარეობს, რომ მასში წინასწარაა გაწერილი თუ როგორ უნდა მოიქცეს პროგრამა გააქტიურებისას. ეს შეიძლება იყოს ადმინისტრატორის უფლებების მოპოვება, კონკრეტული ინფორმაციის ჩამოტვირთვა ბაზიდან, ასევე უშუალოდ კომპიუტერის ან სერვერის დაზიანება მასში მიმდინარე ელექტრული მოვლენების მონაცემებისა და გზების შეცვლით, ძაბვის დატვირთვით ან შემცირებით, რამაც შესაძლოა მიგვიყვანოს პერსონალური მონაცემის დაკარგვამდე. ტროას ვირუსის მეორე ვერსია გაცილებით უფრო რთულად შესაცნობია თანამედროვე კიბერ უსაფრთხოების სპეციალისტებისთვისაც კი. ვირუსის ამ მოდელში განიხილება კიბერ უსაფრთხოების ერთერთი განხრა, კერძოდ ღრმა ჩაშიფვრის მეთოდები. ამ შემთხვევაში ადამიანზე შეგროვებულ ინფორმაციაზე დაყრდნობით ვარჩევთ მისი ინტერესებისა და ასაკისთვის შესაბამის ინფორმაციას და ვაგებთ მსგავს საიტს, ფოტოს, ვიდეოს, აუდიო მასალას ან თუნდაც იგივე ფაილს. შემდეგ ღრმა ჩაშიფვრის მეთოდით შეგვყვავს მასში საკმაოდ დამალულად და შენიღბულად იგივე სახის ვირუსი, რომელმაც გააქტიურების მომენტიდანვე თავისი წინასწარ გაწერილი ბრძანება უნდა შეასრულოს. მსგავსი ვირუსის აღმოჩენის მომენტში ჩვენ ვაცნობიერებთ, რომ ჩვენს ხელთ არსებული ინფორმაცია საკმაოდ დიდი ხნის წინ დავკარგეთ. ვირუსი კი კომპიუტერში რჩება და შავ ჰაკერს შეუძლია ამ კომპიუტერში დამატებული ნებისმიერი ინფორმაციაც თან გაიყოლოს. საადმინისტრატორო უფლების მოპოვებით მას შეუძლია არამარტო ერთი, არამედ სისტემაში არსებული ნებისმიერი კომპიუტერისა და ინფორმაციული ულუფის მართვა. შეუძლია მისი სრული კოპირება სხვადასხვა საიტებზე გატანით ან შესაძლებლობის შემთხვევაში ერთი მაღალი მეხსიერების მქონე ბაზაზე შენახვით.

1.3.1 შავი ჰაკერისგან აღმოცენებული საფრთხე

რატომ უნდა გვეშინოდეს ყველაზე მეტად შავი ჰაკერების თუ ჩვენ სტუდენტები ვართ? შავ ჰაკერს, როგორც უკვე შევთანხმდით არ ადარდებს დაბრკოლებები და საზღვრები. წარმოვიდგინოთ, რომ ჩვენი ელექტრონული სწავლების პლატფორმაზე შესასვლელად

მხოლოდ პირადობის ნომერი გვჭირდება. ესე იგი შავ ჰაკერს შეუძლია ერთი პერსონალური მონაცემის გამოყენებით დაგვიწეროს, გაგვიფუჭოს ან საერთოდ წაგვიშალოს დავალებებისთვის განკუთვნილი დოკუმენტები. შეუძლია ჩვენ მაგივრად შევიდეს გამოცდაზე, სადაც მხოლოდ ერთხელ შესვლის უფლება გვაქვს და ჩვენ მაგივრად დაგვიწეროს გამოცდა ფრიადზე ან მიღებული ქულიდან გამომდინარე ჩაგვჭრას. ნებისმიერ შემთხვევაში მსგავსი ქმედება სასწავლებლის მიერ გასაცემი ან გაცემული დიპლომის გაყალბების ტოფლასია, რაც საერთო ჯამში გვაძლევს სისხლის სამართლის დანაშაულს, რომ აღარაფერი ვთქვათ იმაზე, რომ პერსონალური მონაცემის დაცვის გარეშე არამარტო ჩვენს მონაცემს არამედ ჩვენც კი შეიძლება შეგვექმნას სიცოცხლის საფრთხე რიგ შემთხვევებში.

2. ჰაკერთა მუშაობის პრინციპი

მუშაობის პრინციპის დასაწყისი თითქმის ნებისმიერ შემთხვევაში ერთნაირია. ჰაკერი ქმნის კომპიუტერში ვირტუალურ კომპიუტერს, ეგრედწოდებულ ვირტუალურ მექანიკურ სიმულაციას. ასეთ პროგრამაში მუშაობისას ჩვენ გვაქვს წვდომა ჩვენივე შექმნილ კომპიუტერთან სრულად. შეგვიძლია შევუქმნათ მას შეცვლილი ინტერნეტ მისამართი “IP Address”, შევცვალოთ ჩვენი კომპიუტერის უნიკალური მისამართი “MAC Address”, შევცვალოთ ჩვენივე კომპიუტერიდან გამოყენებული აპარატურის, როგორიცაა მყარი დისკი, ოპერატიული მეხსიერება და ა.შ, დასახელებები და გავიდეთ მსოფლიო ვებ ქსელში სრულიად უცხონი. ეს დაახლოებით იგივეა, რომ ყალბი პირადობის მოწმობით ვიმოძრავოთ და მას ყოველდღიურად ვიყენებდეთ. ნებისმიერი მოვლენის შესრულებისას ჩვენ ვტოვებთ ყალბ მისამართებსა და სახელებს, ამიტომ ჩვენი აღმოჩენა თითქმის შეუძლებელი ხდება. შესაძლოა საქართველოში არსებულ კომპიუტერს საქართველოდან შევუტიოთ, მაგრამ შენიღბულებმა, თითქოს შვეიცარიიდან ვუტევთ ან კანადიდან. შესაძლოა ადმინისტრატორისგან მისი დაქვემდებარებული თანამშრომლის კომპიუტერული მონაცემებით მოვითხოვოთ რაიმეზე ნებართვა და საბოლოოდ მიღებული ინფორმაციის შემდეგ უკვალოდ გავქრეთ, ხოლო სანამ სიტუაციაში გაერკვევიან ჩვენ უკვე სხვა სისტემას ვუტევთ.

3. ლაბორატორიული ექსპერიმენტი

გავეცნოთ ყველაზე მარტივ მაგალითს, კერძოდ თუ რა მოხდება იმ შემთხვევაში თუ „ციხე შიგნიდან გატყდება“.
ლექტორების უმრავლესობას დამახსოვრებული აქვს თავის კომპიუტერში დისტანციური სწავლების პლატფორმის საიტებზე ანგარიშის სახელი და პაროლი. როგორც ვიცით, ანგარიშის სახელი საიტების 99.9%-ში ღია და თვალსაჩინოა, ხოლო პაროლი პირიქით, შენიღბული. შენიღბვის ტიპად გამოიყენება “ Type=’password’ ”. თუ კი შავმა ჰაკერმა მოახერხა და რომელიმე ადამიანის მოტყუებით ციხე შიგნიდან გატეხა მას უკვე შეუძლია ლექტორის კომპიუტერის გამოყენება მაშინაც კი თუ ის გათიშულია, რადგან ის სრულ მონაცემებზე ფლობს კონტროლს. თუ კი ის იგივე ბრაუზერს გახსნის და დისტანციური სწავლების პლატფორმაზე შევა დაინახავს მომხმარებლის სახელსა და პაროლს, რომელიც დამახსოვრებულია და შევსებულია. მას პირდაპირ შეუძლია შევიდეს სისტემაში და შეცვალოს ქულები ერთ ან რამდენიმე სტუდენტზე. რა მოხდება იმ შემთხვევაში თუ ჰაკერს მონაცემი პერიოდულად ჭირდება და არ სურს დროის დაკარგვა მის მოსაპოვებლად? ბრაუზერში სასწავლო საიტზე გადასვლისას, რამდენადაც სამწუხარო არ უნდა იყოს, საიტის შიგნით

მაუსის მარჯვენა ღილაკზე დაკლიკვით იხსნება შემდეგი ფანჯარა, რომლის ბოლოშიც ვნახავთ "inspect"-ს, რომელიც მოკლედ იხსნება "CTRL+SHIFT+I" კომბინაციის გამოყენებისას. საიტზე ვხედავთ, რომ გაიხსნა ახალი ფანჯარა. ამ ფანჯარაში საიტის დამალული მხარეა, წინასწარ გაწერილი საიტის პროგრამის ნაწილი დაწერილი "Java"-ს ენაზე. უშუალოდ ავტორიზაციის გრაფაზე ინსპექტირებით ვგებულობთ, რომ ანგარიშის სახელის გრაფა დაუცველი და თვალსაჩინო კლასისაა, ხოლო პაროლის გრაფა სტანდარტული "Type='password'" კლასის. თუ კი ამ ფანჯარაში ინგლისურ სიტყვას პაროლს ამოვშლით და საიტის კოდს გავუშვებთ ხელახლა, მაშინ პაროლის გრაფაში რაც წერია ან რასაც დავწერთ უახლოს მომავალში საიტის დარესტარტებამდე ყველაფერი გამოჩნდება ისე, როგორი თვალსაჩინოცაა ანგარიშის სახელი.

4. პრაქტიკული ექსპერიმენტი

1) ვხსნით საიტს „Elearning.gtu.ge",[1] რომელზეც დამახსოვრებულია პირის პერსონალური მონაცემები;

2) ვხსნით საიტის საინსპექციო ფანჯარას;

```
<input type="password" name="password" id="password" value class="form-con
trol" placeholder="პაროლი"> == $0
</div>
```

3) სკრიპტიდან ტიპური კლასიფიკაციისგან ამოვიშლით პაროლის გრაფის აღმნიშვნელ სიტყვას.

```
<input type name="password" id="password" value class="form-control"
placeholder="პაროლი"> == $0
```

[1] Elearning.gtu.ge [უ.გ.4.02.2021]

4) პაროლის გრაფა ღიაა. მონაცემები მოპოვებულია წარმატებულად და უსაფრთხოდ.

სახელი: ლექტორი#0123456789
პაროლი: 1970

შენიშვნა: ზემოთ მოყვანილ ფოტოებში აღნიშნული მონაცემები მხოლოდ სამაგალითოა და არ ემთხვევა რეალურ მონაცამებს!

5. სასწავლო და აზარტული პლატფორმების შედარება

აქვე გვიჩნდება კითხვა, თუ რატომ სამწუხარო? შევადაროთ ერთმანეთს ადამიანი და ფული. რომელი უფრო მნიშვნელოვანია? რათქმაუნდა ადამიანი. ახლა შევადაროთ განათლებისთვის დისტანციური სწავლისა და გასართობი აზარტული თამაშების პლატფორმა. კაზინო არასდროს მოგვცემს იმის საშუალებას, რომ მის საიტზე მსგავსი ინსპექტირება მოვახდინოთ, რადგან მისთვის ძირითად ინტერესს ფული წარმოადგენს. დისტანციური სწავლების პლატფორმაზე კი სადაც ფული არაა და ადამიანის პერსონალური მონაცემია, დიახ, მონაცემი რომლის გასაჯაროვებამ და ბოროტად გამოყენებამ შეიძლება ადამიანის სიცოცხლეს ან მისი განათლების ხარისხს საფრთხე შეუქმნას, აქ სამწუხაროდ ინსპექტირება ნებადართულია.

