სსიპ გორის სახელმწიფო სასწავლო უნივერსიტეტი

ანა ნადირაძე

პერსონალური მონაცემების დაცვა ინტერნეტისა და ტექნოლოგიების ეპოქაში

სამაგისტრო ნაშრომი შესრულებულია სოციალურ მეცნიერებათა, ბიზნესისა და სამართალმცოდნეობის ფაკულტეტზე სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: გიორგი გიორგაძე

ასოცირებული პროფესორი

გორი

2019წ.

ანოტაცია:

21-ე საუკუნე ინტერნეტისა და ტექნოლოგიების საუკუნედ მოიაზრება. ტექნოლოგიური პროგრესის მეშვეობით გამარტივდა კომუნიკაცია, შეიქმნა უამრავი ახალი მოწყობილობები, გაუმჯობესდა მომსახურება. ინტერნეტი კი ერთ-ერთ ყველაზე მოთხოვნად საშუალებად იქცა დემოკრატიულ საზოგადოებაში. ტექნოლოგიური ეპოქის მთავარი მამოძრავებელი ძალა პერსონალური მონაცემებია. პრაქტიკულად ყველა ჩვენი ყოველდღიური აქტივობა რეალურ თუ ინტერნეტ სამყაროში პერსონალური მონაცემების გაზიარებას მოითხოვს. თუმცა ახალმა შესაძლებლობებმა ახალ გამოწვევებს ჩაუყარა საფუძველი - პერსონალური მონაცემების კერძოსამართლებრივი დაცვა ინტერნეტისა და ტექნოლოგიების ეპოქაში ერთ-ერთ უმნიშვნელოვანეს პრობლემად იქცა.

თითოეული ჩვენგანი ყოველი ფეხის ნაბიჯზე საკუთარი პერსონალური მონაცემების კვალს ტოვებს. ამ მონაცემებს კი დაცვა და გაფრთხილება სჭირდება, განსაკუთრებით ინტერნეტ სივრცეში. სივრცეში, სადაც ,,მარტივად'' ირღვევა ჩვენი უფლებები და იზღუდება თავისუფლება.

წარმოდგენილი ნაშრომის მიზანია დაანახვოს ინტერნეტ მომხმარებლებს ის, თუ რა საფრთხეები შეიძლება მოჰყვეს მათ მიერ განხორციელებულ ნებისმიერ ქმედებას და როგორ დაიცვან დარღვეული უფლებები. ნაშრომში წარმოდგენილ სიახლეებთან ერთად, ჩემი ამოცანაა სხვა თვალით დავანახვო საზოგადოებას ინტერნეტი და მისი განუსაზღვრელი შესაძლებლობები.

Annotation

,,Personal data secure in the era of the Internet and Technology"

A.Nadiradze

21st century is called "The Digital Age". Through the technological progress communication has been simplified, numerous new gadgets have been created and service has been improved as well. Internet is one of the most popular means in the democratic society. Personal data is considered as the main driving force of the technological era. All our daily activities taking place in real life or the internet space require personal data sharing. However, new opportunities led to the new challenges-personal data security has become one of the most important issues in the epoch of internet and technology.

Each of us leaves digital footprint of own personal data on each step that needs protection especially in the Internet space. In the space where our rights is violated easily and restricted.

The purpose of the presented paper is to show the Internet users the threats they might face and how to vindicate. With the presented novelties in the work my task is to show the public the Internet and its unlimited possibilities.

სარჩევი:

შესავალი

თანამედროვე დემოკრატიულ საზოგადოებაში პერსონალურ მონაცემთა დაცვას მნიშვნელოვანი ადგილი უჭირავს ადამიანის უფლებების სფეროში. ეს საკითხი განსაკუთრებით აქტუალური მას შემდეგ გახდა, რაც ინტერნეტისა და ტექნოლოგიების ეპოქაში აღმოვჩნდით. ინტერნეტს დღესდღეობით საჯარო მომსახურების ღირებულება გააჩნია. ადამიანები, საჯარო დაწესებულებები და კერძო კომპანიები საკუთარი საქმიანობის განხორციელებისას ინტერნეტზე არიან დამოკიდებულები და ლეგიტიმური მოლოდინი გააჩნიათ, რომ ეს სერვისი ფიზიკურად და ფინანსურად ხელმისაწვდომი, უწყვეტი, სანდო და დაცული იქნება ყოველგვარი დისკრიმინაციისაგან. გარდა ამისა, უზრუნველყოფილი უნდა იყოს ის, რომ არავინ დაექვემდებაროს არამართლზომიერ, ზედმეტ და არათანაზომიერ ჩარევას ინტერნეტის გამოყენებით.

გამონაკლისი არც საქართველო აღმოჩნდა. პერსონალურ მონაცემთა დაცვის საკითხი აქაც საკმაოდ აქტუალურია. მონაცემთა დაცვის შესახებ შემუშავებული კანონის სიახლემ განაპირობა აღნიშნულ საკითხთან დაკავშირებული კვლევებისა და პრაქტიკის სიმწირე. ჩვენი მოქალაქეები კი ყოველდღიურად აწყდებიან აღნიშნულ უფლებათა დარღვევის ნათელ მაგალითებს. ამიტომ ბევრი არც მიფიქრია თემის არჩევის დროს და არჩევანი პერსონალურ მონაცემთა დაცვაზე შევაჩერე. წარმოდგენილი ნაშრომი მიზნად ისახავს წარმოაჩინოს ის პრობლემები, რაც ინტერნეტ სივრცეში პერსონალურ მონაცემთა გამჟღავნებას და ხელმისაწვდომობას ეხება. ნაშრომი ასევე მოიცავს სხვადასხვა კატეგორიის მონაცემთა განმარტებას, განიხილავს თითოეულის მნიშვნელობას, რაც დაგვეხმარება უკეთესად გავიაზროთ ის მოსალოდნელი საფრთხეები, რომლებსაც ვაწყდებით ინტერნეტში ნებისმიერი ქმედების განხორციელებისას.

იმის გასარკვევად, თუ რამდენად მაღალია საზოგადოებრივი ცნობიერება და რამდენად არის ინფორმირებული მოსახლეობა პერსონალურ მონაცემთა დაცვის სფეროში, ჩავატარე გამოკითხვა. ისევ და ისევ ინტერნეტის დახმარებით შევადგინე კითხვარი, რომელიც სულ 12 კითხვისგან შედგებოდა (იხ. დანართი N1). კითხვარი შეეძლო შეევსო ნებისმიერი სქესის, განათლებისა და ასაკის ადამიანს. არანაირი შეზღუდვა არ დამიწესებია, რადგან ჩემთვის საინტერესო იყო ის, თუ ზოგადად როგორია მოსახლეობის ინფორმირებულობა პერსონალურ მონაცემთა დაცვის კუთხით.

კითხვარი შეავსო სულ 54-მა ადამიანმა. გამოკითხვის შედეგები მოცემულია დანართის სახით (იხ. დანართი N2). საინტერესო იყო ის ფაქტი, რომ გამოკითხულთა 92%-მა იცის პერსონალურ მონაცემთა შესახებ, თუმცა მათგან 64% თვლის, რომ პერსონალური მონაცემი მხოლოდ სახელი, გვარი, დაბადების თარიღი და პირადი ნომერია. ასევე გამოკითხულთა მხოლოდ 15%-მა იცის ტერმინის Big data - ანუ ,,დიდი მონაცემების'' შესახებ. საზოგადოების ინფორმირებულობა პერსონალურ მონაცემთა კატეგორიების სფეროში საკმაოდ დაბალია, ამიტომ თემის დაწყებაც ამ საკითხის დეტალურად განხილვით დავიწყე. თუ არ ვიცით ზუსტად რას მოიცავს ცნება ,,პერსონალური მონაცემი'', მაქსიმალურად ვერ გავიაზრებთ იმ საფრთხეებს, რომელიც ამ მონაცემების გამჟღავნებას და დაუცველობას შეიძლება მოჰყვეს.

აღსანიშნავია ის ფაქტი, რომ გამოკითხულთა 98% სოციალური ქსელის მომხმარებელია, თუმცა აქედან მხოლოდ 15% თვლის სრულიად დაცულად თავს ინტერნეტ სივრცეში, 42% კი ნაწილობრივ დაცულად. გამოკითხვის შედეგებმა კიდევ ერთხელ დამარწმუნა იმაში, რომ ინტერნეტი ჩვენს განუყოფელ ნაწილად იქცა. ნივთების შესაძენადაც კი მაღაზიებში სიარულს უკვე ონლაინ შესყიდვას ვამჯობინებთ. თუმცა არ ვფიქრობთ ინ საფრთხეებზე და პრობლემებზე, რაც შეიძლება ინტერნეტ მიჯაჭვულობამ გამოიწვიოს. წარმოდგენილ ნაშრომში შევეცდები დეტალურად განვიხილო ყველა ის საკითხი, რაც პერსონალური მონაცემების ინტერნეტ სიცრცეში ხელმისაწვდომობას ეხება.

გამოკითხული 54 ადამიანიდან 83%-მა არ იცის როგორ დაიცვას თავისი პერსონალური მონაცემები ინტერნეტ სივრცეში. ამიტომ ნაშრომის ბოლო თავი მთლიანად პერსონალურ მონაცემთა დაცვას და რეკომენდაციებს მივუძღვენი. რეკომენდაციები, ანუ იგივე რჩევები, დაეხმარება ინტერნეტ მომხმარებლებს მეტი სიფრთხილით განახორციელონ ნებისმიერი ქმედება ინტერნეტ სივრცეში. ხოლო თუ მაინც დაირღვა მათი უფლებები, შეიზღუდა თავისუფლება და არამართლზომიერად მოხდა პერსონალური მონაცემების გამჟღავნება, მომხმარებლებმა უნდა იცოდნენ თუ როგორ აღადგინონ პირვანდელი მდგომარეობა და დაიბრუნონ დარღვეული თავისუფლება.

1. ცნება ,,პერსონალური მონაცემის'' მთავარი ასპექტები

მონაცემი არის პერსონალური თუ იგი უკავშირდება იდენტიფიცირებულ ან, სულ მცირე, იდენტიფიცირებად პიროვნებას ანუ მონაცემთა სუბიექტს. ინფორმაცია შეიცავს მონაცემებს პირის შესახებ თუ:

- პირი ამ ინფორმაციაში არის იდენტიფიცირებული; ან
- პირი არ არის იდენტიფიცირებული, მაგრამ აღწერილია ამ ინფორმაციაში იმგვარად, რომ არსებობს მონაცემთა სუბიექტის ვინაობის დადგენის საშუალება, შემდგომი ძიების შედეგად.

როგორც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის თანახმად, ,,პერსონალური მონაცემი'' განმარტებულია, როგორც ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს, ანუ,, ინფორმაცია პირის შესახებ, რომლის ვინაობა ცნობილია ან შეიძლება დადგინდეს დამატებითი ინფორმაციის მოძიების შედეგად''.

საქართველოს კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ'' თითქმის ანალოგიურად განმარტავს პერსონალურ მონაცემებს. კანონში წერია: ,,პერსონალური მონაცემი (შემდგომ მონაცემი) - ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით''.

რა არის ჩემი პერსონალური მონაცემები? - უფრო მარტივი ენით რომ ჩამოვაყალიბოთ, პერსონალური მონაცემები არის პირის მაიდენტიფიცირებადი ნებისმიერი სახის ინფორმაცია, მაგალითად: სახელი, გვარი, დაბადების თარიღი, პირადი ნომერი, ფოტოსურათი, ვიდეო ჩანაწერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, სოციალური ქსელის ანგარიში, პირადი მიმოწერა. პერსონალური მონაცემია, ასევე, ინფორმაცია სამუშაო ადგილის, შემოსავლების, ოჯახური მდგომარეობის შესახებ და სხვა.

საქართველოს უზენაესმა სასამართლომ პერსონალური მონაცემები ორ ძირითად სახედ - ჩვეულებრივ და განსაკუთრებით მგრძნობიარე პერსონალურ

მონაცემებად, - დაყო.[1] სასამართლო ჩვეულებრივ მონაცემებად მიიჩნევს ყველა იმ მონაცემს, რომელიც საჯარო დაწესებულებაში პირის (გარდა თანამდებობის პირებისა) საქმიანობას ან სხვა ქმედებებს შეეხება, ხოლო განსაკუთრებით მგრძნობიარე პერსონალურ მონაცემებად - დოკუმენტებს, რომლებიც პირის შეწყალებას, ან სხვა მსგავს სენსიტიურ საკითხებს მოიცავს.

1.1 პერსონალური მონაცემების განსაკუთრებული კატეგორიები

როგოც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, არსებობს განსაკუთრებული კატეგორიის მონაცემებიც. განსაკუთრებული კატეგორიის მონაცემთა განმარტებისას, 108-ე კონვენციის მე-6 მუხლი და მონაცემთა დაცვის დირექტივის მე-8 მუხლი ადგენს შემდეგ კატეგორიებს:

- პერსონალური მონაცემი რასისა და ეთნიკური წარმომავლობის შესახებ
- პერსონალური მონაცემი პოლიტიკური შეხედულებების, რელიგიური ან სხვა შეხედულებების შესახებ და
- პერსონალური მონაცემი, რომელიც უკავშირდება ჯანმრთელობის მდგომარეობას ან სქესობრივ ცხოვრებას

მაგალითი: საქმეზე Bodil Lindqvist, [2] მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა - ,,მითითება იმ ფაქტზე, რომ ინდივიდმა დაიზიანა საკუთარი ტერფი და იმყოფება ნახევრად-სამკურნალო მდგომარეობაში, წარმოადგენს პერსონალურ მონაცემს 95/46 დირექტივის მე-8 მუხლის პირველი პუნქტის თანახმად.''

ამ კატეგორიას მიეკუთვნება ინფორმაცია, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული კავშირის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლეობასთან, ადმინისტრაციულ პატიმრობასთან, აღკვეთის ღონისძიების შეფარდებასთან,

[1] საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2010წლის 5ივლისის Nბს-1278-1240(კ-08) განჩინება

[2] მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Linqvist, 6 ნოემბერი 2003 წელი, პარაგ. 51.

საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან. ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია დაცულია როგორც პერსონალურ მონაცემთა დაცვის, ასევე სამედიცინო საქმიანობის მარეგულირებელი კანონმდებლობით. ჯანმრთელობის შესახებ ინფორმაციას იძლევა პირის დიაგნოზი, დანიშნული თუ მიღებული მკურნალობის მეთოდები და შესაბამისი გამოკვლევების შედეგები. ეს მონაცემები, როგორც წესი, ინახება სამედიცინო დაწესებულებებში და მათი მესამე პირებისთვის გაცნობა შესაძლებელია მხოლოდ პაციენტის თანხმობით, ან, მაგ. საზოგადოებრივი ჯანმრთელობის, სასიცოცხლო ინტერესების დაცვის მიზნით და სხვა. ხოლო რაც შეეხება ნასამართლეობას, იგი არის პირის შესახებ ინფორმაცია, რომელიც ცალსახად მიანიშნებს დანაშაულის ჩადენის ფაქტზე. პირი ნასამართლევად ითვლება მის მიმართ გამამტყუნებელი განაჩენის გამოცხადებიდან ნასამართლეობის გაქარწყლების, ან მოხსნის მომენტამდე. ნასამართლეობის შესახებ ინფორმაციას ხშირად ითხოვენ დასაქმების თაობაზე გადაწყვეტილების მისაღებად. იგი ითვლება განსაკუთრებული კატეგორიის მონაცემად და დაცულია სამართალდამცავი ორგანოების მონაცემთა ბაზებში. ამ ინფორმაციაზე წვდომა მკაცრად შეზღუდულია. მისი გამოთხოვა დასაშვებია მხოლოდ კანონით განსაზღვრულ გამონაკლის შემთხვევებში. ამასთან, უნდა გვახსოვდეს, რომ ნასამართლეობა არ წარმოადგენს მუდმივ მონაცემს და მისი მოხსნის ან გაქარწყლების შემდგომ პირი ნასამართლეობის არ მქონედ ითვლება. განსაკუთრებულ კატეგორიაში შედის, ასევე, ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა. აქვე განვმარტოთ, თუ რას ნიშნავს ბიომეტრიული და გენეტიკური მონაცემები.