დასკვნა

როგორ შეიძლება ვებრძოლოთ, თუნდაც იმ გამოწვევას, რასაც ციხის შიგნიდად გატეხვა ეწოდება და რატომ მაინცდამაინც ამ კონკრეტულს? იმიტომ, რომ სხვისი პერსონალური მონაცემის მოპარვის, ნახვისა თუ გამოყენების საუკეთესო მაგალითია და ყველაზე გახშირებული. კარგი იქნებოდა, რომ აღსაზრდელებს, არამარტო სტუდენტებს ასევე მოსწავლეებსაც, ინფორმატიკის გაკვეთილზე ასწავლიდნენ ვირტუალური კომპიუტერის გამოყენებას, რადგან მსგავს ვირტუალურ მანქანაში გახსნილი თუნდაც ტროას ვირუსი ამ

მანქანის ფარგლებს გარეთ ვერ გამოდის. თუ ვირუსს აღმოვაჩენთ სრულიად უსაფრთხოდ შეგვიძლია წავშალოთ ვირტუალური მანქანის მეხსიერება და ხელახლა ჩავრთოთ ის და ასევე უსაფრთხოდ შეიძლება გადამოწმდეს ნებისმიერი საეჭვო ინფორმაცია უცხო პირებისგან მოწოდებული. ერთის მხრივ თუ განათლების სამინისტრო ამ მიმართულებით მსგავს რეფორმას გაატარებს და სასწავლებლებში დანერგავს ამ მოცემულობას ის არამარტო კომპიუტერულ თავდაცვას ასწავლის აღსაზრდელებს, არამედ უფრო მეტად დააინტერესებს მათ კომპიუტერული მეცნიერების მიმართულებით, რაც საკმაოდ მაღალანაზღაურებადი საქმეა დღეს. ეს კონკრეტული პროგრამა კი შეგვიძლია უფასოდ ვიშოვოთ ინტერნეტ სივრცეში, შესაბამისად თანხის ხარჯვა ამ მიმართულებით იქნება დაყვანილი მინიმალურამდე, ხოლო შედეგი იქნება კატასტროფულად მაქსიმალური.

ასევე კარგი იქნება ჩვენს მიერ გამოყენებულ კომპიუტერებში სამუშაოს დასრულების შემდეგ თუ წავშლით ბრაუზერის და პროგრამის გამოყენების ისტორიას მისი არსებობის შემთხვევაში. აქვე საკმაოდ დიდი უპირატესობა მიენიჭება პერსონალური მონაცემის გახსნამდე მის შენიღბვას. პერსონალური მონაცემების მონიტორზე გამოსატანად საჭიროა ისინი დაფარული იყოს, ამ დროს ჩვენ უნდა დავრწმუნდეთ, რომ არ ვიმყოფებით საჯარო სივრცეში, როგორიცაა კომპიუტერების კაფე, სადაც ადმინისტრატორს აქვს უფლება უყუროს ჩვენს ეკრანზე მიმდინარე ნებისმიერ პროცესს, ამასთანავე უნდა დავრწმუნდეთ, რომ ჩვენს ირგვლივ სიახლოვეში არ დგას ადამიანი, რომელიც მას დაინახავს. ყოველივე ამის შემდეგ შეგვიძლია მოვხსნათ დაცვის სისტემა და დავინახოთ ჩვენი პერსონალური მონაცემ(ებ)ი. მსგავსი ელემენტარული დონის ცოდნით ჩვენ სამომავლოდ თაობების მასშტაბით ავირიდებთ ამ და სხვა გარღვევებისგან თავს.

ბიბლიოგრაფია:

1. Elearning.gtu.ge [უკანასკნელად გადამოწმდა 4.02.2021]

Bibliography

1. Elearning.gtu.ge [Last seen 4.02.2021]

COVID-19-ის პანდემიის პირობებში ონლაინ მომსახურებისას პერსონალური მონაცემების დაცვა

სალომე ზეინკლიშვილი,
თავისუფალი უნივერსიტეტი

აბსტრაქტი

თანამედროვე მსოფლიოში პერსონალურ მონაცემთა გამჟღავნებისა თუ გავრცელების უმნიშვნელოვანესი საშუალება ონლაინ სივრცეა. აქედან გამომდინარე, ონლაინ სივრცეში პერსონალურ მონაცემთა დაცვა ყოველთვის აქტუალური პრობლემაა. ცალსახაა, რომ ამ მხრივ ონლაინ მომსახურების სფერო საჭიროებს დიდ ყურადღებას, რადგანაც ამ სერვისის გაწევისას ხშირია სხვადასხვა სახის თაღლითობა და პერსონალური მონაცემების უკანონოდ მოპოვება. აშკარაა, რომ დღევანდელობაში ონლაინ მომსახურებისას პერსონალური ინფორმაციის დაცულობა საზოგადოდ სერიოზული საფრთხის წინაშეა, ამ მდგომარეობას კიდევ უფრო ამწვავებს COVID-19-ის პანდემიით გამოწვეული შედეგები. კერძოდ, უკანასკნელი ერთი წლის განმავლობაში მნიშვნელოვნად გაიზარდა ონლაინ მომსახურების სფერო. ამის გათვალისწინებით მოცემული საკითხი დღევანდელ მსოფლიოში იმაზე უფრო აქტუალურია, ვიდრე ოდესმე.

როგორც უკვე აღინიშნა, Covid-19-ის პანდემიიდან გამომდინარე წარმოუდგენლად გაიზარდა ონლაინ სერვისების რიცხვი თუ სახეები. ამ ყველაფრის შედეგად გამწვავდა არამხოლოდ ონლაინ მომსახურებასთან დაკავშირებული სხვა პრობლემები, არამედ გაჩნდა უამრავი ახალი შესაძლებლობა იმისათვის, რომ მომხმარებელთა პირადი ინფორმაციის დაცვა არ მოხდეს კანონის შესაბამისად. ამავე დრო გაიზარდა ის რისკები, რომლებსაც მომხმარებლები ონლაინ მომსახურების მიღებისას აწყდებიან.

ამასთანავე მნიშვნელოვანია ამ საკითხის აქტუალობა იმ კუთხითაც, რომ საზოგადოების დიდი ნაწილი მოწყვლადია მოცემული პრობლემების წინაშე, რადგანაც არ აქვს სრული ინფორმაცია იმ საფრთხეებზე, რაც შეიძლება პირადი მონაცემების ინტერნეტის სახით გამჟღავნებას მოჰყვეს. ამასთანავე საზოგადოების დიდი ნაწილი პანდემიამდე ამჯობინებდა მომსახურება არ მიეღო ონლაინ, შესაბამისად მათ არამარტო თავის დაცვის შესაძლებლობა არ აქვთ პირადი მონაცემების გამჟღავნების ნაწილში, არამედ შესაძლოა სრულიად გაუცნობიერებლად შეუწყონ ხელი საკუთარი მონაცემების უსაფრთხოების დარღვევას.

აუცილებელია იმ ფაქტორის ხსენებაც, რომ მოცემული საკითხი აქტუალურია არამხოლოდ მოკლე ვადიან პერსპექტივაში, არამედ სამომავლოდაც. კერძოდ, პანდემიის ჩავლის შემდეგ, მოცემულ პირობებში გამჟღავნებული მონაცემების გამოყენება შესაძლოა კვლავ გაგრძელდეს კანონსაწინააღმდეგოდ. ამის გათვალისწინებით, საფრთხე სულ სხვა მასშტაბებს იძენს, რაც საჭიროებს შესაბამის ყურადღებას, განხილვასა და დამუშავებას.

ზემოთ თქმულიდან გამომდინარე, ესეში განხილული იქნება არამხოლოდ მოცემული პრობლემის აქტუალობა, არამედ ის კონკრეტული საფრთხეები, რაც შესაძლოა მოცემულმა საკითხმა წარმოშვას. ასევე წარმოჩენილი იქნება სხვადასხვა ზომები, რომლებიც მიიღო ამა თუ იმ ქვეყანამ, რათა შეემცირებინა მოცემულ საკითხთან დაკავშირებული რისკები. ამავე დროს,

ყურადღება გამახვილდება იმაზეც, თუ როგორ იქნება შესაძლებელი ხსენებული პრობლემების თავიდან არიდება დღევანდელობაში თუ სამომავლოდ.

საკვანძო სიტყვები: პერსონალური მონაცემები, ციფრული ხანა, კიბერდანაშაული, ფიშინგი, თაღლითობა, მონაცემების დამუშავება/გამოყენება

Abstract

The most important means of disclosure or dissemination of modern internet is personal data in the online space. Because of this, the protection of personal data in the online space is always a topical issue. This is necessary for online areas that require a lot of attention, at this type of service often involves various types of fraud and illegal extraction of personal data. The protection of personal information in online services today poses a serious threat to society in general, exacerbated by the effect of the COVID-19 pandemic. In particular, the field of online services has grown significantly over the past years. Given this, the issue is more relevant in today's world than ever before.

As already mentioned, the number and types of online services have increased dramatically since the COVID-19 pandemic. All of the exacerbated not only other problems with online services but also created numerous new opportunities to ensure that users' personal information is not protected under the law. At the same time, the risks users face when receiving online services have increased.

At the same time, it is important to address this issue in the sense that a large part of the public is vulnerable to these problems, as it does not have full information about the dangers that may result from the disclosure of personal data via the internet. At the same time, a large part of the public before the pandemic preferred not to use the service online, therefore they not only do not have the opportunity to protect themselves in the disclosure of personal data, but may unknowingly contribute to the breach of their own data security.

It is also necessary to mention the factor that the given issue is relevant not only in the short run, but also in the future. In particular, after the onset of pandemic, the use of data disclosed under these conditions may continue to be illegal. With this in mind, the threat takes on a whole other scale that requires appropriate attention, consideration and handling.

Given the above, the essay will discuss not only the urgency of the given problem but also the specific threats that the given issue may pose. It will show the various measures taken by this or hat country to reduce the risks associated with the issue. At the same time, the focus will be on how it will be possible to avoid these problems now or in the future.

Key words: Personal data, Digital age, Cyber crime, Phishing, Scam, Data processing

შესავალი

პერსონალური მონაცემების დაცვა წარმოადგენს თანამედროვეობის ერთ-ერთ უმთავრეს გამოწვევას. პერსონალური მონაცემები დაცული უნდა იყოს ისეთი რისკებისგან როგორიცაა, მათი დაკარგვა, გამჟღავნება, შეცვლა ან არაუფლებამოსილი პირის მიერ გამოყენება. დასახელებული რისკები რეალური და საკმაოდ საშიშია, რადგანაც ამ ქმედებებმა შესაძლოა პიროვნებას შეუქმნას ისეთი პრობლემები, რომელთა გადაჭრაც არც ისე მარტივია.

პერსონალური მონაცემების შეგროვება, გენერალიზაცია და გამოყენება გლობალური ეკონომიკის თვალსაზრისით მომგებიანია, ამ ყველაფერს შეუძლია ბევრი ბენეფიტის მოტანა ყოველდღიურობისათვის. ადამიანს მსოფლიოს ერთი კუთხიდან შეუძლია მიიღოს მომსახურება მსოფლიოს მეორე კუთხეში მყოფი კომპანიისგან. კომპანიები და მომხმარებლები კი ამით იღებენ სარგებელს, რაც ეფექტურ მარკეტინგსა და მომსახურებაში გამოიხატება.

თუმცა უამრავი უპირატესობის მიუხედავად, ციფრულ ერას მოჰყვა მზარდი გამომწვევები, რაც დიდწილად პირადი ინფორმაციის დაცვას უკავშირდება. ტექნოლოგიურმა პროგრესმა საფუძველი დაუდო მასიური მონაცემების შეგროვებისა და გაანალიზების სხვადასხვა საშუალებას. შესაბამისად, პერსონალური მონაცემების დიდი რაოდენობა ერთადაა თავმოყრილი, რაც ყოველთვის კარგ გამოსავალს არ წარმოადგენს.

1.COVID-19-ის პანდემიის პირობებში ონლაინ მომსახურებისას პერსონალური მონაცემების დაცვა

ზემოთ თქმულიდან გამომდინარე, პერსონალურ მონაცემთა დაცვა უფრო და უფრო მნიშვნელოვანი ხდება საერთო დაცულობის შეგრძნებისათვის. ამაში, ცხადია, დიდ წილს თამაშობს ის ფაქტორიც, რომ თანამედროვეობაში, სხვადასხვა ტექნოლოგიისა და სქემის გამოყენებით კიდევ უფრო გაადვილდა პერსონალური ინფორმაციის მოპოვება არაკანონიერად. ამის საპასუხოდ კი აუცილებელია ამ საფრთხის თავიდან ასაცილებლად ისეთი მექანიზმების შექმნა, რომელიც მათ ჯეროვან წინააღმდეგობას გაუწევს. მაშასადამე, სწრაფ ტექნოლოგიურ განვითარებასთან ერთად საჭირო გახდა თავის დაცვის საშუალებების განახლებაც, რათა მომხდარიყო ნაბიჯის აწყობა ციფრული ხანისათვის.

პერსონალური ინფორმაციის დაცვისათვის ორი მნიშვნელოვანი პრინციპის გათვალისწინებაა აუცილებელი, პირველს წარმოადგენს მოცემული ინფორმაციის დამუშავების კანონიერება, მეორეს კი ამ ინფორმაციის სუბიექტის თანხმობა და გამომყენებლის უფლებამოსილება ხელი მიუწვდებოდეს მონაცემებზე. პირს მხოლოდ მაშინ შეუძლია ინფორმაციის გამოყენება, როდესაც კანონის თანახმად ან პირის თანხმობის შედეგად აქვს ამის შესაძლებლობა, მაგალითად, როდესაც ინტერნეტ სერვისის მიღებისას პირი აცხადებს თანხმობას, რომ მისი მონაცემები გამოყენებულ იქნას პირობების შესაბამისად.[1]

როგორც უკვე აღინიშნა, მნიშვნელოვან საკითხს წარმოადგენს პერსონალურ მონაცემთა დაცვა ციფრულ ეპოქაში. ეს განსაკუთრებით უკავშირდება ინტერნეტს. ვინაიდან ამ ეპოქაში მომხმარებელი მოწყვლადია ინტერნეტ-თაღლითობასთან, ყოველდღიურად ხდება ახალი საშუალებების გამოყენება, რათა პირადი მონაცემების მოპოვება არაკანონიერად მოხდეს. ამასთანავე, ინტერნეტის საშუალებით პირადი ინფორმაციის მოპოვების უამრავი ხერხი არსებობს. მნიშვნელოვანია იმ ფაქტის აღნიშვნაც, რომ ეს სირთულეს არ წარმოადგენს, მითუმეტეს, რომ ადამიანთა უმეტესობა ინტერნეტში ინფორმაციას ზედმეტი დაყოვნებისა და ფიქრის გარეშე ავრცელებს. ეს ეხება ონლაინ მომსახურებასაც.

გასაკვირი არაა, რომ ეს პრობლემა COVID-19-ის გამოჩენის გამო ბევრად გამწვავდა. ახალი კორონა - ვირუსის გამო მსოფლიოს მასშტაბით მასობრივად მოხდა ყველა შესაძლებელი

[1] ევროპის კავშირი „Privacy and data protection“, 2020 წელი,https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo [უ.გ.11.12.2020]

საქმიანობის ონლაინ სივრცეში გადატანა. აღმოჩნდა, რომ მსგავს საქმიანობათა ჩამონათვალი არც ისე მცირეა, ხოლო ეს საქმიანობები მოითხოვს პირადი ინფორმაციის გამჟღავნებას. შესაბამისად, გაჩნდა ახალი საფრთხეები და გამწვავდა ძველი პრობლემები.

ონლაინ სივრცეზე მორგება მოუწიათ არამარტო სხვადასხვა სფეროს დამსაქმებლებს და დასაქმებულებს, არამედ სასწავლო დაწესებულებებს, სხვადასხვა სერვისის მიმწოდებლებს. ამავე დროს, გაიზარდა ონლაინ შეკვეთა ისეთ პროდუქტებზე, როგორიცაა საკვები და სურსათი. ონლაინ პლატფორმაზე გადაერთო დიდწილად ჯანმრთელობის სექტორიც და სხვა ორგანიზაციებიც.

კოვიდ-19-მა ზეგავლენა მოახდინა არა მხოლოდ ეკონომიკაზე, საზოგადოებაზე და ურთიერთობებზე, არამედ გარკვეულწილად მოხდა იმის ფორმირებაც თუ როგორ აღიქვამს საზოგადოება პირად ცხოვრებას, ამავე დროს ამ მოვლენამ დიდი გავლენა მოახდინა იმაზე თუ რამხელა მნიშვნელობის მინიჭება ხდება პირადი მონაცემების დაცვისათვის. პანდემიის პირობებში აუცილებელი გახდა ფუნდამენტურ უფლებებს შორის ბალანსის დაცვა.

როგორც უკვე აღინიშნა, მონაცემების დაცვა შესუსტდა ისეთ სფეროშიც, რომელიც პირდაპირ კავშირში არაა ვირუსის გავრცელებასთან, ამაში იგულისხმება ონლაინ მომსახურების სფერო. აუცილებელია, საჯარო ინტერესისა და პირადი ცხოვრების ხელშეუხებლობის უფლების შეპირისპირებისას პერსონალური მონაცემების დაცვის საკითხი შეფასდეს ფუნქციურად. ეს იქიდან გამომდინარეობს, რომ მოცემული უფლება კავშირშია არამარტო პირადი ცხოვრების ხელშეუხებლობასთან, არამედ პირადი განვითარებასთანაც. ამიტომაც არასწორია მისი უკანა პლანზე გადანაცვლება. ამის ნაცვლად უნდა მოხდეს ბალანსის დაცვა და ამ უფლების სრულყოფილად დაცვისათვის საჭირო რესურსის გამოყოფა.

პერსონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობის უფლება ერთმანეთთან მკაფიო კავშირშია, უპირველესად, უნდა აღინიშნოს, რომ ისინი იცავენ მსგავს ღირებულებებს, ისეთ ღირებულებებს როგორიცაა ავტონომია, პირის ღირსება და ინდივიდუალობა, ასევე განუსაზღვრავენ ადამიანს პერსონალურ სფეროს, რომელშიც მან თავისუფლად უნდა განავითაროს საკუთარი თავი. ადამიანის უფლებათა ევროპული სასამართლოს 8(2) მუხლში სწორედ ეს აზრია განმტკიცებული.[2]

ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეში Murray v. United Kingdom პირადი მონაცემები, როგორცაა პირის სახელი, გვარი მისამართი და ა.შ. განიხილა პირადი ცხოვრების უფლების ხელშეუხებლობასთან დაკავშირებით.[3] ეს გულისხმობს, რომ სასამართლო პერსონალურ მონაცემებს უკავშირებს პირადი ცხოვრების უფლებას. სასამართლო პერსონალურ მონაცემად განიხილავს არამარტო სახელს, გვარს და მსგავს ინფორმაციას, არამედ სექსუალურ ორიენტაციას და რელიგიურ მრწამსსაც კი.[4]

[2]მუხლი 8, „ადამიანის უფლებათა ევროპული კონვენცია“ 1998, https://www.echr.coe.int/documents/convention eng.pdf [უ.გ. 11.12.2020].

[3] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N18731/91 “Murray v. United Kingdom”, 1994 წლის 28 ოქტომბერი, პარაგრაფები 83-90.

[4] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N 30562/04 „S. and Marper v. the United Kingdom“, 2008 წლის 4 დეკემბერი, პარაგრაფი 43.

პირადი ცხოვრების უფლება და პერსონალურ მონაცემთა დაცვის უფლება წარმოადგენს ფუნდამენტურ უფლებებს, თუმცა ისინი არაა აბსოლუტური, რაც იმას ნიშნავს, რომ შესაძლებელია მათი შეზღუდვა, თუკი ამისათვის საკმარისი საფუძველი იარსებებს.[5]

ამ ნაწილში აუცილებელია მოცემული უფლებების შედარება. კრიზისის დროს შესაძლებელია ზოგიერთ უფლებას უფრო პრიორიტეტული ადგილი მიენიჭოს. როგორც უკვე აღინიშნა, პირადი მონაცემების დაცვის უფლება ფუნდამენტური უფლებაა და მისგან მომდინარეობს სხვადასხვა უფლების სრულყოფილად გამოყენების საფუძველიც, თუმცა შესაძლებელია მისი შეზღუდვაც. ეს ხდება მაშინ, როდესაც საჯარო ინტერესი და კონკრეტული გარემოებები იძლევა იმის საშუალებას, რომ მოხდეს მოცემულ უფლებაში ჩარევა. კოვიდ-19-ის პანდემია ასეთი გარემოებების რიცხვში ექცევა.