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

თითის ანაბეჭდი უნიკალურობის გამო ერთ-ერთი ყველაზე გავრცელებული ბიომეტრიული მონაცემია. გამოიყენება პირის იდენტიფიცირების, ვიზის გაცემისა და საზღვრის კონტროლის, საცავებში ან საიდუმლო ობიექტებზე შესვლის, გამოძიების მიზნებისთვის. ბიომეტრიული მონაცემების გამოყენება, როგორც წესი, დასაშვებია უსაფრთხოების, საკუთრებისა და საიდუმლო ინფორმაციის დასაცავად, თუ ამ მიზნების სხვა საშუალებებით მიღწევა შეუძლებელია. კერძო ორგანიზაცია

ანაბეჭდის აღებამდე ვალდებულია, მოგვაწოდოს ინფორმაცია, რა მიზნით გამოიყენებს ჩვენს მონაცემს და რა ზომებს მიიღებს მის დასაცავად.

პირის იდენტიფიცირება უსაფრთხოების, საკუთრებისა და საიდუმლო ინფორმაციის დაცვის მიზნებისათვის ასევე დასაშვებია თვალის ფერადი გარსის მეშვეობით, რომელსაც ასევე ,,ირისს'' უწოდებენ. თვალის ფერადი გარსი თვალის გუგის ირგვლივ მდებარე ფერადი კუნთოვანი რკალია. უნიკალურობიდან და მუდმივობიდან გამომდინარე ბიომეტრიულ მონაცემს განეკუთვნება. თვალის ფერადი გარსის სკანირება პირის იდენტიფიცირების უტყუარი საშუალებაა. ცალკეული ქვეყნები უკვე განიხილავენ საიდენტიფიკაციო დოკუმენტებში მისი ელექტრონულად დატანის საკითხს, მაგ. საზღვრის გადაკვეთის დროს პირის ზუსტი იდენტიფიცირებისათვის.

გენეტიკური მონაცემი - მონაცემთა სუბიექტის უნიკალური და მუდმივი მონაცემია გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება.

გენეტიკური მონაცემების კატეგორიას განეკუთვნება ღეროვანი უჯრედი, რომელიც უნიკალურობისა და თვითაღდგენის უნარიდან გამომდინარე ძირითადად გამოიყენება სამედიცინო მიზნებისათვის. თუმცა თანამედროვე მეთოდები და ხელსაწყოები ღეროვანი უჯრედით პირის იდენტიფიცირების შესაძლებლობასაც იძლევა. გენეტიკური მონაცემის დაცულობისთვის მნიშვნელოვანია ღეროვანი უჯრედების ფიზიკური უსაფრთხოება და მათი სათანადო წესით შენახვა.

განსაკუთრებული კატეგორიის მონაცემებს ,,ჩვეულებრივი'' მონაცემებისგან ის განასხვავებს, რომ კანონით მათი დაცვის განსაკუთრებით მაღალი სტანდარტია დაწესებული და წესების დარღვევის შემთხვევაში სანქციაც უფრო მკაცრია.

1.2 ანონიმირებული და ფსევდონიმირებული მონაცემები

პერსონალურ მონაცემთა ლიმიტირებული შენახვის პრინციპის თანახმად, რომელიც მოცემულია 108-ე კონვენციით [3] და მონაცემთა დაცვის დირექტივით, მონაცემები შენახულ უნდა იქნეს მონაცემთა სუბიექტის იდენტიფიცირებადი

[3] ევროპის საბჭოს მიერ მიღებული კონვენცია, რომელიც ძალაში შევიდა 01/10/1985 წელს. რატიფიცირებულია საქართველოს პარლამენტის 2005 წლის 28 ოქტომბრის N 2010 – lls დადგენილებით. ძალაშია 2006 წლის 1 აპრილიდან

ფორმით იმ ვადის განმავლობაში, რაც აუცილებელია მონაცემთა შეგროვების ან მათი შემდგომი დამუშავების მიზნის მისაღწევად. შესაბამისად, თუ დამმუშავებელს სურს მათი შენახვა იმ ვადის გასვლის შემდეგ, რაც საჭირო იყო საწყისი მიზნის მისაღწევად, მონაცემი უნდა იქნეს ანონიმირებული.

1.1.1. ანონიმირებული მონაცემები

მონაცემები არის ანონიმირებული, თუ პერსონალური მონაცემებიდან იდენტიფიცირების შემცველი ყველა ელემენტი არის გაუქმებული. არც ერთი ის ელემენტი არ შეიძლება დარჩეს ინფორმაციაში, რომელიც გარკვეული ძალისხმევის გამოყენების შედეგად, შესაძლებელს გახდის მოცემული პიროვნებების იდენტიფიცირებას. იმ შემთხვევაში, თუ მონაცემები წარმატებით იქნა ანონიმირებული, ისინი აღარ მიიჩნევა პერსონალურ მონაცემებად. როდესაც პერსონალური მონაცემი აღარ ემსახურება თავდაპირველ მიზანს, მაგრამ უნდა იქნეს შენახული პერსონიფიცირებული ფორმით ისტორიული, სტატისტიკური ან სამეცნიერო მიზნებისთვის, დირექტივითა[4] და 108-ე კონვენციით ეს შესაძლებელია იმ პირობით, რომ შესაბამისი დამცავი ღონისძიებები უნდა იქნეს დადგენილი მონაცემთა უკანონო გამოყენების წინააღმდეგ.

1.1.2. ფსევდონიმირებული მონაცემები

პერსონალური მონაცემები შეიცავს იდენტიფიკატორებს, როგორიცაა სახელი, დაბადების თარიღი, სქესი და მისამართი. როდესაც პერსონალური ინფორმაცია არის ფსევდონიმირებული, იდენტიფიკატორები ჩანაცვლებულია ფსევდონიმებით. ფსევდონიმირება მიიღწევა პერსონალურ მონაცემებში იდენტიფიკატორების დაშიფრვით. 108-ე კონვენციის განმარტებითი ბარათის 42-ე მუხლი ადგენს, რომ ,,მოთხოვნა, რომელიც ეხება მონაცემთა სახელების შემცველი ფორმით შენახვის ვადებს, არ ნიშნავს იმას, რომ მონაცემები გარკვეული დროის შემდეგ უნდა იყოს აუცილებლად განცალკევებული იმ პიროვნების სახელისაგან, რომელსაც ეკუთვნის მონაცემები, არამედ, არ უნდა იყოს შესაძლებელი მონაცემთა დაკავშირება მათ იდენტიფიკატორებთან''. აღნიშნული შესაძლოა მიღწეულ იქნეს მონაცემთა ფსევდონიმირებით. ფსევდონიმისა და განშიფრვის კოდის ფლობით პიროვნების ვინაობასთან კავშირი ისევ არსებობს. მათთვის, ვინც უფლებამოსილია გამოიყენოს განშიფრვის კოდი, ხელახლა იდენტიფიცირება მარტივადაა შესაძლებელი. დაცული

[4] ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის დირექტივა)

უნდა იყოს არაუფლებამოსილი პირების მიერ განშიფრვის კოდის გამოყენება. მონაცემთა ფსევდონიმირება არის ერთ-ერთი ყველაზე მნიშვნელოვანი საშუალება. რათა ფართო მასშტაბით იქნეს მიღწეული მონაცემთა დაცვა.

მაგალითი: წინადადება ,,ჩარლზ სპენსერი, დაბადებული 1967 წლის 3 აპრილს, არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს'' შესაძლებელია ფსევდონიმირებულ იქნეს რამოდენიმე გზით:

,,ჩ.ს. 1967 არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს;'' ან

,,324 არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს;'' ან

,,YESz320I არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს.''

მომხმარებლები, რომლებსაც აქვთ წვდომა ფსევდონიმირებულ მონაცემებზე, ზოგადად, ვერ შეძლებენ მოახდინონ 1967 წლის 3 აპრილს დაბადებული ჩარლზ სპენსერის იდენტიფიცირება მონაცემიდან 324 ან YESz320I. შესაბამისად, ფსევდონიმირებული მონაცემები არის უფრო მეტად დაცული არასანქცირებული გამოყენებისგან. პირველი მაგალითი ნაკლებად უსაფრთხოა. თუ წინადადება ,,ჩ.ს. 1967 არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს'' გამოყენებული იქნება პატარა სოფლის მასშტაბით, სადაც ჩარლზ სპენსერი ცხოვრობს, იგი შესაძლოა მარტივად ამოცნობადი იყოს. ხოლო ტექნიკური პროგრესის კვალდაკვალ იგი უფრო დიდ ტერიტორიაზე გახდება მარტივად ამოსაცნობი. ფსევდონიმირების მეთოდი გავლენას ახდენს მონაცემთა დაცვის ეფექტურობაზე.

პერსონალური მონაცემები დაშიფრული იდენტიფიკატორებით ბევრ შემთხვევაში გამოიყენება, როგორც პიროვნებების ვინაობის საიდუმლოდ შენახვის საშუალება. ამავდროულად, ფსევდონიმირება არის ძლიერი საშუალება პირადი ცხოვრების გამაძლიერებელ ტექნოლოგიებს შორის.

1.3 Big Data - დიდი მონაცემები

ტექნოლოგიური პროცესისა და ინტერნეტის ეპოქაში თითოეული ჩვენგანი უამრავ აპლიკაციას, საძიებო სისტემას, სოციალურ ქსელს, ონლაინ მომსახურებას იყენებს. ამ მომსახურებების დიდ ნაწილში ფულის გადახდა არ გვჭირდება, თუმცა

ნაკლებად ვუფიქრდებით იმას, რომ უფასო მომსახურებებიც არ არის ბოლომდე უფასო და მათ მისაღებად ჩვენს პერსონალურ მონაცემებს ,,ვიხდით''. კომპანიები აგროვებენ და ამუშავებენ ჩვენს მონაცემებს: სახელს და გვარს, დაბადების თარიღს, ელექტრონული ფოსტის მისამართს თუ ტელეფონის ნომერს, გადაადგილების მარშუტს, საშუალებებს, ინფორმაციას სამუშაო და საცხოვრებელი ადგილის შესახებ. მათთვის ასევე ხელმისაწვდომია ინფორმაცია ჩვენი ინტერესებისა და გემოვნების, შვებულების, ინტერნეტ ძიების ისტორიის თაობაზე, ვაძლევთ წვდომას ტელეფონში არსებულ ფოტოებზე, კონტაქტებზე, საბანკო ბარათების მონაცემებზე და კიდევ ძალიან ბევრ პერსონალურ მონაცემზე, რომელთა ჯამი ჩვენს ციფრულ პორტრეტს ქმნის. მილიარდობით სხვა მონაცემთან ერთად კი შეადგენს ინფორმაციის იმ უზარმაზარ ერთობლიობას, რომელსაც Big Data ანუ დიდ მონაცემებს უწოდებენ. დიდი მონაცემების ანალიზი დიდ შესაძლებლობებს იძლევა. მათი დახმარებით შესაძლებელია ერთის მხრივ, გლობალური მასშტაბის სტატისტიკის, ტენდენციების, განწყობების დადგენა, ხოლო მეორე მხრივ კი კონკრეტული ტიპის ადამიანთა ჯგუფებზე შეთავაზების თუ რეკლამის მორგება. ამიტომ არ უნდა გაგვიკვირდეს, თუ საძიებო სისტემაში ცოტახნის წინ მოძებნილი ნივთები რეკლამების სახით გვიბრუნდება უკან, ან დღეს გაცნობილ ახალ თანამშრომელს სოციალური ქსელი მეგობრებში დასამატებლად გთავაზობთ. ბევრის აზრით, დიდი მონაცემების პოტენციალი იმდენად მასშტაბურია, რომ მისი დახმარებით ადამიანთა არჩევანზე ზემოქმედება და პოლიტიკური ცვლილებების გამოწვევაც არის შესაძლებელი და ეს პოტენციალი ტექნოლოგიურ პროგრესთან ერთად კიდევ უფრო იზრდება. სწორედ ამიტომ ითვლება დიდი მონაცემები პირადი ინფორმაციის დაცვის კუთხით ყველაზე დიდ გამოწვევად. თუ ასეთ მოცემულობაში საკუთარი მონაცემების კონტროლი გვსურს, პირველ რიგში უნდა დავფიქრდეთ იმაზე, თუ რა მონაცემებს გავცემთ ამა თუ იმ მომსახურების სანაცვლოდ, როგორ შეგვიძლია მათი მოცულობის შემცირება და უსაფრთხოების დაცვა.

2. პერსონალური მონაცემების გამჟღავნება და ხელმისაწვდომობა ინტერნეტსივრცეში

ინტერნეტი ერთ-ერთი ყველაზე მოთხოვნადი საშუალებაა დემოკრატიულ საზოგადოებაში. თუმცა, ამავე დროს, ის თავისი ხასიათით პერსონალური მონაცემების ხელყოფის საფრთხეს შეიცავს. კანონმდებელმა მონაცემთა სუბიექტს

(ფიზიკურ პირს) მიანიჭა უფლება, თავად მიიღოს გადაწყვეტილება, ვის, რა მიზნით და რა მოცულობის პერსონალური მონაცემების დამუშავების უფლება მისცეს. ამ წესიდან გამონაკლისი დასაშვებია მხოლოდ და მხოლოდ კანონით პირდაპირ გათვალისწინებულ შემთხვევებში, მაშინ, როდესაც საჯარო და კერძო ინტერესები შესაძლოა აღემატებოდეს მოქალაქის ინტერესებს. ,,პერსონალურ მონაცემთა დაცვის შესახებ'' საქართველოს კანონის მე-4 მუხლით დადგენილი მონაცემთა დამუშავების პრინციპები მონაცემთა დამუშავების საფუძვლებთან ერთობლიობაში ქმნის მონაცემთა სუბიექტების უფლებების დაცვის გარანტიას. პერსონალურ მონაცემთა დამუშავება არის კანონიერი მხოლოდ იმ შემთხვევებში თუ:

- არის შესაბამისობაში კანონთან; და
- ემსახურება ლეგიტიმურ მიზანს; და
- აუცილებელია დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნის მისაღწევად

მონაცემთა დამუშავების პრინციპების დარღვევა განსაკუთრებით საზიანო შეიძლება აღმოჩნდეს მონაცემთა სუბიექტისთვის მისი პერსონალური მონაცემების ინტერნეტში გასაჯაროების შემთხვევაში. ამ სივრცეში ინფორმაცია ხელმისაწვდომია ნებისმიერი მომხმარებლისთვის და პირთა განუსაზღვრელ წრეს ეძლევა შესაძლებლობა, გასაჯაროებული პერსონალური მონაცემები გამოიყენოს პირადი ინტერესებისათვის. ხშირად მონაცემთა გასაჯაროება შეიძლება აღქმული იყოს, როგორც ლეგიტიმური მიზნის მისაღწევად აუცილებელი საშუალება, თუმცა ყოველთვის უნდა მოხდეს შეფასება - შესაძლებელია თუ არა, ინფორმაცია გასაჯაროვდეს იმგვარად, რომ მაქსიმალურად იყოს დაცული მონაცემთა სუბიექტის ინტერესები.

2016 წელს პერსონალურ მონაცემთა დაცვის ინსპექტორს განცხადებით მიმართა სამმა არასრულწლოვანმა. ისინი მიუთითებდნენ, რომ ინტერნეტსივრცეში გასაჯაროებული იყო თბილისის საქალაქო სასამართლოს განჩინება, რომელიც შეეხებოდა განმცხადებლების ერთ-ერთი მშობლისათვის წარმომადგენლობითი უფლების შეზღუდვას. ინტერნეტსაძიებო სისტემაში განმცხადებლების სახელისა და გვარის მითითებისას ხელმისაწვდომი ხდებოდა სსიპ საერთო სასამართლოების დეპარტამენტის ვებგვერდზე განთავსებული განმცხადებლების პერსონალური მონაცემების შემცველი ინფორმაცია, კერძოდ 2014 წლის თბილისის საქალაქო სასამართლოს განჩინება საჯარო შეტყობინების შესახებ.