ბალანსის დადგენის ერთ-ერთი საუკეთესო ტესტი აქვს ადამიანის უფლებათა ევროპულ სასამართლოს. ამ სასამართლოს პრაქტიკის თანახმად, ბალანსის დადგენისას რამდენიმე მნიშვნელოვანი ფაქტორი უნდა იყოს გათვალისწინებული, მათ შორის ერთ-ერთია ის თუ რა სიკეთე შეუძლია მოიტანოს მოცემული მონაცემების გასაჯაროებამ. ევროპის ადამიანის უფლებათა სასამართლომ საქმეში Társaság A Szabadságjogokért v. Hungary დაადგინა, კრიტერიუმი, რომლის გამორკვევაც უნდა მოხდეს ბალანსის დადგენისას. ხსენებული კრიტერიუმი წარმოადენს იმ მიზანს თუ რა მიზნითაც პირადი მონაცემების მიღებაა აუცილებელი. მოცემულ შემთხვევაში ამ მიზანს წარმოადგენს კორონა ვირუსის გავრცელების პრევენცია, რაც საკმაოდ ვალიდური მიზეზია.[6]

მოცემული უფლება ფართოდაა ინტერპრეტირებული სასამართლოს პრაქტიკაში და კონვენცია 108-ში. მოცემული კონვენცია ფარავს ყველა იმ ოპერაციასა და ქმედებას, რაც ინტერნეტში მონაცემების დამუშავებასა და მოპოვებას ეხება. მოცემულ კონვენციაში ისიცაა აღნიშნული, რომ უმნიშვნელოვანესია პირს ჰქონდეს ინფორმაცია იმის შესახებ თუ როგორ ხდება მისი პერსონალური მონაცემების დამუშავება და გამოყენება. მოცემული კონვენციის თანახმად, პერსონალური მონაცემები კანონის შესაბამისად უნდა იყოს გამოყენებული, მხოლოდ გათვალისწინებული მიზნით.[7] ამავე დროს, მოცემული კონვენცია მიუთითებს, რომ პირს უნდა ჰქონდეს საშუალება მართოს მისი პერსონალური მონაცემების ბედი, კერძოდ მას აქვს უფლება მოითხოვოს წაშლა ან თავად წაშალოს ინტერნეტიდან პერსონალური მონაცემები.

ევროპის კავშირის ფუნდამენტური უფლებების შესახებ აქტის 52(1)-ის თანახმად, უფლებაში ჩარევა მხოლოდ მაშინ დაიშვება თუ ეს ყველაფერი ობიექტურად საჭიროა საზოგადო/საჯარო ინტერესისათვის.[8] მაშასადამე, მოცემული აქტი თანხვედრაშია ადამიანის უფლებათა ევროპული სასამართლოს მიდგომასთან.

---

[5] ევროპული კომისია "ფუნდამენტური უფლებები", ხელმისაწვდომია აქ: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/fundamental-rights_en [უ. გ. 12.10.2021].

[6] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე 37374/05 „Társaság A Szabadságjogokért v. Hungary", 2009 წლის 14 აპრილი, პარაგრაფი 164.

[7] იხ. შენიშვნა 1.

[8] 52(1) „ევროპის კავშირის აქტი ფუნდამენტური უფლებების შესახებ", 2012 წლის 26 ოქტომბერი https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT [უ.გ. 12.10.2020].

ევროპის კავშირის გენერალური მონაცემების დაცვის რეგულაცია ამ ყველაფერს ამატებს დეტალურ განმარტებებს. ის მიუთითებს, რომ მონაცემების დაცვა ყოველთვის უნდა განიხილებოდეს არა ცალკეულად, არამედ ფუნქციურად მასთან დაკავშირებულ სხვა საკითხებთანაც, მაგალითად თუ რა მნიშვნელობა აქვს მას საზოგადოებისათვის.[9]

ასევე, პერსონალური მონაცემების დაცვის გენერალური რეგულაციის თანახმად,(GDPR) მონაცემები მხოლოდ იმ სპეციალური მიზნით უნდა იყოს გამოყენებული რისთვისაცაა მოთხოვნილი, წინააღმდეგ შემთხვევაში მათი გამოყენება უფლების დარღვევად ჩაითვლება.[10]

პანდემიის შედეგად საფრთხის ქვეშ დადგა ადამიანთა ჯანმრთელობა, ამიტომაც საჯარო ინტერესს მიენიჭა უპირატესობა, ამ ყველაფრის ფონზე კი პირადი მონაცემების დაცვა სხვადასხვა ასპექტში შესუსტდა. პირველ რიგში, სამედიცინო თვალსაზრისით პერსონალური მონაცემები დაუცველი გახდა, ამავე დროს ზოგიერთ ქვეყანაში ვირუსის გავრცელების პრევენციისათვის იყენებენ სხვადასხვა სისტემას, რომელიც პირის კონტაქტებსა და გადაადგილებას ადგენს. როგორც უკვე აღინიშნა, საფრთხე შეექმნა პირადი მონაცემების დაცვას ონლაინ სივრცეშიც.

ახალი კორონა - ვირუსის პანდემიის დაწყებისთანავე, ონლაინ სივრცეში გამოჩნდა უამრავი აქტორი, რომელიც მიზნად ისახავდა სხვადასხვა ორგანიზაციისა თუ კომპანიის სახელის გამოყენებას იმისათვის, რომ მოეპოვებინა პირადი მონაცემები კანონსაწინააღმდეგო გამოყენებისათვის. ამასთანავე, გაიზარდა ისეთი შეტყობინებების რაოდენობა, რომელიც პირებს სხვადასხვა სერვისს სთავაზობდა, სანაცვლოდ კი პერსონალური ინფორმაციის გადაცემას მოითხოვდა.

ამასობაში სიახლეებს უნდა მორგებოდნენ არამარტო მომხმარებლები, არამედ სხვადასხვა სერვისის მიმწოდებელი კომპანიებიც. მათ მოუწიათ სრულიად ონლაინ სივრცეზე მორგება და ამასთანავე ონლაინ შეკვეთების სწრაფად მზარდი ტალღისთვის გამკლავება, რა პროცესშიც შესაძლოა ისე ვეღარ დაეცვათ თავი კიბერშეტევებისგან, როგორც აქამდე იცავდნენ. უმეტესად, ასეთი კომპანიების რესურსის მობილიზება მოხდა მზარდი მომსახურების შეკვეთის გამკლავებისკენ და არა პირად მონაცემთა დაცვის გაძლიერებისკენ. ამავე დროს, ისიც უნდა აღინიშნოს, რომ მოცემულ პირობებში შეუძლებელია ონლაინ მომსახურებისათვის თავის არიდება.

აშკარაა, რომ ამ ყველაფერმა გაზარდა ფიშინგისა(phishing) და სხვადასხვა კიბერდანაშაულის დონე, ასევე შეიქმნა კიბერდანაშაულის ახალი ტექნიკები, 2020 წლის მარტში ფიშინგის შემთხვევები თითქმის 600 პროცენტით იყო გაზრდილი.[11] მოცემული სქემა მოიცავს პირის დარწმუნებას, რომ გასცეს გარკვეული ინფორმაცია, ეს კი კიბერდამნაშავეებისთვის დიდ შესაძლებლობას წარმოადგენს და განსაკუთრებით შესაძლებელია მისი გამოყენება ონლაინ

[9] „მონაცემთა დაცვის გენერალური რეგულაცია“ (GDPR) 2016 წლის 14 აპრილი, https://gdpr-info.eu/ [უ.გ. 15.03.2020]
[10]ინფორმაციული კომისიის ოფისი “მონაცემთა დაცვის გენერალური რეგულაცია, პრინციპენო, მიზნები, ფარგლები“ 2020, https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-general-data-protectionregulation- gdpr/principles/purpose-limitation/ [უ.გ. 12.01.2020]
[11] ბარაკუდა, „კორონა ვირუსთან დაკავშირებული ფიშინგი.“, 2020 წლის 26 მარტი. ხელმისაწვდომია: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ [უ.გ. 12.10.2020]

მომსახურების სფეროში. ფიშინგი უმეტესად გულისხმობს ელექტრონული წერილების გაგზავნის გზით ადამიანთა მოტყუებით პერსონალური მონაცემების მოპოვებას.[12]

გავრცელებული სქემების თანახმად, დამნაშავეები აყალბებენ სხვადასხვა მომსახურების ვებ - გვერდს, მომხმარებელი ამ სერვისის გამოყენებისას არ აკვირდება ვებ-გვერდს, და პირადი მონაცემები დაუფიქრებლად შეჰყავს, ამას კი ძალიან ხშირად მოჰყვება ფინანსური თაღლითობა, ანგარიშიდან თანხის ჩამოჭრა ან უფრო რთული პრობლემები. კვლევებმა აჩვენა, რომ გაზრდილი თაღლითობების დიდი ნაწილი ხდება სხვადასხვა მომსახურების მიმწოდებლის ბრენდული სახელის გამოყენებით თაღლითების მიერ. ხშირ შემთხვევაში პირი ტყუვდება და მის პერსონალურ მონაცემებს გადასცემს თაღლითს, რომელიც რეალურად არაა იმ მომსახურების მიმწოდებელი რაც მას სურს.

გასაკვირი არაა, რომ აუცილებელია ამ კუთხით ცნობიერების ამაღლება, ამასთან დაკავშირებით იზრდება კიდეც ცნობიერება და უამრავი ადამიანი მსგავსი მაქინაციების პირისპირ უფრო დაკვირვებული გახდა ბოლო პერიოდში. თუმცა, კოვიდ-19-ის შედეგად ონლაინ მომსახურებაზე გადასვლა მოუწიათ ისეთ ადამიანებსაც, ვინც სხვა შემთხვევაში ამ გზას არ გამოიყენებდა მომსახურების მისაღებად. ცხადია, რომ ასეთი ადამიანები განსაკუთრებით მოწყვლადი არიან პერსონალურ მონაცემებთან დაკავშირებული დანაშაულების თვალსაზრისით. ამის რამდენიმე მიზეზი არსებობს; პირველ რიგში მათ არ იციან სხვადასხვა დანაშაულის შესახებ და არ იჩენენ სიფრთხილეს, რაც განსაკუთრებით საჭიროა პანდემიის დროს, ამასთანავე ისინი არც იმას აქცევენ ყურადღებას თუ რა დოზით უნდა მოხდეს პირადი მონაცემების გაზიარება და ვისთვის.

ამ მოწყვლადი ჯგუფის გარდა საფრთხეში არიან ისეთი ადამიანებიც, ვინც საკმაოდ დიდ ყურადღებას აქცევენ მსგავს დეტალებს და მაქსიმალურად ცდილობენ თავი დაიცვან მათი პირადი მონაცემების არაკანონიერად გამოყენებისგან. ეს იქიდან გამომდინარეობს, რომ ახალი კორონა-ვირუსის დაწყებისთანავე ონლაინ სივრცე უკიდურესად გადაიტვირთა, შესაბამისად პრაქტიკულად შეუძლებელია მისი საფუძვლიანად კონტროლი. ამასთანავე, მთელი რესურსი მიმართულია არა პირადი მონაცემების დაცვისაკენ, არამედ საზოგადოებრივი კეთილდღეობისა და კორონა ვირუსის გავრცელების პრევენციისკენ.

კვლევებმა ასევე აჩვენა, რომ ცხოვრების სტილის შეცვლამ და სამუშაო სივრცის სახლში გადანაცვლებამ ადამიანებს მისცა მეტი თავისუფალი დრო, რამაც გაზარდა მათი აქტიურობა ონლაინ სივრცეში, იქნება ეს სოციალური ქსელები თუ ონლაინ მომსახურება. ასევე ცნობილი გახდა, რომ კოვიდ-19-ის პანდემიის დროს სტრესისა და შფოთვის ფონზე (სოციალური აქტივობების ნაკლებობა კარანტინში, მენტალური ჯანმრთელობის პრობლემები) გაიზარდა იმის შანსი, რომ ადამიანი გახდეს უმიზნო შეტევის ადრესატი კიბერდამნაშავეებისგან.[13]

ამავე დროს, კვლევაში გამოიხატება მოსაზრება, რომლის თანახმადაც სამუშაო ადგილების დაკარგვამ პანდემიისას გამოიწვია ის, რომ ბევრი უმუშევარი ადამიანი უფრო მეტ დროს ატარებს სახლში და შესაბამისად უფრო მეტია შანსი, რომ ისინი კიბერდანაშაულს ჩაიდენენ. ამხელა ზრდის ფონზე კი აუცილებელია კანონისმიერი ზომები, რომლებიც ამ დანაშაულებს აღმოფხვრის.