განცხადების განხილვის ფარგლებში გამოვლინდა, რომ საპროცესო კანონმდებლობის საფუძველზე, სსიპ საერთო სასამართლოების დეპარტამენტის ვებგვერდზე პერმანენტულად ქვეყნდებოდა სასამართლოს განჩინებები საჯარო შეტყობინებების შესახებ, თუმცა განსაზღვრული არ იყო, თუ რა ვადაში უნდა მომხდარიყო აღნიშნული მონაცემების ვებგვერდიდან წაშლა. საპროცესო კანონმდებლობის თანახმად, საჯარო შეტყობინების გამოქვეყნებიდან 7 დღის შემდეგ იგი მიიჩნევა მხარისათვის ჩაბარებულად, შესაბამისად აღნიშნული ვადის გასვლის შემდგომ არ იკვეთებოდა პერსონალური მონაცემების შემცველი განჩინების ვებგვერდზე განთავსების კანონიერი მიზანი. აღნიშნულიდან გამომდინარე, სასამართლოს დაევალა, შეეფასებინა და განესაზღვრა, შესაბამისი კანონიერი მიზნის მისაღწევად, რა ვადით და რა მოცულობით იყო საჭირო პერსონალური მონაცემების შემცველი საჯარო შეტყობინებების ვებგვერდზე საჯაროდ განთავსება და უზრუნველეყო ისეთი ორგანიზაციულ-ტექნიკური ზომების მიღება, რომელიც ზემოაღნიშნული ვადის გასვლის შემდგომ შესაძლებელს გახდიდა გასაჯაროებული მონაცემების ვებგვერდიდან წაშლას.

პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილების საფუძველზე საქართველოს იუსტიციის უმაღლესმა საბჭომ მიიღო 2016 წლის 12 სექტემბრის N1/250 გადაწყვეტილება, რომლის თანახმად, ვებგვერდზე გამოქვეყნებიდან 7 დღის გასვლის შემდეგ საჯარო შეტყობინება საჯაროდ ხელმისაწვდომი აღარ არის.

ხშირ შემთხვევაში მოქმედი კანონმდებლობა არ განსაზღვრავს მონაცემთა დამუშავების/გასაჯაროების კონკრეტულ ვადას, ხოლო ორგანიზაციებს არ აქვთ განსაზღვრული მონაცემთა დამუშავების კონკრეტული და მკაფიო მიზანი. შესაბამისად, მონაცემთა დამმუშავებლები მონაცემთა დამუშავების მიზნის მიღწევის შემდეგ არ შლიან არასაჭირო პერსონალურ მონაცემებს, არ ბლოკავენ მათ ან არ ინახავენ პირის იდენტიფიცირების გამომრიცხავი ფორმით (მაგ. ფსევდონიმირებით, ანონიმირებით).

ამ მხრივ განსაკუთრებით პრობლემურია ინტერნეტსივრცეში გასაჯაროებული მონაცემების დამუშავებასთან დაკავშირებული ვადები, ვინაიდან ასეთ შემთხვევაში მონაცემების გასაჯაროების ყოველი დამატებითი დღე არსებითად ზრდის მონაცემთა სუბიექტის კანონიერი ინტერესებისთვის ზიანის მიყენების საფრთხეს. მონაცემთა გასაჯაროების საკითხის შეფასებისთვის აუცილებელია, მონაცემთა დამმუშავებლებმა განსაზღვრონ:

- კონკრეტული, ლეგიტიმური მიზანი, რომელსაც ემსახურება მონაცემების საჯაროდ გამოქვეყნება
- რამდენად არის შესაძლებელი ლეგიტიმური მიზნის მიღწევა პერსონალური მონაცემების შემცველი ინფორმაციის გასაჯაროების გარეშე
- იმ შემთხვევაში, თუ აუცილებელია ლეგიტიმური მიზნის მისაღწევად პერსონალური მონაცემების გასაჯაროება, უნდა მოხდეს მიზნის პროპორციული ოდენობით მონაცემების დამუშავება და მიზნის მიღწევის შემდეგ გასაჯაროებული მონაცემების დაუყოვნებლივ წაშლა ვებგვერდიდან.

მეტი თვალსაჩინოებისათვის, უფრო ზუსტად კი იმისათვის, რომ დავრწმუნებულიყავი ქართულ ვებგვერდებზე რამდენად არის გასაჯაროებული/ხელმისაწვდომი ჩვენი პერსონალური მონაცემები, ჩავატარე კვლევა. კვლევისათვის ვეწვიე ცენტრალური საარჩევნო კომისიის ოფიციალურ ვებგვერდს (www.cesko.ge). ცენტრალური საარჩევნო კომისია (ცესკო) - საქართველოს საარჩევნო ადმინისტრაციის უმაღლესი ორგანოა, რომელიც თავისი უფლებამოსილების ფარგლებში უზრუნველყოფს საქართველოს პრეზიდენტის, საქართველოს პარლამენტის, რეფერენდუმისა და პლებისციტის გამართვას, საქართველოს მთელ ტერიტორიაზე აკონტროლებს საქართველოს საარჩევნო კანონმდებლობის შესრულებას, მის ერთგვაროვნად გამოყენებას და ა.შ.

ვებგვერდზე ამომრჩეველთა განყოფილებაში არის ასეთი გრაფა - გადაამოწმე შენი თავი, რომლის გახსნის შემდეგაც შეგვიძლია ჩვენი პირადი მონაცემების გადამოწმება ამომრჩეველთა ერთიან სიაში. ამისათვის კი მხოლოდ პირადი ნომერი და გვარი გვჭირდება.

პირადი ნომერი - პირის უნიკალური საიდენტიფიკაციო მონაცემია, რომელიც მას დაბადების რეგისტრაციისას ენიჭება. პირადი ნომერი მითითებულია ისეთ დოკუმენტებზე, როგორიცაა პირადობის მოწმობა, პასპორტი, მართვის მოწმობა და ა.შ. იმის გამო, რომ ორი იდენტური პირადი ნომერი არ არსებობს, იგი პირის იდენტიფიცირების ერთ-ერთი ყველაზე ფართოდ გავრცელებული მონაცემია და მისი გამოყენებით მონაცემთა ბაზებში ბევრი სხვადასხვა სახის ინფორმაციის მოძიებაა შესაძლებელი. სწორედ ამიტომ პირადი ნომრის შემცველ დოკუმენტებს განსაკუთრებული გაფრთხილება და დაცვა სჭირდება.

გვარი - პერსონალური მონაცემია, რომელიც პირს დაბადების რეგისტრაციისას ენიჭება. მითითებულია პრაქტიკულად ყველა დოკუმენტში (პასპორტში, პირადობის მოწმობაში, მართვის მოწმობაში, დიპლომში, ხელშეკრულებებში და ა.შ.). სხვა

პერსონალურ მონაცემებთან მაგ. სახელთან და დაბადების თარიღთან კომბინაციაში გვარი შესაძლოა გახდეს პირის უნიკალური მაიდენტიფიცირებელი მონაცემი.

ამ ორი მონაცემის შეყვანის შემდეგ გადავდივართ გვერდზე, სადაც ჩნდება დამატებითი მონაცემები ჩვენს შესახებ: სახელი, დაბადების თარიღი, იურიდიული მისამართი. თუმცა არამხოლოდ ჩვენი პერსონალური მონაცემები, არამედ ამავე იურიდიულ მისამართზე რეგისტრირებული ოჯახის წევრების პერსონალური მონაცემებიც ხდება ხელმისაწვდომი ჩვენთვის (იხ. დანართი N3).

აქედან გამომდინარე, თუ ნებისმიერმა უცხო პირმა იცის ჩვენი პირადი ნომერი და გვარი, მარტივად შეუძლია მოიძიოს დამატებითი ინფორმაცია არამარტო ჩვენს შესახებ, არამედ ჩვენი ოჯახის წევრების შესახებაც. არღვევს თუ არა ცესკო პერსონალურ მონაცემთა გასაჯაროების წესებს?

პირველ რიგში, როგორც ზემოთ აღვნიშნეთ, საქართველოს იუსტიციის უმაღლესი საბჭოს გადაწყვეტილების თანახმად, ვებგვერდზე გამოქვეყნებიდან 7 დღის გასვლის შემდეგ საჯარო შეტყობინება საჯაროდ ხელმისაწვდომი აღარ არის. ამასთან, მონაცემთა გასაჯაროების საკითხის შეფასებისათვის აუცილებელია, რომ მონაცემთა დამმუშავებლებმა განსაზღვრონ კრიტერიუმები. ერთ-ერთი კრიტერიუმის თანახმად, იმ შემთხვევაში, თუ აუცილებელია ლეგიტიმური მიზნის მისაღწევად პერსონალური მონაცემების გასაჯაროება, უნდა მოხდეს მიზნის პროპორციული ოდენობით მონაცემების დამუშავება და მიზნის მიღწევის შემდეგ გასაჯაროებული მონაცემების დაუყოვნებლივ წაშლა ვებგვერდიდან.

ცენტრალური საარჩევნო კომისიის მიზანი მიუკერძოებელი, გამჭვირვალე და მაღალპროფესიულ დონეზე ადმინისტრირებული არჩევნების კანონმდებლობის დონეზე ჩატარებაა, ამასთან, ყველა იმ პირობის შექმნაა, რათა ამომრჩევლებმა და სხვა ჩართულმა მხარეებმა თავისუფლად განახორციელონ საარჩევნო უფლება. საარჩევნო ადმინისტრაცია უზრუნველყოფს ამომრჩევლებისათვის ინფორმაციის ხელმისაწვდომობას და საკუთარი საქმიანობის ღიაობას. ელექტრონული პლატფორმაც - გადაამოწმე შენი თავი, სწორედ ამ მიზანს ემსახურება. ბოლოს, საპრეზიდენტო არჩევნები 2018 წლის 28 ნოემბერს ჩატარდა, მომდევნო საპარლამენტო არჩევნებამდე კი თითქმის 1 წელზე მეტია დარჩენილი. მიუხედავად იმისა, რომ მიზნის მიღწევის შემდეგ გასაჯაროებული მონაცემები დაუყოვნებლივ უნდა წაიშალოს, ცენტრალური საარჩევნო კომისია დღემდე არ ზღუდავს მომხმარებლების წვდომას ამ პლატფორმაზე და დღემდე შეგვძლია ნებისმიერი

პირის და მისი ოჯახის წევრების შესახებ მონაცემების მოძიება მხოლოდ ამ პირის პირადი ნომრისა და გვარის მითითებით.

მეორე მხრივ კი ვთვლი, რომ ცენტრალურ საარჩევნო კომისიას მეტი უსაფრთხოებისთვის უფრო ეფექტური და მძლავრი ბერკეტი სჭრიდება, რათა უზრუნველყოს ამომრჩეველთა პერსონალური მონაცემების დაცვა და არ გახადოს ეს მონაცემები მარტივად ხელმისაწვდომი უცხო პირთათვის. ამ მიზნის მიღწევა კი მრავალი საშუალებით შეიძლება. მაგ: სმს-ხელმოწერით, ელექტრონულ ფოსტაზე დამადასტურებელი კოდის ან ლინკის გაგზავნით და ა.შ.

2.1 ინტერნეტსივრცეში გავრცელებული ვიდეო-აუდიო ჩანაწერები

ინტერნეტსივრცეში მონაცემთა ხელმისაწვდომობის პრობლემატიკის განხილვისას, აუცილებლად უნდა აღინიშნოს სოციალური ქსელებითა და მედიასაშუალებებით პირადი ცხოვრების ამსახველი რამდენიმე ვიდეომასალისა და სატელეფონო საუბრის ჩანაწერების გავრცელების, ასევე პირადი ცხოვრების ამსახველი ვიდეომასალის გამოქვეყნების მუქარის შემაშფოთებელი ფაქტები.

იმას, რომ ვიდეოკამერები ყოველი ფეხის ნაბიჯზე გვხვდება, ალბათ უკვე მივეჩვიეთ, მაგ: მაღაზიებში, აფთიაქში, საზოგადოებრივ ტრანსპორტში, სამსახურში და ა.შ. ვიდეოთვალთვალი მონაცემთა დამუშავების საკმაოდ გავრცელებული და კანონით ნებადართული საშუალებაა, თუმცა კანონივე ადგენს წესებს, რომელთა დაცვაც აუცილებელია. მაგ: ,,პერსონალურ მონაცემთა დაცვის შესახებ'' კანონის მე-11 მუხლის თანახმად, ქუჩაში (მათ შორის, პარკში, სკვერში, სათამაშო მოედანთან, საზოგადოებრივი ტრანსპორტის გაჩერებასთან და სხვა თავშეყრის ადგილზე) და საზოგადოებრივ ტრანსპორტში ვიდეოთვალთვალის განხორციელება დასაშვებია მხოლოდ დანაშაულის თავიდან აცილების, აგრეთვე პირის უსაფრთხოებისა და საკუთრების, საზოგადოებრივი წესრიგისა და არასრულწლოვნის მავნე ზეგავლენისაგან დაცვის მიზნებისათვის. სხვა მიზნებისათვის, მაგ: ქცევის მონიტორინგისთვის ვიდეოთვალთვალის გამოყენება არ შეიძლება. ასევე არ შეიძლება ვიდეოთვალთვალი განხორციელდეს გამოსაცვლელ ოთახებსა და ჰიგიენისთვის განკუთვნილ ადგილებში. ფიზიკური პირის ვიდეო გამოსახულება წარმოადგენს გამოსახულებათა თანმიმდევრობის ჩანაწერს, რომელიც შეიძლება შეიქმნას ვიდეოთვალთვალის, ვიდეოკამერის, სმარტფონის ან სხვა ელექტრონული მოწყობილობების დახმარებით. ვიდეოგამოსახურება გამოიყენება ადამიანის

ამოსაცნობად, კონკრეტულ დროს და კონკრეტულ ადგილზე მისი მდებარეობის და მის მიერ განხორციელებული ქმედების დასადგენად. გამოსახულების ამსახველი ჩანაწერები კი ხელმისაწვდომია მხოლოდ სათანადო უფლებამოსილების მქონე პირთა ვიწრო წრისთვის.

ვიდეოთვალთვალთან დაკავშირებით საქმეზე ,,ლოპეზ რიბალდა და სხვები ესპანეთის წინააღმდეგ'' ადამიანის უფლებათა ევროპული სასამართლოს განმარტებით: ,,ადამიანის გამოსახულება მისი პიროვნულობის ერთ-ერთი მთავარი ატრიბუტია, ვინაიდან ის ამჟღავნებს პიროვნების უნიკალურ მახასიათებლებს და გამოარჩევს მას სხვებისაგან''. შესაბამისად, საკუთარი გამოსახულების დაცვის უფლება პირის განვითარების აუცილებელი კომპონენტია.

,,გმადლობთ, რომ დაგვიკავშირდით. გაცნობებთ, რომ მომსახურების გაუმჯობესების მიზნით თქვენი საუბარი იწერება.'' - ეს ტექსტი უცხო ალბათ არავისთვისაა, თუმცა ალბათ ბევრს არ უფიქრია, რომ ეს პერსონალური მონაცემების დამუშავების შესახებ ინფორმირებას წარმოადგენს. სატელეფონო მომსახურება არ არის ერთადერთი შემთხვევა, როდესაც ჩვენი ხმა იწერება. ხმის ჩაწერა ხდება სასამართლო დარბაზებში და სხდომებზე, ბანკში, აფთიაქებში და სხვა.

გასულ წლებში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა შეამოწმა არაერთი სააფთიაქო ქსელი, რომლებიც მომსახურების ხარისხის გაუმჯობესების მიზნით ვიდეოკონტროლთან ერთად მომხმარებელსა და მომსახურე პერსონალს შორის კომუნიკაციის აუდიოჩაწერასაც ახორციელებდნენ. შედეგად, არაერთ სააფთიაქო ქსელში შეწყდა აუდიოჩაწერა და დაინერგა მომსახურების კონტროლის სხვა მექანიზმები, რომლებიც დასაქმებულთა და მომხმარებელთა პირად ცხოვრებაში ნაკლებად ჩარევის საშუალებას იძლევა.

გამოვლენილი დარღვევები ცხადყოფს, რომ საჭიროა ამ საკითხის ნორმატიულ დონეზე დარეგულირება, რათა ნათლად და მკაფიოდ განისაზღვროს აუდიოჩაწერის ფუნქციის მქონე სისტემის დაყენებისას დამმუშავებლის ვალდებულებები, აუდიომონიტორინგის განხორციელების კანონიერი მიზნები და საფუძვლები.

ადამიანის პირად ცხოვრებაში ჩარევის ფორმის, მასშტაბისა და სენსიტიურობიდან გამომდინარე დაუშვებელია ნებისმიერი სახის ვიდეომასალისა თუ აუდიოჩანაწერის ინტერნეტსივრცეში გამოქვეყნება.

ცოტა ხნის წინ, პირადი ცხოვრების ამსახველი ვიდეომასალის ინტერნეტსივრცეში გავრცელების რამდენიმე შემთხვევაში სახელმწიფო უწყებების

ძალისხმევით ვიდეოჩანაწერების გამოქვეყნებიდან მალევე შეიზღუდა მასალაზე წვდომა, თუმცა დროის მცირე მონაკვეთიც საკმარისი იყო ვიდეოჩანაწერების გადმოწერისთვის და არსებობდა მათი შემდგომი გავრცელებისა და, შესაბამისად, ჩანაწერებში ასახული პირებისა და ოჯახის წევრების ინტერესების შელახვის მაღალი რისკი. წინა წლებისგან განსხვავებით, 2016 წელს ტელემედიისა და სოციალური ქსელების მომხმარებლების დიდმა ნაწილმა გამოავლინა მაღალი პასუხისმგებლობა და მასალის შემდგომი ტირაჟირებაც ნაკლებად მოხდა. საზოგადოება ასევე ერთიანი იყო ამ დანაშაულების სწრაფად და ეფექტიანად გამოძიების აუცილებლობის მოთხოვნისას, მათ შორის, ჩანაწერების წარმომავლობისა და ავთენტურობის საკითხების დადგენის კუთხით.

მიუხედავად იმისა, რომ 2016 წელს გახმაურებული ყველა შემთხვევა შეიცავდა დანაშაულის ნიშნებს და, შესაბამისად, სცდებოდა პერსონალურ მონაცემთა დაცვის ინსპექტორის კომპეტენციას, ინსპექტორმა საჯარო განცხადებების საშუალებით არაერთხელ გაუსვა ხაზი გამოძიებისა და ამგვარი დანაშაულის პრევენციის ეფექტიანი და სწრაფი მექანიზმების აუცილებლობას, ამ მიზნით უცხოელი ექსპერტების ჩართვის საჭიროებას, გამოძიების შედეგების მიმართ არსებულ მაღალ საჯარო ინტერესებს და აუდიო-ვიდეო ჩანაწერების გავრცელების ტენდენციის უარყოფით გავლენას არა მხოლოდ კონკრეტული პირების პირადი ცხოვრების ხელშეუხებლობის უფლებაზე, არამედ საზოგადოების აღქმასა და დამოკიდებულებაზე.

საანგარიშო პერიოდში ერთ-ერთი გაზეთის ინტერნეტგვერდის მეშვეობით გავრცელდა ვიდეომასალა - ე.წ. ციხის კადრები, რომელიც იძლეოდა პირთა სრულად იდენტიფიცირების საშუალებას, რაც ხელყოფდა მათ პატივსა და ღირსებას, ზიანს აყენებდა მათი და ოჯახის წევრების ინტერესებს. მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორის მანდატი არ ვრცელდება საზოგადოების ინფორმირების მიზნით მედია-საშუალებების საქმიანობის პროცესზე, ინსპექტორმა თავის საჯარო განცხადებაში ხაზი გაუსვა მედიის ვალდებულებას, დაიცვას ბალანსი საზოგადოების ინფორმირებასა და მოქალაქეთა პატივისა და ღირსების ხელშეუხებლობას შორის, მით უფრო, როდესაც საქმე ეხება წამებისა და არაადამიანური მოპყრობის არაერთ მსხვერპლს და გავრცელების ფორმა იძლევა მასზე შეუზღუდავი ხელმისაწვდომობის საშუალებას, რაც ყოვლად დაუშვებელია.

2018-2019 წლებშიც ჰქონდა ადგილი პირადი ცხოვრების ამსახველი ვიდეოკადრების ინტერნეტში გავრცელებას. არაერთი ცნობილი ადამიანი თუ

პოლიტიკოსი გახდა ვიდეოთვალთვალის მსხვერპლი. მომხდარ ფაქტებზე მიმდინარეობს გამოძიება საქართველოს სისხლის სამართლის კოდექსის 157-ე მუხლით, რაც პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ გამოყენებას ან/და გავრცელებას, ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით გულისხმობს.

სახელმწიფოს ვალდებულებაა გაატაროს მკაცრი პოლიტიკა და დასაჯოს დამნაშავე პირები. ამასთან, საზოგადოება უნდა იყოს ინფორმირებული, რომ პირადი ცხოვრების ამსახველი მასალის გავრცელება, შენახვა თუ დაარქივება სისხლის სამართლის დანაშაულია და უმკაცრეს სასჯელს ითვალისწინებს.

საქართველოს სისხლის სამართლის კოდექსი არაფერს ამბობს ისეთი ქმედების მიმართ, როცა საქმე ეხება არასრულწლოვანი პირისათვის პირადი ცხოვრების ამსახველი ვიდეოკადრების გავრცელებას. ვთვლი, რომ როცა საქმე არასრულწლოვანს ეხება, კანონი უფრო მკაცრი უნდა იყოს, რადგან ასეთი პირები ჯერ კიდევ ვერ არიან როგორც ფიზიკურად, ასევე ფსიქიკურად ბოლომდე ჩამოყალიბებულნი და შესაძლოა პირადი ცხოვრების ამსახველი კადრების გავრცელებამ უარესად დააზიანოს მათი ფსიქიკა.

აუცილებელია სახელმწიფო ორგანოებმა საფუძვლიანად იმუშაონ ამ მიმართულებით და შეიტანონ ცვლილებები სისხლის სამართლის კოდექსში, რათა განსხვავებულად, უფრო ზუსტად კი, მკაცრად დაისაჯოს ის პირი, ვინც ინტერნეტში გაავრცელებს არასრულწლოვანი პირების პირადი ცხოვრების ამსახველ ვიდეომასალას, ან დააშანტაჟებს მათ ამგვარი კადრების გავრცელებაზე. ქმედითი ნაბიჯების გარეშე კი ამგვარი პრობლემის აღმოფხვრა შეუძლებელია.

2.2 ტექნოლოგია და პერსონალური მონაცემები

ჩვენ ვცხოვრობთ სამყაროში, სადაც თითოეული ფეხის ნაბიჯზე საკუთარი პერსონალური მონაცემების კვალს ვტოვებთ. ტექნოლოგიური პროგრესის საუკუნეში ყოველ ახალ წელს ახალი შესაძლებლობები მოაქვს. იქმნება ახალი მოწყობილობები, უმჯობესდება მომსახურება, მარტივდება კომუნიკაცია, თუმცა ახალ შესაძლებლობებს თან ახლავს ახალი გამოწვევებიც, მათ შორის პერსონალური მონაცემების დაცვის კუთხით. სწრაფმა ტექნოლოგიურმა განვითარებამ და გლობალიზაციამ წარმოქმნა პერსონალური მონაცემების დაცვის ახალი გამოწვევები,

პერსონალურ მონაცემთა შეგროვებისა და გაცვლის მასშტაბი მნიშვნელოვნად გაიზარდა. ტექნოლოგია, როგორც კერძო, ასევე საჯარო უწყებებს თავისი საქმიანობის განხორციელებისას პერსონალური მონაცემების უპრეცედენტო მასშტაბით გამოყენების შესაძლებლობებს აძლევს. ფიზიკური პირები თავის პერსონალურ მონაცემებს უფრო მეტად ასაჯაროებენ და გლობალურად ხელმისაწვდომს ხდიან. ტექნოლოგიამ გარდაქმნა როგორც ეკონომიკა, ისე საზოგადოებრივი ცხოვრება, და მომავალში კიდევ უფრო გააადვილებს ინფორმაციის თავისუფალ მიმოცვლას ევროკავშირის შიგნით და მის მიღმა არსებულ ქვეყნებსა და საერთაშორისო ორგანიზაციებს შორის.

სწორედ ამ მოვლენებთან გასამკლავებლად შეიქმნა უფრო ძლიერი და თანმიმდევრული მარეგულირებელი ჩარჩო - პერსონალურ მონაცემთა დაცვის ახალი ევროპული რეგულაცია GDPR, რომელიც ძალაში შევიდა 2018 წლის მაისში. რეგულაცია სავალდებულოა არამხოლოდ ევროკავშირის წევრი ქვეყნებისათვის, არამედ იმ ორგანიზაციებისთვის, რომლებიც მის ფარგლებს გარეთ არიან რეგისტრირებულნი, მაგრამ ამუშავებენ ევროკავშირის წევრი ქვეყნების მოქალაქეთა პერსონალურ მონაცემებს. მაგ: მათ შორის არიან ისეთი გიგანტი კომპანიები, როგორიცაა Google, Facebook და სხვა.

დავფიქრებულვართ იმაზე, თუ რა პრინციპით გვთავაზობს ყველასათვის ,,საყვარელი" და პოპულარული Facebook-ი შესაძლო ნაცნობთა სიას?

Facebook-ის ოფიციალური წარმომადგენლები ამასთან დაკავშირებით ამბობენ, რომ შესაძლო ნაცნობების მეგობრებში დამატებას რამდენიმე ინფორმაციის საფუძველზე გვთავაზობს:

- საერთო მეგობრები
- Facebook-ის რომელიმე საერთო ჯგუფში ყოფნა ან ერთ ფოტოზე მონიშვნა
- კავშირები
- კონტაქტები (მობილურიდან, ელექტრონული ფოსტიდან და სხვა)

ელექტრონული ფოსტა - პერსონალური მონაცემია, რომელიც ელექტრონული კომუნიკაციისთვის გამოიყენება. ელექტრონული ფოსტის გარეშე შეუძლებელია დარეგისტრირება სოციალურ ქსელებში, სხვადასხვა ვებგვერდებსა თუ ონლაინ მაღაზიებში. მიუხედავად იმისა, რომ ელექტრონული ფოსტა სხვა განზომილებაა და Facebook-ი სხვა, ეს უკანასკნელი მაინც ახერხებს წვდომას მომხმარებლის ფოსტაზე და ამუშავებს მონაცემებს. გარდა ელექტრონული ფოსტისა, Facebook-ი ამუშავებს ასევე ჩვენს პერსონალურ მონაცემებს, კონტაქტებს, კავშირებს, რომელზე წვდომის

უფლებასაც ჩვენ თავად ვაძლევთ მას და სწორედ ამის საშუალებით გვთავაზობს იგი შესაძლო ნაცნობთა სიას.

რა ინფორმაციას ინახავს Google ჩვენს შესახებ?

Google-ის ანგარიშებზე შესვლის მომენტიდან მისი სერვისების საშუალებით განხორციელებული ნებისმიერი აქტივობა, მათ შორის: რას ვეძებთ, რომელ ვიდეოს ვუყურებთ, რა დროს სად ვიმყოფებით, მობილურით შევედით თუ პერსონალური კომპიუტერით, ჩვენი კონტაქტები, კალენდარი და სხვა. შესაძლებელია განუსაზღვრელი ვადით ინახებოდეს. აქტივობები შესაძლებელია ინახებოდეს მაშინაც, როდესაც ინტერნეტში არ ვართ და Google-ის სერვერებზე იგზავნებოდეს ინტერნეტთან დაკავშირების შემდეგ. Google-ის ანგარიშებზე ინახება ყველაფერი, მათ შორის რა ,,დავგუგლეთ'', რა დროს და რა სიხშირით, რომელ საიტს ვეწვიეთ, რამდენჯერ და რომელი მოწყობილობებიდან. ეს, ერთის მხრივ, გვეხმარება ძებნის სწრაფი და ჩვენზე მორგებული შედეგების და პროდუქტების მიღებაში, მეორე მხრივ კი, საშუალებას აძლევს Google-ს ფლობდეს ინფორმაციას ჩვენი ინტერესების, გემოვნების, ინტერნეტის ისტორიის და კიდევ სხვა ძალიან ბევრი რამის შესახებ.

ინტერნეტის ისტორია - ინტერნეტის მომხმარებლის მიერ გამოყენებული ვებგვერდების ჩამონათვალია, რომელსაც ბრაუზერი ინახავს. იგი მოიცავს ვებგვერდის დასახელებას, ვიზიტის დროს და კონკრეტულ ლინკს. უფრო ფართო გაგებით კი ინტერნეტისტორია ასახავს მომხმარებლის მიერ ინტერნეტში დატოვებულ ნებისმიერ კვალს. ინტერნეტის ისტორიაზე ხელმისაწვდომობის სრული შეზღუდვა პრაქტიკულად შეუძლებელია, თუმცა არსებობს კონტროლის მექანიზმები. მაგ: ისტორიის წაშლა, რის საშუალებასაც ნებისმიერი ბრაუზერი იძლევა.

Google ინახავს ინფორმაციას ჩვენი ლოკაციის შესახებ. ლოკაცია - ეს არის ინფორმაცია ფიზიკური პირის ან მასთან დაკავშირებული რომელიმე ელექტრონული მოწყობილობის შესახებ, რომლითაც შესაძლებელია დადგინდეს გეოგრაფიული ადგილსამყოფელი, გადაადგილების მიმართულება ან დრო. ინფორმაციას ლოკაციის შესახებ თავად გავცემთ. მაგ: ვაძლევთ წვდომის უფლებას ინტერნეტ აპლიკაციებს, ვებგვერდებს, ვაკეთებთ მონიშვნებს სოციალურ ქსელში და ა.შ. ლოკაციის შესახებ ინფორმაციის გაცემამდე აუცილებელია დავფიქრდეთ იმაზე, თუ რამდენად სანდოა ესა თუ ის აპლიკაცია ან ვებგვერდი და რამდენად აუცილებელია ჩვენი ლოკაციის გაზიარება მათთვის.

Facebook-ის და Google-ის შემთხვევაში დავრწმუნდით, რომ როგორც დასაწყისში აღვნიშნეთ, უფასო მომსახურებებიც არ არის ბოლომდე უფასო და მათ მისაღებად ჩვენს პერსონალურ მონაცემებს ,,ვიხდით'', თავად ვაძლევთ უფლებას კომპანიებს დაამუშაონ და შეაგროვონ ჩვენს შესახებ ინფორმაცია და შემდგომ ეს ყველაფერი გამოიყენონ საკუთარი მიზნებისათვის, მაგ: მარკეტინგისათვის.

2.3 პირდაპირი მარკეტინგული საქმიანობა ინტერნეტსივრცეში

საქართველოს კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ'' პირდაპირ მარკეტინგს შემდეგნაირად განმარტავს: ,,პირდაპირი მარკეტინგი - ფოსტის, სატელეფონო ზარების, ელექტრონული ფოსტის ან სხვა სატელეკომუნიკაციო საშუალებით საქონლის, მომსახურების, დასაქმების ან დროებითი სამუშაოს შეთავაზებაა.''

პირდაპირი მარკეტინგის განმახორციელებელი არის საჯარო დაწესებულება, ფიზიკური ან იურიდიული პირი, რომელიც განსაზღვრავს პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა დამუშავების საშუალებებს, უშუალოდ ან უფლებამოსილი პირის (მაგალითად, სარეკლამო კომპანია) მეშვეობით ახორციელებს მონაცემთა დამუშავებას. ხოლო პირდაპირი მარკეტინგის სუბიექტი არის ნებისმიერი ფიზიკური პირი (მომხმარებელი), რომელიც მისი პერსონალური მონაცემების დამუშავების შედეგად იღებს მომსახურების ან საქონლის შეთავაზებას.

,,პერსონალურ მონაცემთა დაცვის შესახებ'' საქართველოს კანონი განსაზღვრავს პირდაპირი მარკეტინგის სუბიექტის უფლებებს:

- იცოდეს მონაცემთა შეგროვების წყარო, მარკეტინგის განმახორციელებლის ვინაობა, მონაცემთა დამუშავების მიზანი და კანონიერი საფუძველი;
- იცოდეს, რა მონაცემები მუშავდება მის შესახებ და ნებისმიერ დროს მოითხოვოს მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა ან განადგურება;
- მოითხოვოს მისი მონაცემების პირდაპირი მარკეტინგის მიზნებისათვის გამოყენების შეწყვეტა ნებისმიერ დროს (მიუხედავად იმისა, აქვს თუ არა თანხმობა გაცემული) იმავე ფორმით, რა ფორმითაც ხორციელდება მარკეტინგი ან გამოიყენოს სხვა ხელმისაწვდომი და ადეკვატური საშუალება;
- უარი განაცხადოს მისი მონაცემების მესამე პირებისთვის გადაცემაზე.

პირდაპირი მარკეტინგის მიზნებისთვის პერსონალური მონაცემები შეიძლება შეგროვდეს:

- საჯაროდ ხელმისაწვდომი წყაროებიდან; ან
- უშუალოდ მომხმარებლისგან.