[12]იხ. შენიშვნა 10.
[13]იხ. შენიშვნა 10.

უნდა აღინიშნოს ისიც, რომ მომხმარებლის მიერ ყველა საფრთხის გაანალიზების შემთხვევაშიც კი შესაძლებელია მათი პირადი მონაცემების გამჟღავნება. ამ შემთხვევაში პასუხისმგებლობა სერვისის მიმწოდებელ მხარეზე გადადის. ამ საფრთხეში იგულისხმება ის შემთხვევა, როცა კიბერდამნაშავეებს ეძლევათ შესაძლებლობა თავს დაესხან ონლაინ მომსახურების ამა თუ იმ სერვერს და მოიპოვონ მასზე არსებული ინფორმაცია, რაც უმეტესწილად მოიცავს ამ სერვისის მომხმარებელთა პირად მონაცემებს. ამის პრევენციისათვის აუცილებელია მოხდეს ამ სფეროს უფრო ეფექტიანად დაცვა სერვისის მიმწოდებელთა მხრიდან, თუმცა მოცემულ პანდემიაში ეს დაცვა არა თუ გაიზარდა, არამედ შემცირდა, ვინაიდან, როგორც უკვე აღინიშნა, კომპანიებისათვის პრიორიტეტს წარმოადგენს მომატებული მოთხოვნების შესრულება მომხმარებელთათვის და არა მათი პირადი მონაცემების დაცვა.

აქედან გამომდინარე, პერსონალური ინფორმაციის არაკანონიერად გამოყენებისა და დამუშავების საფრთხის თავიდან აცილებისათვის საჭირო ზომების მიღება უმეტესად თავად მომსახურების მიმწოდებელ კერძო კომპანიების მოუწევთ, ამისათვის კი სხვადასხვა გზა არსებობს. იმისათვის, რომ კრიზისში პერსონალურ მონაცემთა დაცვა ხარისხიანად განხორციელდეს ორგანიზაციებსა და მომსახურების მიმწოდებელ კომპანიებს მოეთხოვებათ გაატარონ კიბერუსაფრთხოების ის საშუალებები, რომლებიც ზემოთ ნახსენებ საფრთხეებს აღმოფხვრის. მათი ვალდებულებაა ეს ინფორმაცია შეინახონ და დაიცვან. თავის მხრივ, მომხმარებლებს შეუძლიათ მეტი ყურადღებით დააკვირდნენ თუ ვის გადასცემენ პერსონალურ მონაცემებს.

თავდაპირველად მომსახურების მიმწოდებლებმა ობიექტურად უნდა განსაზღვრონ თუ რა ინფორმაციაა საჭირო იმისათვის, რომ მომსახურების მიწოდება სრულყოფილად მოხდეს, ამ გზით მომხმარებელს აღარ მოუწევს ზედმეტი ინფორმაციის მიწოდება მისთვის, რაც თავის მხრივ მოახდენს პრევენციას, რათა ზედმეტი ინფორმაციის არაკანონიერად დამუშავება არ მოხდეს.

მნიშვნელოვანია, რომ პერსონალური მონაცემების გადამუშავება და შენახვა ორგანიზაციებსა თუ კომპანიებს მხოლოდ იმ პერიოდით შეეძლოთ რა პერიოდითაც ეს მონაცემები სჭირდებათ, თუმცა ხშირ შემთხვევაში ამის დაცვა არ ხდება. ონლაინ მომსახურება იძლევა შესაძლებლობას პირადი მონაცემების შენახვა მოხდეს იმაზე უფრო დიდი ხნით ვიდრე ეს საჭიროა, რადგანაც ონლაინ სერვერზე ინფორმაციის განთავსების შემდეგ მისი შენახვა სირთულესთან არ ასოცირდება. მაშასადამე, ეს იძლევა არამარტო იმის საშიშროებას, რომ პირი დაუყოვნებლივ გახდება კიბერდანაშაულის მსხვერპლი, არამედ შესაძლოა ეს რისკი განხორციელდეს განუსაზღვრელ მომავალში. ეს დამატებით სირთულესთან ასოცირდება, ვინაიდან მომხმარებელს არ უნდა ჰქონდეს იმის მოლოდინი, რომ მისი მონაცემების გამოყენება შესაძლოა სამომავლოდ მოხდეს მისი ნებართვის გარეშე.

ამ თვალსაზრისით უმჯობესი იქნება თუკი მოცემული ინფორმაცია გარკვეული დროის შემდეგ წაიშლება. ცხადია, მონაცემების წაუშლელად დატოვება გარკვეული პროცესების გაადვილებასთან ასოცირდება მომხმარებლისათვის, თუმცა მოცემულ ვითარებაში მათი დროდადრო წაშლა უფრო დაცულს გახდის პირს. იქნება ეს გარე კიბერშეტევის შემთხვევა თუ თავად მომსახურების მიმწოდებლის მიერ არაკანონიერად მონაცემების გამოყენება.

ამასთანავე, მომსახურების მიმწოდებლებს შეუძლიათ გამოიყენონ ონლაინ პლატფორმები იმისათვის, რათა გააფრთხილონ მომხმარებლები და მიაწოდონ მათ ინფორმაცია იმის შესახებ თუ როგორ უნდა დაიცვან თავი პერსონალური მონაცემების არაუფლებამოსილი პირისადმი განდობისგან. ამასთანავე, მათ შეუძლიათ მიაწოდონ მომხმარებლებს ის ინფორმაცია, რომელიც უშუალოდ მათი სერვისის მიწოდებას უკავშირდება, მაგალითად ვებ-გვერდისა თუ აპლიკაციის ორიგინალური მახასიათებლები, რათა მომხმარებელმა არ დაუშვან შეცდომა და თავი აარიდონ კიბერდამნაშავეების მახეებს, მაგალითად ფიშინგს.

პერსონალური მონაცემების დამუშავება ასევე ძლიერი იარაღია კორპორაციების ხელში, დღეს ასეთ კორპორაციებს აქვთ დეტალური ინფორმაცია ადამიანის ფინანსური სიტუაციის შესახებ. რისკები უმეტესად უკავშირდება იმ საშიშროებას, რომ ინფორმაცია შესაძლოა აღმოჩნდეს არაუფლებამოსილი პირის ხელში. კომპანიამ შესაძლოა თავად გამოიყენოს მოცემული მონაცემები არაკანონიერად, უფლებამოსილების ფარგლების დარღვევით.

საბოლოოდ, აუცილებელია, ონლაინ მომსახურების მიმწოდებლებმა თავად გააძლიერონ კიბერუსაფრთხოება, ვინაიდან ყველა ზემოთ ჩამოთვლილი ხერხი ამაო იქნება, თუკი კიბერდანაშაულის შედეგად სერვერის დაზიანება და სხვადასხვა პერსონალური მონაცემის ამ გზით მოპოვება გახდება შესაძლებელი.

დასკვნა

ზემოთ მოყვანილი მსჯელობიდან გამომდინარე, პანდემიამ კიდევ უფრო მძაფრად წარმოაჩინა საჭიროებია იმისა, რომ ციფრულ ერაში პერსონალური მონაცემების დაცვისათვის დამატებითი მექანიზმების გამოყენებაა აუცილებელი. კომპანიები, რაც უფრო მეტ ინფორმაციას იღებენ მით უფრო მეტ ძალაუფლებას იძენენ, ამ მხრივ ყველაზე დიდი ინფორმაცია მოცემულ პერიოდში დიდმა კორპორაციებმა მიიღეს, რომელთაც პირადი მონაცემების დიდი რაოდენობა გააჩნიათ. მოცემული ინფორმაციის არაუფლებამოსილი პირის ხელში ჩავარდნა კი სავალალო შედეგებს გამოიწვევს.

ამასთანავე, იმისათვის, რომ არ მოხდეს უფლების დარღვევა, აუცილებელია „ოქროს შუალედის“ პოვნა. მაშასადამე იმ ბალანსში, სადაც პერსონალურ მონაცემთა დაცვის უფლება და საჯარო ინტერესი დგას სასწორზე აუცილებელია ბალანსის დაცვა მომხმარებელსა და სერვისის მიმწოდებლის უფლება - მოვალეობებს შორისაც.

იმ შემთხვევაში თუკი ფუნდამენტურ უფლებებს შორის დადგინდება აუცილებელი ბალანსი, ამავე დროს მომსახურების მიმწოდებელი და მიმღებიც გაატარებენ საჭირო ზომებს თავის დასაცავად, პერსონალური მონაცემები იმაზე ბევრად დაცული გახდება მომავალში, ვიდრე ახლაა.

ბიბლიოგრაფია:

1. ბარაკუდა „კორონა ვირუსთან დაკავშირებული ფიშინგი.“, 2020 წლის 26 მარტი https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ [უკანასკნელად გადამოწმდა 12.10.2020];
2. „მონაცემთა დაცვის გენერალური რეგულაცია“ (GDPR) 2016 წლის 14 აპრილი, https://gdpr-info.eu/ [უკანასკნელად გადამოწმდა 15.03.2020.];
3. 52(1) „ევროპის კავშირის აქტი ფუნდამენტური უფლებების შესახებ“, 2012 წლის 26 ოქტომბერი,https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT [უკანასკნელად გადამოწმდა 12.10.2020];
4. ადამიანის უფლებათა ევროპული კომისია, 1998 ;
5. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე 37374/05 “Társaság A Szabadságjogokért v. Hungary“, 2009 წლის 14 აპრილი;
6. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N 30562/04 „S. and Marper v. the United Kingdom“, 2008 წლის 4 დეკემბერი;
7. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე N18731/91 “Murray v. United Kingdom”, 1994 წლის 28 ოქტომბერი;
8. ევროპის კავშირი „Privacy and data protection“, 2020 წელი, https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo [უკანასკნელად გადამოწმდა 12.10.2020];
9. ევროპის კომისია, “ფუნდამენტური უფლებები”,https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/fundamental-rights_en [უკანასკნელად გადამოწმდა 12.10.2020.];
10. ინფორმაციული კომისიის ოფისი “მონაცემთა დაცვის გენერალური რეგულაცია, პრინციპენო, მიზნები, ფარგლები“ 2020, https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/purpose-limitation/ [უკანასკნელად გადამოწმდა 12.01.2020.].

Bibliography:

1. ECHR case: 37374/05 Társaság A Szabadságjogokért v. Hungary, 14/4/2009;
2. European convention on human rights, 1998;
3. European Commission “fundamental rights”, access: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/fundamental-rights_en [Last seen 12.10.2020];
4. „Privacy and data protection “, Council of Europe, last modified 2020, Access: https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo[Last seen 12.10.2020];
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1;

6. The Information Commissioner's Office, "General data protection regulation (gdpr): Principle (b): Purpose limitation," 2020, https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/purpose-limitation/[Last seen 12.01.2020];
7. ECHR case: N18731/91 "Murray v. United Kingdom", 28/10/1994;
8. Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02;
9. „coronavirus-related phishing." Barracuda, last modified March 26, 2020. access: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/[Last seen 12.10.2020];
10. ECHR case: N 30562/04 „S. and Marper v. the United Kingdom, 4/12/2008.

არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარების საფრთხეები.

ნანა მახარაძე,
თბილისის სახელმწიფო უნივერსიტეტი

აბსტრაქტი

წინამდებარე ნაშრომის კვლევის საგანს წარმოადგენს არასრულწლოვანთა პერსონალური მონაცემების ინტერნეტში გაზიარებიის საფრთხეები. დღესდღეისობით მსოფლიოში გავრცელებული პანდემიის ფონზე, სხვადასხვა ქვეყნის მოსახლეობა უფრო მეტად დამოკიდებული გახდა ონლაინ პლათფორმებზე. ძალაუნებურად გვიწევს ყოველდღირად საათობით დრო გავატაროთ ონლაინ სივრცეში, მაგრამ არასრულწლოვნების შემთხვევაში საქმე უფრო რთულ ვითარებასთან გვაქვს. არასრულწლოვნები ხშირ შემთხვევაში ისე გადართული არიან ონლაინ სივრცეში რომ რეალობას მოწყვეტილნი აღარ ეკონტაქტებიან ოჯახის წევრებსაც კი ნაკლებად გათვიცნობიერებული არიან პერსონალური დაცვის საკითხებში, ისინი ხშირად მიდრეკილნი ხდებიან ისეთი საგნების მიმართ, რომელთა დადებითი მხარეები სათუოა. როგორ უნდა დავიცვათ ისინი ონლაინ სივრცის საფრთხეებისგან? რა მოვიქმედებოთ მათი პერსონალური მონაცემების დასაცავად? ჩვენი ეპოქის თანმდევი აქტუალური საკითხია არამატო საქართველოში, არამედ მთელ მსოფლიოში. ამ პრობლემის გადასაჭრელად საჭიროა თავად კონკრეტული საფრთხეები გამოვკვეთოდ. არასრულწლოვნებთან დაკავშირებული პერსონალური მონაცემების დაცვის თემატიკა, საფრთხეები, რეკომენდაციები და მაგალითები მოწოდებული უნდა იყოს ორი ასპექტით განპირობებული:

- არასრულწლოვნები 6 წლიდან – 10 წლამდე
- არასრულწლოვნები 10წლიდან–17წლამდე.

ასეთი დაყოფა დაგვეხმარება უკეთ გამოვკვეთოთ ასაკობრივი საფრთხეები და შესაბამისი რეკომენდაციები გავცეთ. მაგალითად: 6 წლიდან 10 წლამდე არასრულწლოვნები რომ დავიცვათ კიბერბულგისგან, უნდა დავიხმაროთ თავად მშობლები, რომელთა ჩარევაც და კონტროლიც სავალდებულოა მათი შვილების კეთილდღეობისთვის. ხოლო რაც შეეხება 10 წლიდან 17 წლამდე არასრულწლოვნებს აქ უკვე მეტი მუშაობა არის საჭირო,უფრო მეტ საფრთეებსა და პრობლემებს ვაწყდებით.მათი კონტროლი ხშირ შემთხვევაში შეუძლებელია,მშობლებისგან დამალული მოქმედება- ონლაინ სივრცეში ხოლმე საუბედურო შედეგამდე მიგვიყვანს. განსაკუთებით მნიშვნელოვანი ფაქტორია კიბერბულინგი, რადგან ამ შემთხვევაში არასრულწლოვანის მხოლოდ პერსონალურ მონაცემთა დაუცველობის გარდა ფსიქოლოგიურ ტრავმასთანაც გვაქვს საქმე. ეს ნათელი მაგალითია, იმას თუ როგორი ზიანი შეიძლება მოუტანოს მოზარდს ონლაინ სივრცემ, როგორ იწვევს პერსონალური მონაცემების დარღვევა, არასრულწლოვანის ცხოვრების დანგრევასა და უნდობლობას. ამის გარდა, საინტერესეო თავად ამერიკის შეერთებული შტატების მაგალითი და საერთოდ როგორ უმკლავდებიან წამყვანი ქვეყნები ასეთ დაბრკოლებებს. შედარებითსამართლებრივი ანალიზი დაგვეხმარება ჩვენი ქვეყნის არასრულწლოვნების პერსონალური მონაცემების დაცვაში, ინტერნეტში გავრცელებული პირადი ინფორმაციის გაზიარების შედეგად გამოწვეული საფრხეების შემცირებასა და უკეთესი პრევენციის განხორციელებაში.

საკვანძო სიტყვები: კიბერბულინგი, მშობელების როლი, შედარებითსამათლებრივი ანალიზი, პრევენციის გზები .

Abstract

The subject of the present study is the dangers of sharing personal data of minors on the Internet. In the face of the pandemic that is spreading around the world today, people in different countries have become more dependent on online platforms .But juveniles are often so switched on online that they are disconnected from reality and no longer have contact with even family members who are less aware of personal protection issues, they are often prone to subjects whose positive aspects are questionable. How can we protect them from the dangers of online space? What can we do to protect their personal data? The current issue of our era is relevant not only in Georgia, but all over the world. To solve this problem, we need to identify specific threats. The topics, threats, recommendations and examples of personal protection related to minors should be provided in two aspects: Minors from 6 to 10 years, Minors from 10 to 17 years.

Such a division will help us better identify age-related threats and make appropriate recommendations. Cyberbullying is a particularly important factor, because in this case, to protecting only the personal data of the juvenile, we are also dealing with psychological trauma. This is a clear example of how it leads to the violation of personal data, the destruction of a minor's life and mistrust. In addition to the interesting example of Germany and the United States themselves how leading countries deal with such obstacles - comparative legal analysis will help us to protect the personal data of our country's minors, reduce the risks posed by sharing personal information spread on the Internet and better prevention.

Key words: cyberbullying, parent role, recommendations, ways of prevention.

შესავალი

ჩვენ ვცხოვრობთ საინფორმაციო ტექნოლოგიების რევოლუციურად განვითარებულ მსოფლიოში, შესაბამისად თანამედროვე ცხოვრების განუყოფელ ნაწილად იქცა სოციალური ქსელები, ინტერნეტ სამყარო რომელიც საზოგადოების ყველა სფეროში გვესაჭიროება. საზღვრების, დისტანციის, ხანგრძლივი მანძილის მიუხედავად ადაიანები ვახერხებთ ურთიერთობას. მსოფლიო შეიცვალა გამარტივდა ადამაინური ურთიერთობები, მაგრამ უფრო მეტი საფრთხები წარმოეშა ადამიანის უფლებებს.თანამედროვე საზოგადოებამ გამარტივებული ურთიერთობების გარდა შეისწავლა პირველადი ინფორმაციის, სწორედ, სოციალური ქსელების მეშვეობით გავრცელება. სამწუხაროდ, ზრდასრული პირების გარდა ასეთ საქმიანობას უფრო მეტმა არასრულწლოვანმა მიჰყო ხელი. ამას კი თან ერთვის მშობლების ინიციატივით გასაჯაროვებული არასრულწლოვნების ვიდეოები, ფოტოები როელიც მხარს უჭერს და ახალისებს მოზარდებს, რომ დამოუკიდელად შექმნან თავიანთი ვირტუალური სამყარო. უნბლიედ ისინი ახდენენ თავიანთი პერსონალური მონაცემების გასაჯაროებას ისეთ რისკების და საფრთხეების წინაშე დგებიან რომ საბოლოოდ სავალალო შედეგებამდე მივყავართ მაგალითად არასრულწლოვანი კიბერბულნგს, შევიწროვებას ვერ უმკლავდება და თვითმკვლელობას სჩადის. ამდენად, დღესდღეისობით არასრულწლოვანთა პერსონალური მონაცემთა ინტერნეტში გაზიარების საფრთხეები მეტად აქტუალური თემა არის. სწორედ რომ მოვახდინოთ ანალიზი უნდა ვიმსჯელოთ ყველა არსებულ პრობლემაზე, რეკოენდაციები გაცემის დროს კი, განსაკუთრებული ყურადღება მაინც

მშობელთა როლს უნდა მივაქციოთ, როცა საქმე არასრულწლოვათა უსაფრთხო ცხოვრებისთვის საჭირო პირობების შექნას ვგულისხმობთ.

1. კონკრეტული საფრთხეები

სტატისტიკური მონაცემებით უფრო მეტი 18 წლიდან 24 წლამდე ასაკის მომხმარებელი ფიქსირდება ინტერნეტ სივრცეში ვიდრე მოზარდები თუმცა მკვლევარებმა ისიც დაადგინეს,რომ 7 წლიდან 18 წლამდე არასრულწლოვნები გამოირჩევიან აქტიურობით. ისინი რეაგირებენ დაუყოვნებლივ ყველა განახლებასა და ახალ შეტყობინებებზე.[1] მუდმივად აქვეყნებენ ფოტოებს, ვიდეოებს ერთვებიან სხვადასხვა თამაშებში, საბოლოოდ კი ეს ყოველივე მოქმედებს არასრულწლოვნების განვითარებაზე. შესაძლებელია, ითქვას რომ საფრთხეები მრავლადა, კერძოდ: ფიშინგი, ტროლინგი, სექსტინგი, ადამიანთა ვაჭრობა, პირადი ინფორმაციის დატაცება, მავნე პროგრამები, მაგრამ ყველაზე მნიშვნელოვან გამოწვევად მაინც კიბერბულინგი რჩება.[2]

2. კიბერბულინგი და სამართლებრივი ანალიზი

იმისათვის რომ, მკითხველმა სათანად გაიგოს მსჯელობის არსი საჭიროა მეტი ყურადღება დაეთმოს კიბრბულინგის განმარტებას და კონკრეტულ პრობლემებს. უნდა გვესმოდეს არასრულწლოვანთა ვირტუალურ სივრცეში, როცა საქმე მათ პერსონალურ მონაცეთა დაცვის დარღვევას ვაწყდებით რატომ არის მნიშვნელოვანი რომ პირველადი აქცენტის გავაკეთოდ კიბერბულინგზე. როგორც მოგეხსენებათ, კიბერბულინგი ციფრული ტექნოლოგიების გამოყენებით, ფარული ან აშკარა დაშინების მიზნით განხორციელებული ქმედება არის. კიბერბულინგში ასევე მოიაზრება: უხამსი ჭორების გავრცელება, მავნე მოკლე ტექსტური შეტყობინებების გაგზავნა, დამცინავი და შეურაცხმყოფელი კომენტარების გაკეთ ებას მუქარა, სხვადასხვა ტიპის ჩაგვრა. ასევე ხდება არასრულწლოვნების ცხოვრებაშიც, თუმცა უფრო რთული შემთხვევა გაქვს სახეზე, კერძოდ პერსონალურ მონაცემთა დაცვის დარღვევა შემდეგნაირად ხორციელდება:

- პირადი ცხოვრების კადრების გასაჯაროება
- შანტაჟი - არასრულწლოვანთა პირადი ინფორმაციის გამოძალვის მიზნით
- ვირტუალურ სივრცეში დატერორება, რასაც თან ახლავს ზეგავლენის მოხდენა და შემდგომ მოჰყვება მსხვერპლი არასრულწლოვანთა სახელით გვერდებისა და სოციალურ ქსელებში ანგარიშების შექმნა.
- სოციალურ ქსელებში შეურაცხმყოფელი ფოტოების ან ვიდეოს განთავსება, რაც არასრულწლოვანის თანხმობის გარეშე ხორციელება

გულისხმობს თანატოლის არასასურველი ფოტოების გამოქვეყნებას, რაც ძლიერ მოქმედებს მათ ფსიქიკაზე. როგორც ვხედავთ, ტრადიციული ბულინგისგან განსხვავებით, კიბერბულინგს არ სჭირდება ფიზიკური ძალა ან პირისპირ შეხვედრა. ხშირად ის ძალიან ბევრი მოწმის წინაშე ხდება.