საჯაროდ ხელმისაწვდომი წყაროებიდან შეიძლება შეგროვდეს მხოლოდ შემდეგი მონაცემები: **სახელი, გვარი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი და ფაქსის ნომერი.** იმ შემთხვევაში, თუ სუბიექტის შესახებ გროვდება ჩამოთვლილთაგან განსხვავებული მონაცემები, **აუცილებელია მონაცემთა სუბიექტის წერილობითი თანხმობა.**

მაღაზიაში ნივთის შეძენისას პირმა დატოვა საკონტაქტო მონაცემები და სურს, მიიღოს შეტყობინება ახალი პროდუქციის შესახებ.

იმის გამო, რომ წლების განმავლობაში არ არსებობდა პერსონალური მონაცემების დაცვის შესახებ კანონმდებლობა, ხშირად ხდებოდა სხვადასხვა სახის პერსონალური მონაცემების გასაჯაროება, გაზიარება, გაყიდვა. შესაბამისად, წარმოიქმნა საკმაოდ მოცულობითი ბაზები, რომელთა ლეგიტიმურობისა და წყაროს დადგენა სირთულეებთან არის დაკავშირებული. ამასთანავე, მოქმედი კანონი 2016 წლამდე არ ითვალისწინებდა კერძო სექტორის მიმართ ინსპექტირებისა და შესაბამისი სანქციების გამოყენების შესაძლებლობას, რის გამოც ვერ ხდებოდა ეფექტური რეაგირება მოქალაქეების საჩივრებზე. დღეისათვის კი, თუ უარის მიუხედავად კომპანია კვლავ აგრძელებს სარეკლამო შეტყობინებების გამოგზავნას, მომხმარებელს უფლება აქვს მიმართოს პერსონალურ მონაცემთა დაცვის ინსპექტორს ან სასამართლოს. ,,პერსონალურ მონაცემთა დაცვის შესახებ'' კანონით დადგენილი წესების დარღვევის გამოვლენის შემთხვევაში პირდაპირი მარკეტინგის განმახორციელებელი კომპანია დაჯარიმდება 3 000 ლარით, ხოლო თუ იგი ერთი წლის განმავლობაში კვლავ დაარღვევს კანონს, ჯარიმა 10 000 ლარს შეადგენს.

ბოლო დროს მოქალაქეებისათვის მოკლე ტექსტური შეტყობინებების გზით სხვადასხვა სახის პროდუქციისა თუ მომსახურების შეთავაზებამ იმდენად მასშტაბური ხასიათი მიიღო, რომ მოქალაქეთა უკმაყოფილება სწორედ არასასურველ შეტყობინებებს და ამ მიზნით მათი პერსონალური მონაცემების დამუშავებას ეხება. სუბიექტები ვერ იღებენ ინფორმაციას მათი მონაცემების შეგროვების წყაროსა და დამუშავების შეწყვეტის საშუალებების შესახებ, ვინაიდან მათთვის უცნობია ვინ არის მონაცემთა დამმუშავებელი - მობილური ოპერატორი, სარეკლამო კომპანია თუ რეკლამის დამკვეთი.

მოქალაქეებისთვის, და პირადად ჩემთვისაც უცნობი იყო, თუ საიდან მოხვდა ტელეფონის ნომერი თუ ელ.ფოსტის მისამართი კერძო კომპანიების ხელთ. პრაქტიკულად 2014 წლამდე შეუძლებელი იყო მონაცემთა დამუშავების შეწყვეტის მოთხოვნა. განსაკუთრებით მაშინ, როცა რეკლამის განმახორციელებელი ორგანიზაციის იდენტიფიცირება ვერ ხდებოდა. გარდა ამისა, ადგილი ჰქონდა ინტერნეტსივრცეში საჯაროდ განთავსებული სატელეფონო ნომრების მარკეტინგული მიზნით გამოყენებას. არსებული საკანონმდებლო რეგულაცია კი ვერ უზრუნველყოფდა მოქალაქეთა უფლებების დაცვას.

საკითხის აქტუალობიდან გამომდინარე, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა მოამზადა კანონპროექტი, რომლის თანახმადაც გამარტივდა სარეკლამო შეტყობინებებზე უარის თქმის მექანიზმი და მოქალაქეებს მიეცათ შესაძლებლობა, ნებისმიერ დროს მოითხოვონ მათი მონაცემების გამოყენების შეწყვეტა. ხოლო პირდაპირი მარკეტინგის განმახორციელებელი კომპანიები/ორგანიზაციები ვალდებულნი არიან, შექმნან უარის თქმის მექანიზმი იმავე ფორმით, რა ფორმითაც ხორციელდება პირდაპირი მარკეტინგი ან/და შეიმუშაონ სხვა ხელმისაწვდომი და ადეკვატური საშუალება.

2015 წელს პირდაპირი მარკეტინგის განმახორციელებელი ორგანიზაციების უმრავლესობამ უზრუნველყო შეტყობინებებზე უარის თქმის მექანიზმის დანერგვა, რომელიც შეტყობინების ადრესატს აძლევს შესაძლებლობას, მითითებული ტექსტი გაგზავნოს კონკრეტულ ნომერზე და ამგვარად განაცხადოს უარი მისი მონაცემების პირდაპირი მარკეტინგის მიზნით გამოყენებაზე. აღნიშნული მექანიზმის პრაქტიკაში გამოყენებისა და ეფექტურობის მაგალითად შეიძლება ერთ-ერთი სარეკლამო მომსახურების გამწევი კომპანიის მონაცემების მოყვანა, რომლის თანახმადაც შეტყობინებების მიღებაზე უარის თქმის მექანიზმით ისარგებლა 311 962 აბონენტმა.

გარდა მოკლე ტექსტური შეტყობინებებისა, კომპანიები ხშირად ახდენენ მათი საქონლის ან მომსახურების შეთავაზებას ელექტრონული ფოსტისა თუ სოციალური ქსელის მეშვეობით. ამ შემთხვევაში მნიშვნელოვანია, ორგანიზაციებმა პირდაპირი მარკეტინგის განხორციელებისას გაითვალისწინონ, რომ აღნიშნული გზებით სარეკლამო შინაარსის შეტყობინებების გაგზავნისას ასევე სავალდებულოა ,,პერსონალურ მონაცემთა დაცვის შესახებ'' საქართველოს კანონით დადგენილი პირდაპირი მარკეტინგის განხორციელების წესების დაცვა, როგორც მოკლე ტექსტური შეტყობინებების გაგზავნის დროს.

როგორ ხდება პირდაპირი მარკეტინგული საქმიანობა სოციალურ ქსელში?

წინა თავში ორი მსხვილი კომპანიის Google და Facebook-ის მაგალითები განვიხილეთ და აღვნიშნეთ, რომ კომპანიებს ჩვენ თავად ვაძლევთ უფლებას დაამუშაონ ჩვენი პერსონალური მონაცემები და გამოიყენონ ისინი საკუთარი მიზნებისთვის. კომპანიები ჩვენს პერსონალურ მონაცემებს რეკლამის სწორად შესარჩევად იყენებენ და ამ ფაქტს არც მალავენ. მაგ. Facebook-ის კომპანიის პრესსპიკერი ამბობს: ,,ჩვენ გვინდა, რომ რეკლამები, რომლებსაც Facebook-ის მომხმარებლები ხედავენ, გამოსადეგი და შესაბამისი იყოს''.

კომპანია რეკლამების შესაბამისობას ჩვენს გემოვნებასთან და სურვილებთან კი შემდეგი გზებით ახერხებს:

- აანალიზებს ჩვენს ონლაინ აქტივობას (გვერდებს, რომლებსაც ვიწონებთ; რეკლამები, რომლებსაც ვნახულობთ);
- აკვირდება ჩვენს ტელეფონს და კომპიუტერს (რომელ ბრენდს ვიყენებთ, რომელი ტიპის ინტერნეტს ვანიჭებთ უპირატესობას, ტელეფონიდან უფრო ხშირად ვსტუმრობთ აღნიშნულ სოციალურ ქსელს თუ კომპიუტერიდან და ა.შ.);
- აანალიზებს ჩვენს და ჩვენთან დაკავშირებული ადამიანების მონაცემებსა და გემოვნებას (ვინ არიან ჩვენი მეგობრები, ოჯახის წევრები; ვინ არია ადამიანები, რომლებთანაც ყველაზე ხშირად გვაქვს კომუნიკაცია და ა.შ.);
- აანალიზებს ჩვენს ქცევას (სად ვმუშაობთ, სად ვცხოვრობთ, რა ტიპის სტატიებს ვკითხულობთ და ვაზიარებთ).

ერთად თავმოყრილი მთელი ეს ინფორმაცია ჩვენს სრულყოფილ ციფრულ პორტრეტს იძლევა, ამიტომ არ უნდა გაგვიკვირდეს, რომ Facebook-ს ჩვენი ,,აზრების კითხვა'' შეუძლია.

როგორ მოვიქცეთ იმ შემთხვევაში, თუ არ გვინდა ჩვენი ,,აზრები წაიკითხონ''?

ამისათვის კომპანია თავის მომხმარებლებს აძლევს რეკლამების დამალვის და რეკლამის სასურველი ტიპის შერჩევის შესაძლებლობას, თუმცა როგორც ექსპერტები ამბობენ, ამით ,,ციფრული პორტრეტის'' მხოლოდ გაფერმკრთალება შეგვიძლია, ბოლომდე გაქრობა კი არა.

არის თუ არა ასეთი მოქმედება სარეკლამო შეტყობინებებზე უარის თქმის ხელმისაწვდომი და ადეკვატური საშუალება?

როგორც მსოფლიო მოსახლეობის უმრავლესობა, მეც ვსარგებლობ სოციალური ქსელით - Facebook აპლიკაციით. დასმულ კითხვაზე პასუხის გასაცემად

ჩავატარე კვლევა. ჩემს პერსონალურ Facebook გვერდზე ვცადე ყველანაირი რეკლამის დამალვა, თუმცა უშედეგოდ. დამალული რეკლამის ადგილას სხვა, ახალი რეკლამა ჩნდებოდა და ასე დაუსრულებლად.

ჩემს მიერ ჩატარებულმა კვლევამ მაჩვენა, რომ რეკლამის დამალვა არ აძლევს სოციალური ქსელის მომხმარებლებს იმის საშუალებას, რომ უარი თქვან სარეკლამო შეტყობინებებზე. აქედან გამომდინარე კი ვთვლი, რომ ინტერნეტმომხმარებლებისთვის შეთავაზებული გზები, სარეკლამო შეტყობინებებზე უარის თქმასთან დაკავშირებით, არ არის ხელმისაწვდომი და ადეკვატური. არ არის იმდენად ეფექტური, როგორც მოკლე ტექსტური შეტყობინებებით მარკეტინგის განხორციელებისას. არადა დასაწყისში აღვნიშნეთ, რომ ,,პერსონალურ მონაცემთა დაცვის შესახებ'' საქართველოს კანონით დადგენილი პირდაპირი მარკეტინგის განხორციელების წესები ორივე შემთხვევაში საერთოა.

მეტი თვალსაჩინოებისათვის წარმოგიდგენთ რამოდენიმე პოპულარული სოციალური ქსელის მაგალითს, რომელიც პერსონალურ მონაცემთა დაცვის ინსპექტორის, ,,ინტერნეტ სივრცეში პერსონალურ მონაცემთა დაცვის შესახებ'', რეკომენდაციაშია განხილული:

ქსელი: / ფუნქციები:	Facebook	Twitter	Linked in	Google+
რეკლამების კონტროლი	√	X	X	X
სარეკლამო შეთავაზებებზე უარის თქმა	X	X	X	X

დასკვნის სახით ჩამოვაყალიბებ, რომ პირდაპირი მარკეტინგული საქმიანობა ინტერნეტსივრცეში დასახვეწია. თუ კომპანიები ჩვენივე თანხმობით ამუშავებენ მონაცემებს სარეკლამო შეტყობინებებისთვის, მათივე ვალდებულებაა შემოგვთავაზონ უარის თქმის ისეთი მექანიზმები, რომლებიც ეფექტურად ,,მუშაობენ'' და გვანიჭებენ უფლებას, სამუდამოდ დავემშვიდობოთ არასასურველ სარეკლამო შეტყობინებებს.

2.4 ონლაინ შესყიდვა

როდესაც საქმე პერსონალური მონაცემების ინტერნეტსივრცეში გამჟღავნებას და ხელმისაწვდომობას ეხება, არ უნდა დავივიწყოთ ონლაინ შესყიდვები. ონლაინ შესყიდვა (online shopping) - სულ უფრო პოპულარული ხდება და ყოველდღიურად იზრდება იმ მომხმარებელთა რაოდენობა, რომლებიც არჩევანის მრავალფეროვნების, ფასის, ხარისხის, სიმარტივისა და სხვა მახასიათებლების გამო უპირატესობას ონლაინ მაღაზიებს ანიჭებენ. ონლაინ ვაჭრობას თან ახლავს ჩვენს პერსონალურ და ფინანსურ მონაცემთა დაცულობასთან დაკავშირებული რისკები. უფრო ზუსტად კი, ჩვენი საბანკო ანგარიშები ან მონაცემები შეიძლება ხელმისაწვდომი გახდეს უამრავი ცნობისმოყვარე თვალისთვის, რადგან ნებისმიერ საიტზე, სადაც შეგვიძლია ონლაინ შესყიდვის განხორციელება, რეგისტრაციისას ვუთითებთ არამარტო ჩვენს პერსონალურ მონაცემებს, არამედ საბანკო ბარათებს, ანგარიშებს და ა.შ.

მომხმარებლები უპირატესობას ანიჭებენ შეიძინონ ნივთები სახლიდან გაუსვლელად. ონლაინ მაღაზიები კი ასეთ მომხმარებლებს სთავაზობენ სავაჭრო ობიექტებში ან სხვა საზოგადოებრივი თავშეყრის ადგილებში სიარულის ალტერნატივას. მეტიც, ონლაინ შესყიდვას იმაზე ნაკლები დრო სჭირდება, ვიდრე მაღაზიებში სიარულს და სასურველი ნივთების მოძიებას.

ინტერნეტ-მაღაზიები იყენებენ სხვადასხვა ტექნოლოგიებს, რათა სავაჭრო პროცესი იყოს უფრო ეფექტური და სასიამოვნო. ამ ყველაფრის მიზანი კი გაყიდვების გაზრდაა. მაგ. ბევრ ინტერნეტ-მაღაზიას აქვს შესაძლებლობა დაიმახსოვროს ინფორმაცია ჩვენს საკრედიტო ბარათზე (ბარათის ციფრები, CVV კოდი, ანგარიშის ნომერი), ასევე შეაგროვოს ინფორმაცია იმის შესახებ, თუ რომელი კატეგორიის ნივთებს უფრო მეტ ყურადღებას ვუთმობთ. ეს ყველაფერი კი ისევ და ისევ მარკეტინგისთვის ესაჭიროებათ. ინტრნეტ-მაღაზიები იმახსოვრებენ ჩვენს შესყიდვების ისტორიას (თუკი რაიმე ნივთი შეგვიძენია ონლაინ შესყიდვით), იქმნიან წარმოდგენას იმის შესახებ, თუ სხვა რა ნივთები ან პროდუქტები შეიძლება შემოგვთავაზონ და ჩვენც სიამოვნებით შევიძინოთ.

მაგრამ, სანამ ვზივართ კომპიუტერთან, ან მობილური ტელეფონით ვარჩევთ ნივთებს, რომლის შეძენაც გვსურს, გვიფიქრია იმაზე თუ დროის დაზოგვის ან სახლიდან გაუსვლელობის გამო რა საფრთხეს ვუქმნით ჩვენს პერსონალურ მონაცემებს?