კიბერბულინგი ყველა ფორმით და სახით არსებობს – ნებისმიერს, ვისაც ინტერნეტი ან მობილური ტელეფონი აქვს, შეუძლია წამოიწყოს კიბერბულინგი ვიღაცის მიმართ, ხშირად

[1]UNICEF – "ბავშვები ციფრულ სამყაროში" 2017 – გვ.24-25.

[2] WILLARD, N. (2011). School response to cyberbullying and sexting: The legal challenge. Brigham Young University Education & Law Journal, 1, 75–125.

ანონიმურად. კიბერბულინგის განმახორციელებელს,პირობითად კიბერაგრესორს, შეუძლია მსხვერპლის დამცირება 24 საათის განმავლობაში, ხოლო მსხვერპლმა აგრესია შეიძლება ნებისმიერ ადგილას მიიღოს, ანუ არავითარი ადგილი, სახლიც კი, აღარ არის უსაფრთხო, და მხოლოდ რამდენიმე ღილაკის დაჭერით ამ პროცესს შეიძლება ონლაინ შეესწროს ასობით ან ათასობით ადამიანი.იმისთვის რომ მოხდეს შესაბამისი რეკომენდაციების გაცემა უნდა შევძლოთ ზუსტად პრობლემის საწყისების დანახვა ,რეალურაად მშობლებს თანამედროვე ეპოქაში უფრო მეტად უნდა ეშინოდეთ მათი შვილების ჩაგვრა არ მოხდეს ვირტუალურ სივრცეში.ყველაზე მნიშვნლოვანი ფაქტია რომ კიბერაგრესორები ეგრედ წოდებული ვირტუალურ სივრცეში -"ნიღბის" ქვეშ ამოფარებული უფრო მეტ გამბედაობას იჩენენ, ვიდრე მის გარეთ. რაც მთავარია უფრო მარტივი არის არასრულწლოვნებზე ზეგავლენის მოხდენა სოციალურ ქსელებში, საბოლოოდ კი უფრო გამარტივებულად ეძლევად არა მარტო თანატოლებს არამედ სრულწლოვან აგრესორებს არასრულწლოვნებს სხვადასხვა ხერხითა და საშუალებით დასტყუოს მათი პერსონალური მონაცემები და გამოიყენონ სარგებლობისთვის.

მეთოდები, რომელთაც ბავშვები და მოზარდებიკიბერბულინგისთვის იყენებენ, ისეთივე განსხვავებული და მრავალფეროვანია, როგორც მათთვის ხელმისაწვდომი ტექნოლოგიები: მუქარის შემცველი ან შემაშინებელი მესიჯების გაგზავნით დაწყებული, იმეილის ანგარიშის გატეხვით და ონლაინ იდენტობის მითვისებით დამთავრებული. ზოგიერთი სრულწლოვანი კიბერაგრესორი ცალკეულად ვებსაიტს ან სოციალური მედიის გვერდსაც კი ქმნის მსხვერპლის დასამცირებლად. ტრადიციული ბულინგის მსგავსად, კიბერბულინგში ბიჭებიც და გოგოებიც თანაბრად მონაწილეობენ, მაგრამ ზოგადად განსხვავებულ ხერხებს იყენებენ. ბიჭები მეტწილად სექსუალური ხასიათის ან ფიზიკური ზიანის მუქარის მესიჯებს აგზავნიან. გოგოები კი ძირითადად ავრცელებენ ჭორებს და მცდარ ინფორმაციას მსხვერპლის შესახებ, ამჟღავნებენ საიდუმლოს, მსხვერპლს რიცხავენ გარკვეული წრიდან ან ელექტრონული კომუნიკაციის ჯგუფიდან. კიბერბულინგი ძალიან სწრაფად მოქმედებს, ბავშვი ან მოზარდი იოლად იცვლის როლს, შეიძლება კიბერბულინგის მსხვერპლიდან ერთ წუთში გადაიქცეს აგრესორად და შემდეგ ისევ მსხვერპლად.

ამიტომაც არის რომ კრიინოლოგიის წარმომადგენლები ხშირად ფიქრობენ კონკრეტული საფრთხის დროს არ მოხდეს მავნე ჩვევის დასწავლა. შეიძლბა ერთ დღეს არასრულწლოვანი იქცეს მსხვერპლად მაგრამ მომავალში თავადვე მოიხიბლოს სხვისი დაშინებით ,პერსონალური მონაცემების გამოძალვით ან უბრალოდ შურისძიების გამო მიჰყოს ხელი დანაშაულებრივ ქმედებას. კრიმინოლოგები ,როცა დანაშაულის პრევენციის, დამნაშავის რესოციალიზაციისა და მსხვერპლის მდგომარეობის გაუმჯობესებისთვის სასჯელის გარდა სახელმწიფოს სხვადასხვა პრევენციულ ღონისძიებებს სთავზობს, ხშირად უთითებენ ემირ დიურკემისა და სხვა ცნობილი სოციოლოგების ნააზრევს, ერთერთი კი მსურს რომ განვიხილო და მივურგო არასრულწლოვანთა პერსონაური მონაცემთა ინტერნეტში გაზიარების საფრთხეებს,ეს არის დასწავლის თეორია. რეალურად შეიძლბა ვირტუალურ სივრცეში მოხდეს მსხვერლის მომრავლება, მაგრამ როცა საქმე გვაქვს არასრულწლოვანთან გასათავლისწინებელი ფაქტია იმის საშიშროება ,რომ ის სწორად ვერ აანალიზებს პრობლემის არსს, მავნე თვისებებსა და არაკანონიერ ქმედებებს მალე ითვისებს. მსხვერპლად გახდომის საფრთხეს თან ახლავს დამნაშავის ქცევის დასწავლა, რაც უფრო მეტად სახიფათოა. ამ მეთოდით ყალიბდება ადამიანები სერიულ დამნაშავეებად და მოძალადეებად. ბავშვობიდან ისინი ვერ გრძნობენ თავს ამ სამყაროს

საზოგადოების სრულფასოვან წევრად რაც უბიძგებს მათ დანაშაულისკენ. მათ გააჩნიათ სისასტიკის, შურისძიებისა და ბოროტების შეგრძნება. ვფიქრობ რომ არასრულწლოვანთა შემთხვევაშიც ესე ხდება ჯერ განიცდიან, შემდეგ ეჩვევიან მოსწონთ და საბოლოდ კი სხვა პირებს, რომლებმაც მათ ვირტუალურ სივრცეში პერსონალური მონაცემების გაზიარების შემდგომ ზემოქმედება მოახდინეს ფსიქოლოგიურად არასრულწლოვანი მსხვერპლი ემზგავსება მათ და უკვე თავად არღვევს სხვათა უფლებებს. ცნობილ კრიმინოლოგებს დავესესხები და ვიტყვი რომ სანამ არასრულწლოვანი მსხვერპლი ან დამნაშავე გახდება მანამდე უნდა შევძლოდ სწრაფი რეაგირების მოხდენა, მაგალითად მშობლების დახარებით. ამასთან დაკავშირებით არაერთი საინტერესო კვლევა ჩატარდა ამერიკის შეერთებულ სტატებში, რომელიც ამ აზრს ეთანხმება და მშობლებს მოუწოდებს ფხიზლად იყვნენ [3]

3. ამერიკის შეერთებული შტატების მაგალითზე

ამერიკის შეერთებული შტატების განათლების დეპარტამენტის მიერ ჩატარებული კვლევის თანახმად, აშშ- ს ქალაქებში არსებულ სკოლებში კიბერბულინგის მაჩვენებელი, ბოლო 2 წლის განმავლობაში, თითქმის სამჯერ გაიზარდა. აღნიშნულის შესახებ საინფორმაციო სააგენტო nyposto იუწყება. ამიტომაც ექსპერტებმა გადაწყვიტს რომ სპეციალური სასწავლო კურსი შეექნათ და სტიპენდიით დაფიანსებული კვლევა ეწარმოებინათ -შედეგის მაჩვენებლის შესამცირებლათ არასრულწლოვანთა კეთილდღეობის მიზნით.კვლევა კიბერბულინგის პრევენციასა და ინტერვენციაზე მიდგომები არის განვითარებული ბევრ ქვეყანაში, მათ შორის კანადაში. აქ ჩატარდა 2 კიბერბულინგის პროგრამების სისტემატური მიმოხილვა, სადაც პროგრამა სპეციალურად მიზნად ისახავდა მდგომარეობის შეფასებას და პრობლემის აღმოფხვრის საშუალებების მოძიებას. სისტემატური მიმოხილვის დროს, ექსპერტებმა დაარსეს 3 პროგრამა საერთო სახელით „კიბერბიუზა“ პირველი, აშშ – ს მიერ შემუშავებული I-SAFE სასწავლო პროგრამა მოიცავდა 5 გაკვეთილს (60 წთ) თემებზე: ინტერნეტის უსაფრთხოება, კიბერ საზოგადოების მოქალაქეობა, კიბერ უსაფრთხოება, პირადი უსაფრთხოება, ინტელექტუალური საკუთრება, და სამართალდამცავი ინტერნეტით. გაკვეთილები ჩაატარეს მასწავლებლებმა კლასში და თითქმის ყველა აქტივობის სამიზნე იყო მოსწავლეები მე-5 დან მე-8 კლასებში.[4] თუმცა სასურველი შედეგი ვერ გამოიღო.მეორე, კანადური პროგრამა გახლდათ ინტერაქტიული კომპიუტერული თამაში შექმნილი ახალგაზრდებისთვის ინტერნეტის უსაფრთხოების შესახებ .კერძოდ თამაშის დროს, არასრულწლოვანთა როლი მოიცავდა პოლიციელის პასუხისმგებლობას, რომელიც ეძებდა დაკარგულ თინეიჯერს. თუმცა არასრულწლოვან კლასელებს მოთხოვნა არც კი გაუგია, ერთმანეთს ესაუბრებოდნენ უგზავნიდნენ ინფორმაციას საინფორმაციო ჩატში სხვა თემებზე საუბრობდნენ ზედმეტი კითხვების გარეშე მიაწოდეს ერთმანეთს პირადი ინფორმაცია, როგორიცაა მეილი(თამაშის განახლებითვის). მესამე პროგრამა მოიცავდა არასრულწლოვანთა საუბრებს საკუთარ თავზე, თუ როგორ იქცევიან ისინი ვირტუალურ სივრცეში. ნაპოვნია საკვლევი

[3] J. GOMES, & M. ROMÃO, Investments in information systems and technology in the healthcare: Project management mediation. Journal of Information Systems Engineering & Management, 1(1), 15-24(2016).