ნებისმიერი ნივთის ონლაინ შეძენის დროს, პარალელურ რეჟიმში ხდება ჩვენი საბანკო ბარათიდან თანხის მოხსნა და ონლაინ შესყიდვის განმახორციელებელი კომპანიის ანგარიშზე გადარიცხვა. ამიტომ ერთ-ერთი მნიშვნელოვანი საკითხია იმ კომპანიის ლეგიტიმურობა და სანდოობა, რომელიც ახორციელებს ონლაინ შესყიდვას. თუ შესყიდვას ვახორციელებთ ისეთი ვებგვერდიდან, რომელიც ელექტრონული ფოსტის ან ნებისმიერი სოციალური ქსელის ე.წ საეჭვო გზავნილების (Spam-ის) საქაღალდეში შემოვიდა რეკლამის სახით, ასეთი ვებგვერდიდან შესყიდვის განხორციელება საფრთხის შემცველია, რადგან შესაძლოა გავხდეთ ე.წ. ,,phishing''-ის (ფიშინგი) მსხვერპლი. ფიშინგი - ინტერნეტ-თაღლითობის ფორმაა, როდესაც ხდება პირადი დაცული ინფორმაციის მოპარვა. იგი ყალბი ელექტრონული ფოსტის დაგზავნით ან ყალბ ვებგვერდზე ჩვენი შეტყუებით ანგარიშის, პაროლის, ფინანსური და სხვა პერსონალური მონაცემების მითვისებას ისახავს მიზნად. ზოგიერთი კომპანია სწორედ საეჭვო შეტყობინებების (spam) გაგზავნით ახდენს აკრძალული პროდუქციის ან მომსახურების რეკლამირებას. ფიშინგის დროს იქმნება ჩვენს პერსონალურ ინფორმაციაზე, მათ შორის საბანკო მონაცემებზე არასანქცირებული წვდომის რეალური საფრთხე. ამიტომ, თუ გვინდა, რომ დავიცვათ ჩვენი როგორც პერსონალური, ისე ფინანსური მონაცემები, ონლაინ შესყიდვა ისეთი ვებგვერდიდან უნდა განვახორციელოთ, რომელსაც მისამართის ველში თან ერთვის **ბოქლომის სიმბოლო**, რაც მიუთითებს ტრანზაქციების დაცულობაზე. ვებგვერდზე ბარათის მონაცემების შეყვანისას, ბოქლომის სიმბოლოსთან ერთად მისამართის პანელი უნდა იწყებოდეს HTTPS://-ის გამოსახულებით (ნაცვლად HTTP://-ისა), სადაც S-ი (secure) მიუთითებს ვებგვერდის უსაფრთხოებაზე.

2.4.1 ინტერნეტთაღლითობა ფინანსური მონაცემების მოსაპოვებლად

აქვე განვიხილავ კიდევ ერთ საკითხს, რომელიც ისევ და ისევ ,,ფიშინგს'' ეხება. ინტერნეტთაღლითობა მსოფლიოში და უკვე რამოდენიმე თვეა საქართველოშიც გავრცელებული დანაშაულია. ცხოვრების თანამედროვე ტემპმა, ციფრული არხებით სარგებლობაზე მზარდმა მოთხოვნამ ადამიანებში, გამოიწვია უსაფრთხოებასთან დაკავშირებული გარკვეული საკითხების აქტუალიზებაც, რაც მეტ გასაქანს აძლევს მთელს მსოფლიოში ინტერნეტთაღლითობას, ე.წ. ,,ფიშინგს''. თუმცა ეს იმას არ ნიშნავს, რომ არ უნდა ვენდოთ ისეთ კომფორტულ საშუალებებს, როგორებიცაა მობილბანკი და ინტერნეტბანკი. ჩვენგან საჭიროა ცოტა მეტი ყურადღება, სიფრთხილე და დაკვირვება, რადგან ინტერნეტთაღლითები ბანკის სახელს, ლოგოს,

ყალბი ვებგვერდის მისამართებს არიან ამოფარებულები და ასე ცდილობენ მახეში გააბან მომხმარებლები და მოიპოვონ მათ ფინანსურ მონაცემებზე წვდომა.

ფიშინგი არის კიბერთაღლითობის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლს მოტყუების გზით მოპაროს სენსიტიური ინფორმაცია. შეტევის დროს გამოიყენება მეილი, რომელიც იგზავნება კიბერ-კრიმინალების მიერ. ძირითადად, მეილი წარმოჩენილია როგორც სანდო წყაროსგან მიღებული შეტყობინება. მაგ: როგორიცაა ბანკი ან ნებისმიერი სხვა ორგანიზაცია თუ პირი, ვისთანაც მსხვერპლს შესაძლოა ქონდეს ურთიერთობა. ამასთან, მეილი შენიღბულია როგორც სასწრაფო შეტყობინება, რომელშიც დამატებითი ინფორმაციისთვის მოთავსებულია ვებ-ბმულები ან მიმაგრებული დოკუმენტები. ფიშინგ მეილში მოთავსებულ ბმულზე გადასვლის, ან ფაილის გახსნის შედეგად შესაძლებელია მოხდეს მსხვერპლის კომპიუტერში შეღწევა ან მისგან დამატებით სენსიტიური ინფორმაციის მოთხოვნა (პაროლი, მომხმარებლის სახელი, ბარათის ინფორმაცია და სხვა). კიბერ-დამნაშავეები ცდილობენ ფიშინგ მეილები დააგზავნონ მასიურად, მაქსიმალურად მეტ ადრესატთან, რაც მათი წარმატების ალბათობას რეალურს ხდის.

მაგ. საქართველოს ბანკი - საქართველოს წამყვანი ბანკია, რომელიც ემსახურება 2,3 მილიონ მომხმარებელს. იგი გარდა სტანდარტული მომსახურებებისა, თავის ერთგულ მომხმარებლებს სთავაზობს ინტერნეტბანკს და მობილბანკს, რაც თავის მხრივ ეხმარება ადამიანებს სწრაფად და მარტივად, ასევე სახლიდან გაუსვლელად შეასრულონ გადახდები, გადარიცხვები, შეამოწმონ ანგარიშები და ა.შ. საქართველოს ბანკისთვის ერთ-ერთი მთავარი ვალდებულებაა მისი მომხმარებლების ფინანსური მონაცემების დაცვა ინტერნეტთაღლითებისგან. ბანკი ოფიციალური გვერდის საშუალებით აფრთხილებს მომხმარებლებს, თუ როგორ დაიცვან ფინანსური მონაცემები და იგრძნონ თავი უსაფრთხოდ. (იხ. დანართი N4)

პირველ რიგში უნდა გავიაზროთ, რომ გარკვეულ დროს შეიძლება ნებისმიერი ჩვენგანი გახდეს ფიშინგის მსხვერპლი. ამიტომ ზუსტად უნდა ვიცოდეთ ის, თუ როგორ დავიცვათ ჩვენი ფინანსური მონაცემები ინტერნეტთაღლითებისგან. მთავარია გამოვიჩინოთ სიფრთხილე და ყურადღებით ვიყოთ სანამ ნივთის ონლაინ შესყიდვას, ან თუნდაც ინტერნეტბანკით რაიმე ტრანზაქციას განვახორციელებთ. ფინანსური და ზოგადად, პერსონალური მონაცემების დაცვა კი პირადი სივრცის დაცვაში დაგვეხმარება.

3. პერსონალური მონაცემების დაცვა ინტერნეტ სივრცეში

წინა თავებში დეტალურად განვიხილეთ პერსონალური მონაცემების ძირითადი ასპექტები, განსაკუთრებული კატეგორიები, ჩვეულებრივი და ,,დიდი მონაცემები''. ასევე განვიხილეთ ის საკითხები, რაც პერსონალური მონაცემების ინტერნეტ სივრცეში გამჟღავნებას და ხელმისაწვდომობას ეხება. შევეხეთ ისეთ სენსიტიურ საკითხებს, როგორებიცაა პირადი ცხოვრების ამსახველი ვიდეომასალებისა თუ აუდიოჩანაწერების ინტერნეტ სივრცეში გავრცელება. განვიხილეთ ინტერნეტთაღლითობის ახალი ფორმა - ფიშინგი, რომელიც სულ რამოდენიმე თვეა რაც გავრცელდა საქართველოში.

ახლა დროა ინტერნეტმომხმარებლებს, და ზოგადად მოსახლეობას მივაწოდოთ ინფორმაცია იმის შესახებ, თუ როგორ დავიცვათ ჩვენი უფლებები ინტერნეტ სივრცეში და რომელია ის მნიშვნელოვანი გარემოებები, რომლებიც აუცილებლად უნდა გავითვალისწინოთ სოციალურ ქსელსა თუ ზოგადად, ინტერნეტში პერსონალური მონაცემების შემცველი ინფორმაციის გამოყენებისას.

ადამიანები განსხვავდებიან ინტერესების, შეხედულებების, გემოვნების, აზროვნების მიხედვით, თუმცა ყველა მათგანს აერთიანებს თანაბარი უფლებები და ამ უფლებების დაცვა მათი განსხვავებულობიდან გამომდინარე. კანონის წინაშე ყველა თანასწორია და აკრძალულია რაიმე სახის დისკრიმინაცია ,,რასის, კანის ფერის, ენის, სქესის, ასაკის, მოქალაქეობის, წარმოშობის, დაბადების ადგილის, საცხოვრებელი ადგილის, ქონებრივი ან წოდებრივი მდგომარეობის, რელიგიის ან რწმენის, ეროვნული ან სოციალური კუთვნილების, პროფესიის, ოჯახური მდგომარეობის, შეზღუდული შესაძლებლობის, სექსუალური ორიენტაციის, გენდერული იდენტობისა და გამოხატვის, პოლიტიკური ან სხვა შეხედულებების ან სხვა ნიშნის მიუხედავად.'' ნებისმიერ ფიზიკურ პირს აქვს შესაძლებლობა საქართველოს კანონმდებლობით დადგენილი უფლებებით ისარგებლოს თანასწორად, ამიტომ მნიშვნელოვანია ყველა ჩვენგანმა იცოდეს, თუ როგორ დაიცვას დარღვეული უფლებები, განსაკუთრებით კი ინტერნეტ სივრცეში.

უპირველეს ყოვლისა, როგორც ნაშრომის წინა თავებში აღვნიშნეთ, თითოეულ ჩვენს მიერ განხორციელებულ ქმედებას მოსდევს შედეგი. შედეგი, რომელიც ხშირად არასასიამოვნო და არასასურველია ჩვენთვის. ალბათ არც ვუფიქრდებით იმას, რომ ჩვენს პერსონალურ მონაცემებს ჩვენთვითონვე ვუქმნით საფრთხეს და ვასაჯაროებთ უამრავი ცნობისმოყვარე თვალისთვის. ამიტომ სანამ არასასურველი რეალობის წინაშე აღმოვჩნდებით, ჩვენ თვითონვე უნდა დავფიქრდეთ იმაზე, თუ რა შედეგი

შეიძლება მოჰყვეს ინტერნეტ სივრცეში განხორციელებულ ნებისმიერ ქმედებას. მნიშვნელოვანია გვახსოვდეს, რომ ინტერნეტში არაინფორმირებულმა და გაუაზრებელმა ქმედებამ შესაძლოა საფრთხე შეუქმნას პირადი ცხოვრების ხელშეუხებლობას. არ უნდა დავივიწყოთ ისიც, რომ ჩვენი უფლებების დამცველნი, პირველ რიგში, ისევ და ისევ ჩვენ ვართ.

ინტერნეტ სივრცეში ნებისმიერი სახის მოქმედების განხორციელებისას აუცილებელია მომხმარებელი დაინტერესდეს შემდეგი ინფორმაციით:

- ვინ ამუშავებს (აგროვებს, ინახავს, ცვლის და ა.შ.) მის შესახებ მონაცემებს?
- რამდენად აუცილებელია კონკრეტული მონაცემის მიწოდება?
- როგორ მოხდება ამ მონაცემის გამოყენება და რა შედეგი მოჰყვება მას?

განსაკუთრებული სიფრთხილეა საჭირო, როდესაც მომხმარებლებისგან ითხოვენ საბანკო ანგარიშებისა თუ საკრედიტო ბარათების შესახებ ინფორმაციას. ჩვენივე მონაცემების დასაცავად, ინტერნეტ შესყიდვების განხორციელებამდე აუცილებელია წინასწარ მოვიძიოთ ინფორმაცია ვებგვერდის და რეალიზატორის შესახებ. ასევე აუცილებელია, რომ გამოვიყენოთ სანდო ვებგვერდი. ვებგვერდის სანდოობაზე კი ნაშრომის წინა თავში ვისაუბრეთ. ამგვარი წინდახედული ქმედებები დაგვეხმარება დავიცვათ ჩვენი, როგორც პერსონალური, ისე ფინანსური მონაცემები ინტერნეტთაღლითებისგან.

ის, რომ მსოფლიო მოსახლეობის უმრავლესობა სარგებლობს სოციალური ქსელით, ახალი ამბავი არავისთვისაა. ჩემს მიერ ჩატარებულმა გამოკითხვამაც დაადასტურა, რომ 54 გამოკითხული ადამიანიდან მხოლოდ 2 არ არის სოციალური ქსელის მომხმარებელი. პერსონალური მონაცემები კი ყველაზე დაუცველი სწორედ აქაა, რადგან უამრავი ჩვენი მონაცემი იყრის თავს. მაგ. ფოტო, სახელი, გვარი, ტელეფონის ნომერი, ელ.ფოსტის მისამართი; პირადი ინფორმაციაც კი, როგორიცაა ოჯახური მდგომარეობა, სამუშაო თუ საცხოვებელი ადგილი და ა.შ. ნებისმიერი სახის სოციალურ ქსელში მომხმარებელი კარგავს კონტროლს მის მიერ გაზიარებულ ონფორმაციაზე, რაც საფრთხეს უქმნის პერსონალური მონაცემების კონფიდენციალურობასა და პირად ცხოვრებას. ამიტომ სანამ ასეთი დიდი მოცულობით მონაცემებზე წვდომის უფლებას მივცემთ მესამე პირებს, აუცილებელია ვაკონტროლოთ მონაცემების გასაჯაროების ფარგლები. არსებობს ინფორმაციაზე წვდომის სამი ძირითადი სახე:

1. პირადი - მონაცემების მესაკუთრის გარდა არავის აქვს მათი ნახვის უფლება

2. საზიარო - მომხმარებელს შეუძლია გაუზიაროს განთავსებული ინფორმაცია სასურველ პირებს
3. საჯარო - განთავსებული ინფორმაციის ნახვა შეუძლია ნებისმიერ მსურველს.

აქედან გამომდინარე, მომხმარებლებმა აუცილებლად უნდა განსაზღვრონ ის, თუ ვის შეიძლება ჰქონდეს წვდომა მათ მიერ გამოქვეყნებულ ამა თუ იმ ინფორმაციაზე და თუ საჭიროა, ზოგიერთი ცხოვრებისეული მოვლენა იქნება ეს თუ უბრალოდ პერსონალური მონაცემი, აუცილებლად უნდა დამალონ მესამე პირებისგან.

სოციალურ ქსელებში ხელმისაწვდომი ინფორმაციით ხშირად სარგებლობენ თაღლითები. ამიტომ ინტერნეტთაღლითობის მსხვერპლი რომ არ გავხდეთ, ჯობია თავიდანვე ვაკონტროლოთ მონაცემების გასაჯაროების ფარგლები და თავი შევიკავოთ ისეთი ინფორმაციის განთავსებისგან, როგორიცაა მაგ. პირადი ნომერი, პასპორტის მონაცემები და ა.შ.

ინტერნეტმომხმარებელს უფლება აქვს ინტერნეტ მომსახურების გამწევისგან მიიღოს ინფორმაცია მისი მონაცემების დამუშავების შესახებ. მაგ:

- რა სახის მონაცემი მუშავდება მის შესახებ, რა არის მათი დამუშავების მიზანი და სამართლებრივი საფუძველი;
- მონაცემთა შეგროვების წყარო;
- ხდება თუ არა მონაცემთა მესამე პირებზე გადაცემა და რა მიზნით.

იმ შემთხვევაში თუ მომხმარებელი აღმოაჩენს უზუსტობას მონაცემებში, ან ჩათვლის რომ არასწორად ხდება მისი რომელიმე მონაცემის დამუშავება, ან ამ მონაცემების გამოყენების მიზანი აღარ არსებობს, მას აქვს უფლება მოითხოვოს მისი პერსონალური მონაცემების წაშლა. ინტერნეტ მომსახურების გამწევი კი, თავის მხრივ, ვალდებულია დაუყოვნებლივ შეასრულოს აღნიშნული მოთხოვნა.

მაგ. მომხმარებელმა გააუქმა საკუთარი ანკეტა ინტერნეტ შესყიდვებისთვის განკუთვნილ ვებგვერდზე. გვერდის ადმინისტრატორს უფლება აღარ აქვს დაამუშაოს მონაცემები მომხმარებლის მიერ განხორციელებული შესყიდვებისა და ტრანზაქციების შესახებ.