[4] JS CHIBARRO, “School counselors and the cyberbully: Interventions and implications”, (2007). Professional School Counseling, Fauman, MA (2008). “Cyber bullying: Bullying in the digital age”, American Journal of Psychiatry,

მტკიცებულებები რომ პროგრამებმა გაზარდა ინტერნეტის უსაფრთხოების ცოდნა, მაგრამ არ იმოქმედა არასრულწლოვანთა სარისკო ონლაინ ქცევაზე. ამრიგად, აშშ-ში გადაწყვიტეს რომ დამატებითი საჭიროა ჩატარდეს კვლევა, თუ როგორ შეიძლება გავლენა იქონიოს პროგრამებმა ახალგაზრდების ქცევაზე. თუმცა როგორც ხედავთ 3 პროგრამის კვლევამ სასურველი შედეგი ვერ გამოიღო, ამიტომაც კანადის ექსპერტები თვლიან რომ მშობლის როლი ასეთ საფრთხეების აღმოსაფხვრელად უფრო დიდია. ამიტომაც ამერიკის შეერთებული შტატების მაგალითზე, შემიძლია ვთქვა რომ საქართველოში არასრულწლოვანთა შემეცნების პროგრამები დამატებით დამხმარე ობიექტად უფრო გამოგვადგება, თუმცა პრობლემას ვერ აღმოფხვრის. სკოლაში პერსონალურ მონაცემთა ინტერნეტში გაზიარების საფრთხეებზე საუბარი, კონკრეტულ საფრთხის დელიტს ხელს ვერ შეუშლის თუმცა მაინც საჭიროა, ხოლო პრობლემის აღმოფხვრისთვის ამერიკის მაგალითზე მივიჩნევ რომ მშობლების პასუხიმგებლობა, მართლაც რომ დიდი არის.

დასკვნა

დღესდღეისობით, ექსპერტები ამუშავებენ პრევენციის პროგრამებს კიბერბულინგის აღმოსაფხვრელად და კიბერუსაფრთხოების დასაცავად. მართალია, რომ ვებსაიტები ან სხვა ონლაინ რესურსები შეიძლება იყოს, სადაც მშობლები იღებენ ინფორმაციას იმის შესახებ, თუ როგორ საუკეთესოდ დაიცვან თავიანთი შვილები. თუმცა, როგორც ჩანს, ონლაინ რესურსებს ხშირად ხელს უწყობენ ორგანიზაციები, რომლებიც ყიდიან პროდუქტებს და იშვიათად ემყარება კვლევას. არსებობს რისკი, რომ ეს ინფორმაცია შეიძლება იყოს საზიანო. მშობლები, მასწავლებლები, სკოლა ადმინისტრატორები და სამედიცინო მომსახურების მიმწოდებლები ფრთხილად უნდა იყვნენ ამ საიტებზე ინფორმაციის გადახედვისას და ყურადღება უნდა მიაქციოს ონლაინ რესურსებს,[5] რომლებსაც უზრუნველყოფს სამთავრობო სააგენტოები და ადვოკატირების ჯგუფები, რომლებიც იყენებენ კვლევას მათი რეკომენდაციების წარმართვის მიზნით. არასრულწლოვანთა დაცვისთვის გაცილებით მეტი მითითებაა საჭირო რათა თავიდან აიცილონ გრძელვადიანი ბულინგის შედეგები.[6] მიუხედავად იმისა, რომ ახალგაზრდები და მშობლები მზად არიან გაამჟღავნონ მათი გამოცდილება ბულინგის მიმართ ეს არ არის საკმარისი საჭიროა ესეთ გამჟღავნებას საზოგადოებამ საჭიროებისამებრ აუცილებელი წესით განიხილოს. საზოგადოებაში ზუსტად დასმული შეკითხვები უნდა გაჟღერდეს, კერძოდ კითხვები უნდა შეიცავდეს თუ როგორ, ახალგაზრდები ატერორებენ სხვებს ან აშინებენ როგორ აისახება ეს ახალგაზრდის ფსიქიკურ, ფიზიკურ და სოციალურ ჯანმრთელობაზე. ამიტომაც საჭიროა ჯანდაცვის პროვაიდერები -კვლევების სწორი წარმართვისთვის. ჯანდაცვის პროვაიდერებმა უნდა ესაუბრონ მშობლებს ინტერნეტ სივრცეში დროის შესაბამისი შეზღუდვების დაწესებაზე, ტექნოლოგიის სწორ გამოყენებაზე, საჭიროა არასრულწლოვნებს ესაუბრონ მშობლებმა -ინტერნეტის უსაფრთხოებისა და კონფიდენციალურობის შესახებ. საჭიროა შვილება გაიგონ რა არის იდენტიფიკაცია? დაუმალავად აუხსნან საფრთხეები. როგორც ხედავთ სახელმწიფო რეფორმების გარდა დიდი ყურადღება ეთმობა მშობელს რომ ეს პრობლემა აღმოიფხვრას. არის შემთხვევები,

[5]JS CHIBARRO, „School counselors and the cyberbully: Interventions and implications" (2007). Professional School Counseling, 11(1), pp. 65–68. Fauman, MA (2008). "Cyber bullying: Bullying in the digital age", American Journal of Psychiatry, 165(6), pp.780-781

[6] AI, ALIFIROV, IV. MIKHAYLOVA, AS MAKHOV, & MS BELOV, (2018). "Introducing chess education in USA school system: theoretical and practical aspects", Theory and practice of physical culture.

როცა არასრულწლოვნები მოსალოდნელ კიბერბულინგზე ფლობდნენ ინფორმაციას თუმცა მაინც ხდებიან მსხვერპლი ამიტომაც ჩემს მიერ მოწოდებულ რეკომნდაციებში ჩავთვალე საჭიროდ ამეხსნა არასრულწლოვნების ქმედებანი ,როცა ვირტუალურ სივრცეში უსიამოვნება ხდება მათ თავს. შვილები, თუ კიბერბულინგის მსხვერპლი არიან, შემდეგი ფსიქოლოგების კვლევებით სავარაუდო ნიშნები გააჩნიათ, არასრულწლოვანი: ხდება სევდიანი, გაბრაზებული ან დათრგუნული ინტერნეტის გამოყენების შემდეგ შფოთავს, როცა იღებს ტექსტურ მესიჯს ან იმეილსთავს არიდებს ოჯახის წევრებს, მეგობრებს ამბობს სკოლაში წასვლაზე უარს,არ ესწრებაკონკრეტულ საგნებს ეცვლებახასიათ ი,ქცევა.როგორცხედავთ, მისი შინაარსიდან გამომდინარე არასრულწლოვანთა პერსონალური მონაცემთა ინტერნეტში გაზიარების საფრთხეები აწუხებს არა მარტო საზოგადოებას არამედ სახელმწიფოს. რადგან არასრულწლოვნებს ჰყავთ მშობლები, სულაც არ თვლის სახელმწიფო რომ მხოლოდ რომელიმე კონკრეტული ოჯახის სატკივარია კიბერბულინგი ეს პრობლემა ოჯახში ძალადობის მსგავსია თავისი გავრცელების არეალითა და საშიშროებით.[7]ოჯახში ძალადობის მსგავსად, როცა არსრულწლოვნებს ეხება საქმე უფრო მეტად ყურადღებას იჩენენ ფსიქოლოგები იურისტები, სახელმწიფო. თუმცა მხოლოდ საკანონმდებლო რეფორმები ვერ დაგვეხმარება პრობლემის აღმოსაფხვრელად, საჭიროა თავად საზოგადოებაში ცნობიერების ამაღლება.

[7]T. ARICAK, S. SIYAHHAN, A. UZUNHASANOGLU, S. SARIBEYOGLU, S. CIPLAK, N. YILMAZ, & C. MEMMEDOV, (2008). “Cyberbullying among Turkish adolescents”, CyberPsychology & Behavior, 11(3), pp. 253-261.

ბიბლიოგრაფია

1. UNICEF – “ბავშვები ციფრულ სამყაროში” 2017;
2. ნ. ვილარდ. სკოლის რეაგირება კიბერბულინგზე და სექსტინგზე: სამართლებრივი გამოწვევა. ბრიგჰემ იანგის უნივერსიტეტის განათლებისა და სამართლის ჟურნალი,(2011);
3. S. HINDUJA & JW PATCHIN, "ბულინგი სკოლის ეზოს მიღმა: კიბერბულინგის პრევენცია და რეაგირება", Corwin Press. (2014);
4. JS CHIBARRO, ”სკოლის მრჩეველები და კიბერდანაშაული: ინტერვენციები და შედეგები”(2007). პროფესიული სკოლის კონსულტაცია, ფაუმანი MA ”კიბერ ბულინგი: ბულინგი ციფრულ ეპოქაში”, ფსიქიატრიის ამერიკული ჟურნალი, (2008);
5. J. GOMES & M. ROMÃO, ინვესტიციები ინფორმაციულ სისტემებსა და ტექნოლოგიებში ჯანდაცვის სფეროში: პროექტის მენეჯმენტის შუამავლობა. ჟურნალი ინფორმაციული სისტემების ინჟინერია და მენეჯმენტი (2016);
6. AI, ALIFIROV, IV MIKHAYLOVA, AS MAKHOV, MS & BELOV “Introducing chess education in USA school system: theoretical and practical aspects”, Theory and practice of physical culture. (2018);
7. T.ARICAK, S. SIYAHHAN, A.UZUNHASANOGLU, S.SARIBEYOGLU, S. CIPLAK, N.YILMAZ, & C.MEMMEDOV (2008). “Cyberbullying among Turkish adolescents”, CyberPsychology & Behavior.

Bibliography

1. UNICEF - "Children in the Digital World" 2017;
2. N. WILLARD, School response to cyberbullying and sexting: The legal challenge. Brigham Young University Education & Law Journal, (2011);
3. S. HINDUJA & JW PATCHIN, “Bullying beyond the schoolyard: Preventing and responding to cyberbullying”, Corwin Press. (2014);
4. JS. CHIBARRO, (2007). “School counselors and the cyberbully: Interventions and implications”, Professional School Counseling, Fauman, MA (2008). “Cyber bullying: Bullying in the digital age”, American Journal of Psychiatry;
5. J. GOMES & M. ROMÃO Investments in information systems and technology in the healthcare: Project management mediation. Journal of Information Systems Engineering & Management (2016);
6. AI, ALIFIROV, IV MIKHAYLOVA, AS MAKHOV, MS & BELOV (2018). “Introducing chess education in USA school system: theoretical and practical aspects”, Theory and practice of physical culture;
7. T. ARICAK, S. SIYAHHAN, A. UZUNHASANOGLU, S. SARIBEYOGLU, S. CIPLAK, N. YILMAZ & C. MEMMEDOV, „Cyberbullying among Turkish adolescents”, CyberPsychology & Behavior, (2008).