თუ ინტერნეტმომხმარებელი აღმოაჩენს, რომ მის შესახებ მუშავდება მცდარი, მოძველებული ან არაზუსტი ინფორმაცია, მას აქვს უფლება მოითხოვოს ამ მონაცემების გასწორება, განახლება, დამატება, წაშლა ან განადგურება.

განსაკუთრებულ ყურადღებას მოითხოვს არასრულწლოვანთა მიერ ინტერნეტის გამოყენების საკითხი. თანამედროვე რეალობაში ბავშვები უფრო მეტად იყენებენ ონლაინ რესურსებს, ვიდრე მათი მშობლები. თუმცა, ხშირად, ისინი სათანადოდ ვერ აფასებენ მონაცემთა გამჟღავნებასთან და თაღლითურ სქემებთან დაკავშირებულ საფრთხეებს. ინტერნეტში არსებობს საკმაოდ ბევრი, სხვადასხვა ტიპის თაღლითური ვებგვერდი. თაღლითური სქემების ნაწილია ასევე ე.წ. საეჭვო ელექტრონული წერილები (Spam E-mail), რომლებიც, როგორც აღვნიშნეთ, ელ.ფოსტის მისამართების შემთხვევითი შერჩევის გზით მილიონობით ადრესატს ეგზავნება. მსგავსი სახის წერილები ხშირად ვირუსული ხასიათისაა ან/და იძლევა ინტენეტმომხმარებლის მონაცემების არამართლზომიერად მოპოვების საშუალებას. ისინი შესაძლებელია საფრთხეს უქმნიდეს კომპიუტერს ან სხვა მოწყობილობას, ან/და მასში დაცულ დოკუმენტებს, საბანკო მონაცემებს, პაროლებს და სხვა. საკმაოდ გავრცელებულია ასევე თაღლითების მიერ დაზარალებულების საიდენტიფიკაციო ნომრისა და დაბადების თარიღის გამოყენებით ახალი საკრედიტო ანგარიშების გახსნა და ბარათის გამოყენება, ასევე, ტელეფონის, ინტერნეტისა და სხვა კომუნალური მომსახურებების გადასახადის გაფორმება დაზარალებულის სახელზე ან დავალიანების დაფარვა დაზარალებულის ანგარიშიდან.

პერსონალური მონაცემების დაცვის მიზნით, აუცილებელია, რომ მშობლებმა თვალყური ადევნონ შვილების ქცევას ონლაინ სივრცეში. ასევე აუცილებელია, ბავშვებს განვუმარტოთ, რომ არ განათავსონ ინტერნეტში ისეთი მონაცემები, როგორიცაა ტელეფონის ნომერი, პაროლი, დაბადების თარიღი და სხვა, არ გახსნან ისეთი ელექტრონული წერილები და ბმულები, რომლებიც უცხო პირებისგან/კომპანიებისგან არიან გამოგზავნილი, რადგან ისინი შეიძლება შეიცავდნენ ვირუსს.

ინტერნეტის უკიდეგანო შესაძლებლობები, სპეციალური პროგრამების გამოყენებით, საშუალებას გვაძლევს ვაკონტროლოთ ბავშვების აქტივობები ინტერნეტში და ასევე თუ საჭირო გახდა, შევუზღუდოთ მათ გარკვეულ ვებგვერდებზე წვდომის უფლება.

არის შემთხვევები, როდესაც პერსონალური მონაცემების დაცვა ჩვენს შესაძლებლობებს აღემატება. მაგ. როცა საქმე ეხება ინტერნეტსივრცეში გავრცელებულ ვიდეო-აუდიო ჩანაწერებს. ამ შემთხვევაში ერთადერთი გამოსავალი გასაჩივრებაა. ,,პერსონალურ მონაცემთა დაცვის შესახებ'' საქართველოს კანონით დადგენილი წესით მომხმარებლებს უფლება აქვთ მიმართონ პერსონალურ მონაცემთა დაცვის ინსპექტორს ან სასამართლოს.

როგორც აღვნიშნეთ, ადამიანის პირად ცხოვრებაში ჩარევის ფორმის, მასშტაბისა და სენსიტიურობიდან გამომდინარე დაუშვებელია ნებისმიერი სახის ვიდეომასალისა თუ აუდიოჩანაწერის ინტერნეტ სივრცეში გამოქვეყნება. განსაკუთრებით ბოლო პერიოდში მიიღო მასშტაბური ხასიათი ამგვარი ვიდეოკადრების გავრცელებამ, რაც ჩემი აზრით მეტნაკლებად სახელმწიფოს ბრალიცაა. პირველივე გავრცელებულ ვიდეომასალას არ მოჰყოლია სწრაფი რეაგირება შესაბამისი ორგანოების მხრიდან. რეაგირებაში ვგულისხმობ იმ ღონისძიებებს, რაც შეიძლება გატარებულიყო საზოგადოებრივი ცნობიერების ამაღლების მიზნით. უფრო ზუსტად კი იმ მიზნით, რომ საზოგადოება ყოფილიყო მეტად ინფორმირებული იმასთან დაკავშირებით, თუ რამდენად მძიმე დანაშაულია სხვისი პირადი ცხოვრების ამსახველი ვიდეოკადრების გავრცელება, რა შედეგი შეიძლება მოჰყვეს ამ ყველაფერს და ბოლოს, როგორია დამნაშავის ბედი, ანუ რა სამართლებრივი პასუხისმგებლობა ეკისრება მას. აქვე ვიტყვი იმას, რომ კანონიც არ არის სრულყოფილი ამ კუთხით. სისხლის სამართლის კოდექსი არაფერს ამბობს იმის შესახებ, თუ რა ელის დამნაშავეს, რომელიც ავრცელებს ვიდეომასალას არასრულწლოვნის მონაწილეობით, ან აშანტაჟებს მას ამგვარი ვიდეოს გავრცელებით. აუცილებელია ცვლილებების შეტანა კანონში, რადგან როცა საქმე არასრულწლოვანს ეხება, პირს, რომელიც ბოლომდე არ არის ჩამოყალიბებული, როგორც ფიზიკურად ისე ფსიქიკურად, ამ შემთხვევაში სასჯელი ცოტა მკაცრი უნდა იყოს. თუ პრეტენზია გვაქვს ნებისმიერი სახის დანაშაულის პრევენციაზე, აუცილებელია, რომ ვიზრუნოთ მის აღმოფხვრაზე პირველივე შემთხვევისთანავე, ისეთი საშუალებებით, როგორიცაა სწრაფი რეაგირება და საზოგადოებრივი ცნობიერების ამაღლება.

ის ფაქტი, რომ ჩემი და ჩემი ოჯახის წევრების პერსონალური მონაცემები არ არის სათანადოდ დაცული ინტერნეტ სივრცეში, უსამართლობის განცდას მიქმნის. ცენტრალური საარჩევნო კომისიის ვებგვერდი ვერ უზრუნველყოფს კონფიდენციალურობის სათანადო დაცვას. ჩემი უფლების დასაცავად ამ შემთხვევაშიც გასაჩივრება მიმაჩნია ერთადერთ გზად. თუ ცესკოს მიზანი არჩევნების გამჭვირვალობა და ამომრჩევლებისთვის მეტი კომფორტის შექმნაა, ჩემთვის მთავარი ჩემი და ჩემი ოჯახის წევრების პერსონალური მონაცემების დაცვაა მესამე პირებისგან. ამიტომ მომავალში ვგეგმავ, მივმართო პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატს იმ მოტივით, რომ ცესკოს მიზანი მიღწეულია, მონაცემები კი ისევ ხელმისაწვდომი და დაუცველი.

რამოდენიმეჯერ ვახსენე პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი. მეტი ინფორმაციისთვის მოკლედ დავახასიათებ ამ ორგანოს. სახელმწიფო ინსპექტორის სამსახური დამოუკიდებელი სახელმწიფო ორგანოა, რომელიც როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამონაცვლე, საქართველოში 2019 წლის 10 მაისიდან ამოქმედდა. მისი საქმიანობის ძირითადი მიმართულებებია:

- პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი;
- ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი;
- სამართალდამცავი ორგანოს წარმომადგენლის, მოხელის ან მასთან გათანაბრებული პირის მიერ ადამიანის უფლებებისა და თავისუფლებების წინააღმდეგ ჩადენილი განსაკუთრებით მძიმე დანაშაულის და ძალადობის ან დაზარალებულის ღირსების შეურაცხყოფით ჩადენილი სამოხელეო დანაშაულის მიუკერძოებელი და ეფექტიანი გამოძიება.

პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი მონაცემთა დამუშავების კანონიერების კონტროლს 2013 წლიდან, ფარულ საგამოძიებო მოქმედებებზე კონტროლს კი 2015 წლიდან ახორციელებს. სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ძირითადი პრინციპებია:

- კანონიერება;
- ადამიანის უფლებათა და თავისუფლებათა დაცვა;
- დამოუკიდებლობა და პოლიტიკური ნეიტრალიტეტი;
- ობიექტურობა და მიუკერძოებლობა;
- პროფესიონალიზმი;
- საიდუმლოებისა და კონფიდენციალურობის დაცვა.

პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი ,,ახალი'' სახელმწიფო ორგანოა, რომელიც სულ რამოდენიმე წელია, რაც შეიქმნა და მოქალაქეებს ეხმარება დარღვეული უფლებების დაცვაში. როგორც ზემოთ აღვნიშნეთ, სახელმწიფო ინსპექტორის სამსახურის ერთ-ერთი ძირითადი ფუნქცია პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი და მათი დაცვაა. ინსპექტორის სამსახური ამ საქმიანობას ოთხი ძირითადი მიმართულებით ახორციელებს:

- საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების შემოწმება;
- მონაცემთა დაცვასთან დაკავშირებით მოქალაქეთა განცხადებების განხილვა;

- საჯარო და კერძო დაწესებულებებისათვის, აგრეთვე ფიზიკური პირებისთვის მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციის გაწევა;
- საქართველოში მონაცემთა დაცვის მდგომარეობისა და მასთან დაკავშირებული მნიშვნელოვანი მოვლენების შესახებ საზოგადოების ინფორმირება.

აღსანიშნავია ის ფაქტი, რომ სახელმწიფოში გვაქვს ისეთი ორგანო, რომელიც პერსონალურ მონაცემთა დაცვის კუთხით მუშაობს და მნიშვნელოვან საკითხებს აგვარებს. გარდა ამისა, სახელმწიფო ინსპექტორის სამსახური რეკომენდაციების სახით ცდილობს უფრო მეტად აამაღლოს საზოგადოებრივი ცნობიერება და მიაწვდინოს მოქალაქეებს ინფორმაცია იმის შესახებ, თუ როგორი მნიშვნელოვანია ჩვენი პერსონალური მონაცემები და რა საფრთხეები ემუქრება მათ არამიზნობრივ/არასამართლიან გამოყენებას. ჩემი მიზანიც თითქმის იგივე იყო, მაგრამ უფრო კონკრეტულ და ვიწრო საკითხზე. ჩატარებულმა გამოკითხვამ დამანახვა, რომ გამოკითხულთა უმრავლესობამ არ იცის ცნება ,,პერსონალური მონაცემი'' რას მოიცავს და რა საფრთხეები ემუქრება ამ მონაცემების ინტერნეტ სივრცეში გასაჯაროებას/ხელმისაწვდომობას. ამიტომ საჭიროდ ჩავთვალე, ჯერ ამომეწურა საკითხი პერსონალური მონაცემების შესახებ, შემდეგ დამენახვებინა, ის, თუ რა ხდება ინტერნეტ სამყაროში და ბოლოს რეკომენდაციების სახით ჩამომეყალიბებინა ის მნიშვნელოვანი გარემოებები, რომლებიც აუცილებლად უნდა გაითვალისწინონ ინტერნეტ მომხმარებლებმა ნებისმიერი ქმედების ინტერნეტ სივრცეში განხორციელებისას.

დასკვნა

წარმოდგენილი ნაშრომი რომ შევაჯამოთ, ვიტყვი, რომ ცნება ,,პერსონალური მონაცემი'' საკმაოდ ვრცელი კატეგორიაა და იმაზე მეტი ელემენტისგან შედგება, ვიდრე წარმომედგინა. კვლევის პროცესში აღმოვაჩინე უამრავი ისეთი მონაცემი, რომელიც ვერც კი დავუშვი, რომ შეიძლებოდა პერსონალური მონაცემი ყოფილიყო. მაგ: კომუნიკაცია. კომუნიკაციის დაცულობა თანამედროვე ტექნოლოგიების ეპოქაში ერთ-ერთი მთავარი გამოწვევაა, თუმცა ბევრმა შეიძლება არც იცოდეს, რომ დაცვა სჭირდება არამარტო კომუნიკაციის შინაარსს, არამედ მისი მონაწილეების მაიდენტიფიცირებელ მონაცემებსაც. კომუნიკაციის განმახორციელებელი კომპანიები ფლობენ ისეთ მონაცემებს, როგორიცაა ტელეფონის ნომერი, მომხმარებლის სახელი და მისამართი, ინტერნეტპროტოკოლის (IP) მისამართი, კომუნიკაციის თარიღი, დრო და ხანგრძლივობა, გამოყენებული ინტერნეტ და

სატელეფონო სერვისები და სხვა. კომუნიკაციის განმახორციელებელი კომპანია ვალდებულია დაიცვას ამ მონაცემების კონფიდენციალურობა. გარდა კომუნიკაციისა, პერსონალური მონაცემების კატეგორიას განეკუთვნება: ჭორი, ჟესტიკულაცია, უნარები, ყოფაქცევა, სასამართლოში მოწმის, ბრალდებულის ან დაზარალებულის მიერ მიცემული ჩვენება და ა.შ. თითოეული მონაცემი ერთად აღებული ქმნის ჩვენს ციფრულ პორტრეტს, ინფორმაციის უზარმაზარ ერთობლიობას ანუ ,,დიდ მონაცემებს'', რომელთა დაცვაც საკამოდ რთულია ინტერნეტ სივრცეში. სივრცეში, სადაც თითოეული მოქმედების განხორციელების სანაცვლოდ ჩვენს პერსონალურ მონაცემებს ,,გავცემთ''. ნაშრომში ასევე ვისაუბრეთ იმ საფრთხეებზე, როგორებიცაა ინტერნეტ თაღლითობა, პირადი ცხოვრების ხელშეუხებლობის ხელყოფა, სხვისი პირადი ინტერესებისათვის ჩვენი მონაცემების დამუშავება (მაგ; პირდაპირი მარკეტინგისთვის) და სხვა. აქვე აღვნიშნავ იმასაც, რომ დასახვეწია სარეკლამო შეტყობინებებზე უარის თქმის მექანიზმები. აუცილებელია, რომ თითოეულ ინტერნეტ მომხმარებელს ჰქონდეს შესაძლებლობა, სამუდამოდ დაემშვიდობოს რეკლამებს, რომლებიც ხშირად ,,გვაბეზრებს'' თავს და დიდ დისკომფორტს გვქმნის. განვიხილე სახელმწიფო ინსპექტორის სამსახურის აპარატი, რომელიც სულ რამოდენიმე წელია დგას ჩვენი მონაცემების დაცვის სადარაჯოზე და იმედი მაქვს, რომ მომავალში უფრო მეტი შესაძლებლობა ექნება, რათა უფრო ეფექტურად დაიცვას ჩვენი დარღვეული უფლებები. პირველ რიგში კი მე თვითონ დამეხმარება იმაში, რომ დავიცვა ცენტრალური საარჩევნო კომისიის მიერ გამოქვეყნებული, საჯაროდ ხელმისაწვდომი, ჩემი და ჩემი ოჯახის წევრების პერსონალური მონაცემები. ასევე დიდი იმედი მაქვს იმის, რომ ჩემს მიერ წარმოდგენილი ნაშრომიც მნიშვნელოვან წვლილს შეიტანს საზოგადოებრივი ცნობიერების ამაღლების კუთხით.

ბიბლიოგრაფია:

1. ბიჭია მ. 2017 წლის 7 ივლისი, ,,პერსონალური მონაცემებისს კერძოსამართლებრივი დაცვის პრობლემა ინტერნეტსამყაროში, 2019 წლის 25 მარტი, http://inso.ge/inso2017/wp-content/uploads/2017/07/7-personaluri-monacemebis-dacva-internetshi.pdf
2. გოშაძე კ. 2014 წლის 28 მაისი, ჟურნალი ,,ლიბერალი'', ,,პერსონალურ მონაცემთა დაცვა: ახალი გამოწვევა'', 2019 წლის 20 მარტი, http://liberali.ge/blogs/view/5894/personalur-monatsemta-datsva-akhali-gamotsveva
3. გოშაძე კ. (2015), მონაცემთა დაცვის ევროპული სამართალი, თბილისი: ,,იურისტების სამყარო''
4. დირექტივა, (1995), 95/46/EC ,,პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ''
5. კონვენცია, (1985), ,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ''
6. მთივლიშვილი ო., ჯავახიშვილი დ., (2017), პერსონალური მონაცემების დაცვის საკითხების სამართლებრივი მოწესრიგება და ადმინისტრაციულ ორგანოთა ვალდებულება, (,,საქართველოს იურიდიული ფირმებს ასოციაციის ჟურნალი'', N4, თბილისი: ,,შპს ბიარტი'', 42-55 გვ.)
7. მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Linqvist, 6 ნოემბერი 2003 წელი, პარაგ. 51.
8. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2014 წლის 1 მარტი, ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში''
9. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2014 წელი, ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში''
10. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2015 წელი, ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ''
11. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2016 წელი, ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ''
12. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2017 წელი, ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ''

13. რეგულაცია, (2016), (EU) 2016/679 ,,პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ'', ევროკავშირის მონაცემთა დაცვის რეგულაცია (GDPR)
14. საქართველის კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ''
15. საქართველოს სისხლის სამართლის კოდექსი
16. საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2010 წლის 5 ივლისის №ბს-1278-1240(კ-08) განჩინება
17. კითხვარი, (2019), ,,პერსონალურ მონაცემთა დაცვის შესახებ'', გორი, https://docs.google.com/forms/d/e/1FAIpQLSe61c3PqOhaXvIMlweGtpwdq9MiqLuJ4-YIMDKqcbEZUr8Fhg/viewform?fbclid=IwAR04C7I-JT0B1UixJ4KAp51N007byNnZkMSff2PCIVFhhRXFkY3hvgDAruY

დანართები:

დანართი N1:

კითხვარი

პერსონალურ მონაცემთა დაცვის შესახებ

1. გსმენიათ თუ არა პერსონალური მონაცემების შესახებ?
    - კი
    - არა

2. პერსონალურ მონაცემებს განეკუთვნება:
    - სახელი, გვარი, დაბადების თარიღი, პირადი ნომერი
    - საბანკო ანგარიში, ანაბეჭდი, წარმომავლობა
    - ლოკაცია, ღეროვანი უჯრედი, ხმის ჩანაწერი
    - ყველა ზემოთ ჩამოთვლილი

3. გსმენიათ რაიმე ტერმინის ,,Big Data" - ანუ დიდი მონაცემების შესახებ?
    - კი
    - არა

4. თქვენი აზრით, რამდენად არის დაცული თქვენი პერსონალური მონაცემები ინტერნეტ სივრცეში?
    - სრულიად დაცულია
    - ნაწილობრივ დაცულია
    - არ არის დაცული

5. თქვენი აზრით, შეუძლია თუ არა უცხო პირს ინტერნეტის საშუალებით მოიძიოს ინფორმაცია თქვენი ან თქვენი ოჯახის წევრების შესახებ?
    - არ შეუძლია
    - შეუძლია

6. დასაშვებია თუ არა ნებისმიერი სახის ვიდეომასალისა თუ აუდიოჩანაწერის ინტერნეტ სივრცეში გამოქვეყნება?
    - დასაშვებია
    - გააჩნია ვიდეომასალას/აუდიოჩანაწერს
    - არ არის დასაშვები

7. ხართ თუ არა რომელიმე სოციალური ქსელის (მაგ. Facebook, Twitter, Instagram) მომხმარებელი?
    - კი
    - არა

8. იმ შემთხვევაში თუ სოციალური ქსელის მომხმარებელი ხართ, გაწუხებთ თუ არა სარეკლამო შეტყობინებები?
    - კი
    - არა

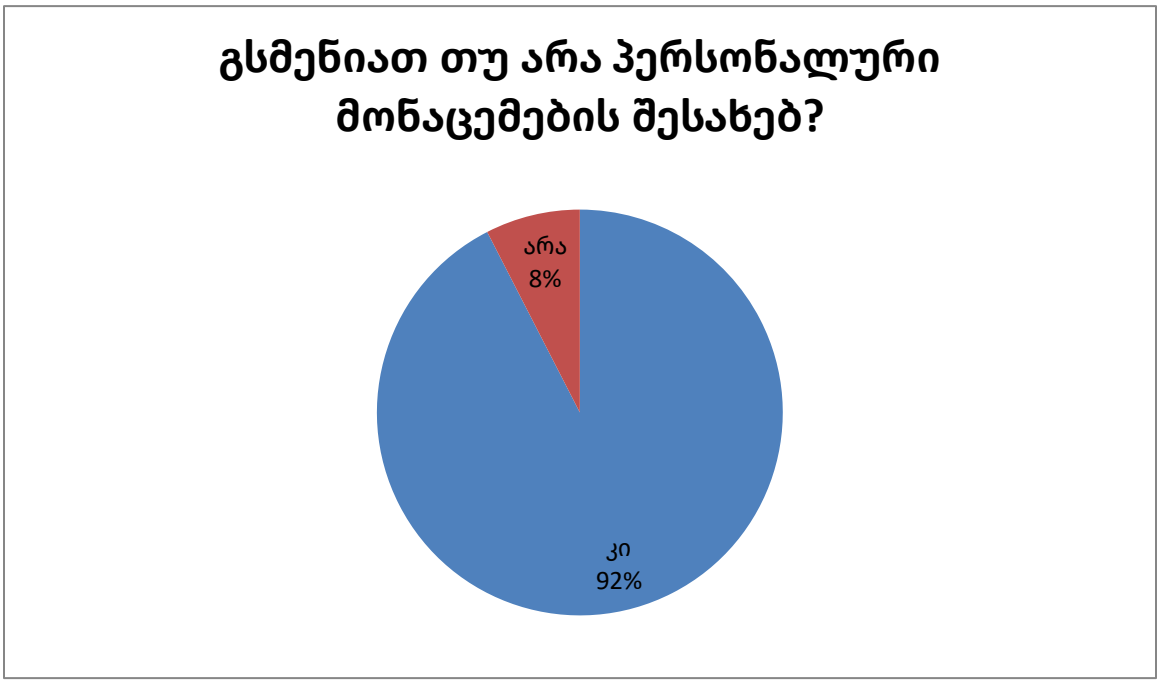
9. ხართ თუ არა ონლაინ შესყიდვების (Online Shopping) მოყვარული?
    - კი
    - არა

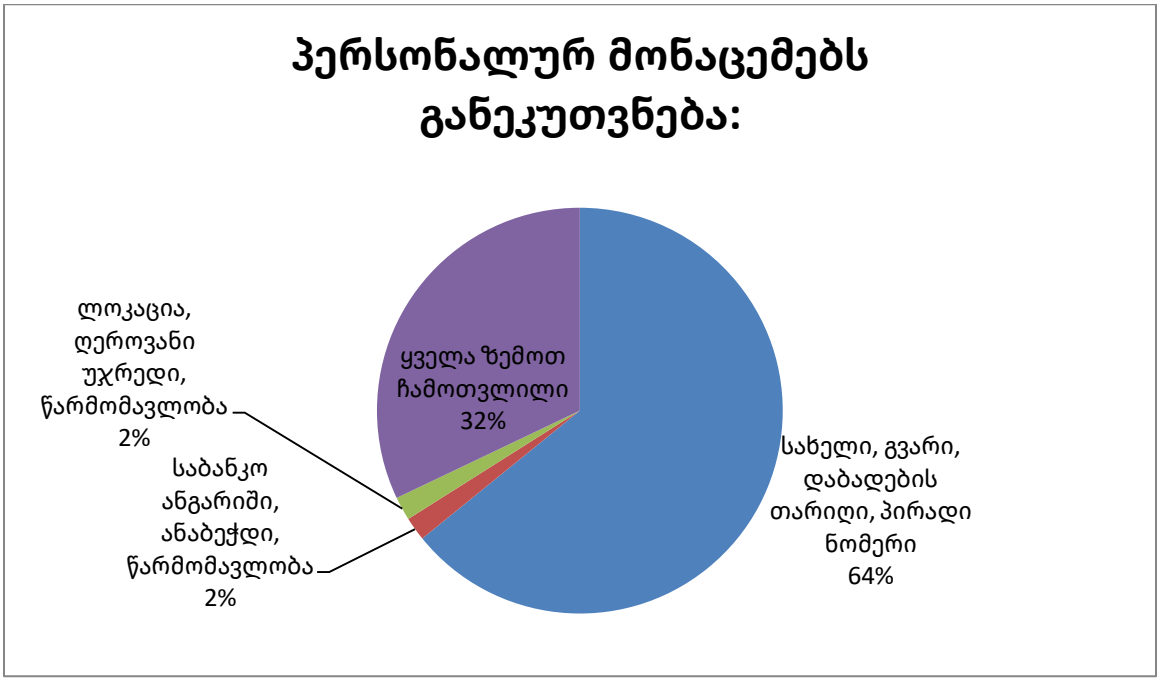
10. გსმენიათ თუ არა რაიმე Phishing - ანუ ,,ფიშინგის" შესახებ?
    - კი
    - არა

11. იცით თუ არა, როგორ დაიცვათ თქვენი პერსონალური მონაცემები ინტერნეტ სივრცეში?
    - კი
    - არა

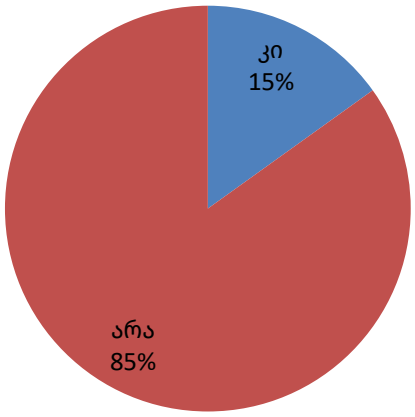
12. გსმენიათ რაიმე პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატზე?
    - კი
    - არა

დანართი N2:

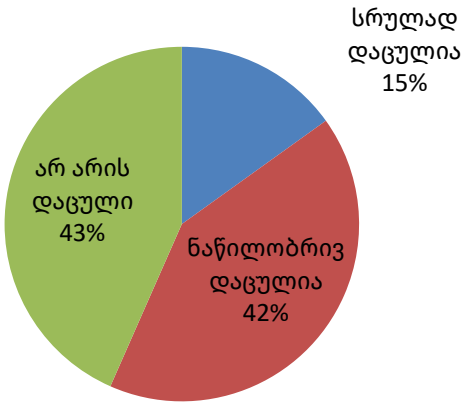

გსმენიათ თუ არა პერსონალური მონაცემების შესახებ?
არა 8%
კი 92%


პერსონალურ მონაცემებს განეკუთვნება:
ლოკაცია, ღეროვანი უჯრედი, წარმომავლობა 2%
საბანკო ანგარიში, ანაბეჭდი, წარმომავლობა 2%
ყველა ზემოთ ჩამოთვლილი 32%
სახელი, გვარი, დაბადების თარიღი, პირადი ნომერი 64%

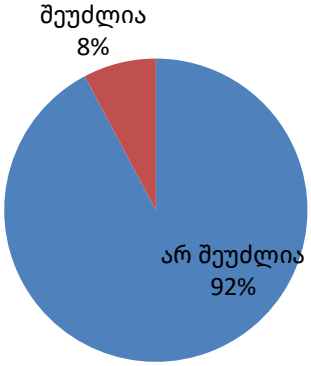
გსმენიათ რაიმე ტერმინის ,,Big Data'' - ანუ დიდი მონაცემების შესახებ?



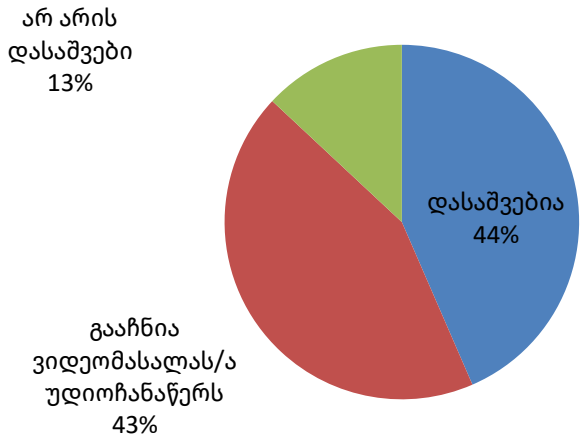
თქვენი აზრით, რამდენად არის დაცული თქვენი პერსონალური მონაცემები ინტერნეტ სივრცეში?



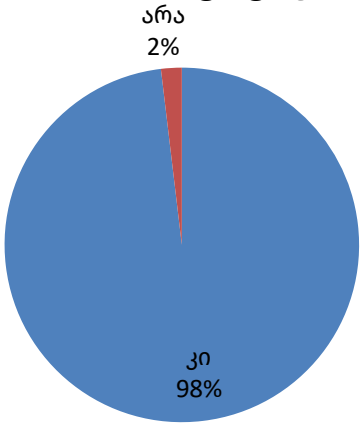
თქვენი აზრით, შეუძლია თუ არა უცხო პირს ინტერნეტის საშუალებით მოიძიოს ინფორმაცია თქვენი ან თქვენი ოჯახის წევრების შესახებ?



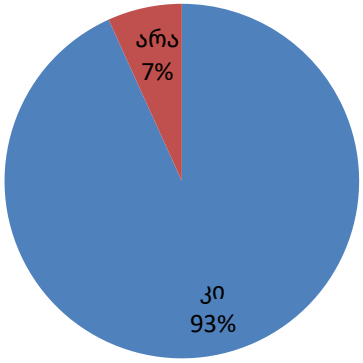
დასაშვებია თუ არა ნებისმიერი სახის ვიდეომასალისა თუ აუდიოჩანაწერის ინტერნეტ სივრცეში გამოქვეყნება?



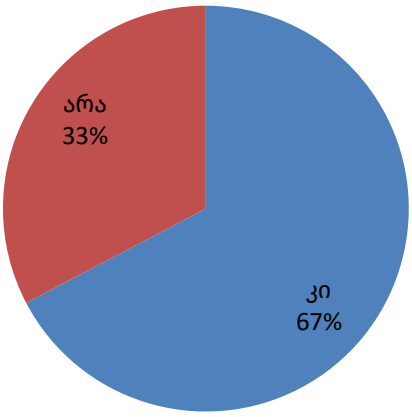
ხართ თუ არა რომელიმე სოციალური ქსელის (მაგ. Facebook, Twitter, Instagram) მომხმარებელი?



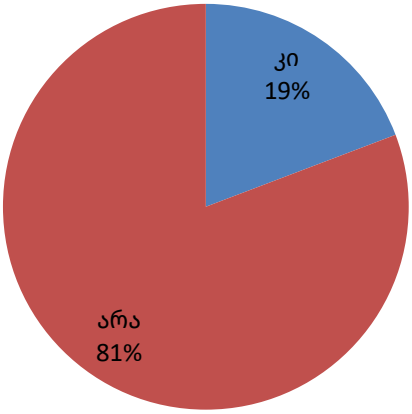
იმ შემთხვევაში თუ სოციალური ქსელის მომხმარებელი ხართ, გაწუხებთ თუ არა სარეკლამო შეტყობინებები?



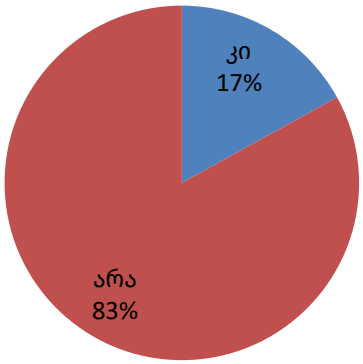
ხართ თუ არა ონლაინ შესყიდვების (Online Shopping) მოყვარული?



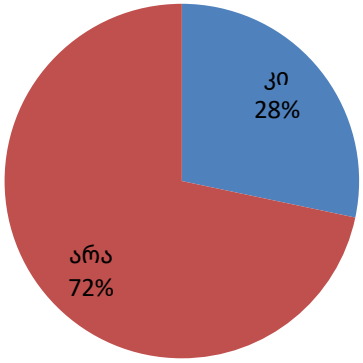
გსმენიათ თუ არა რაიმე Phishing - ანუ ,,ფიშინგის'' შესახებ?



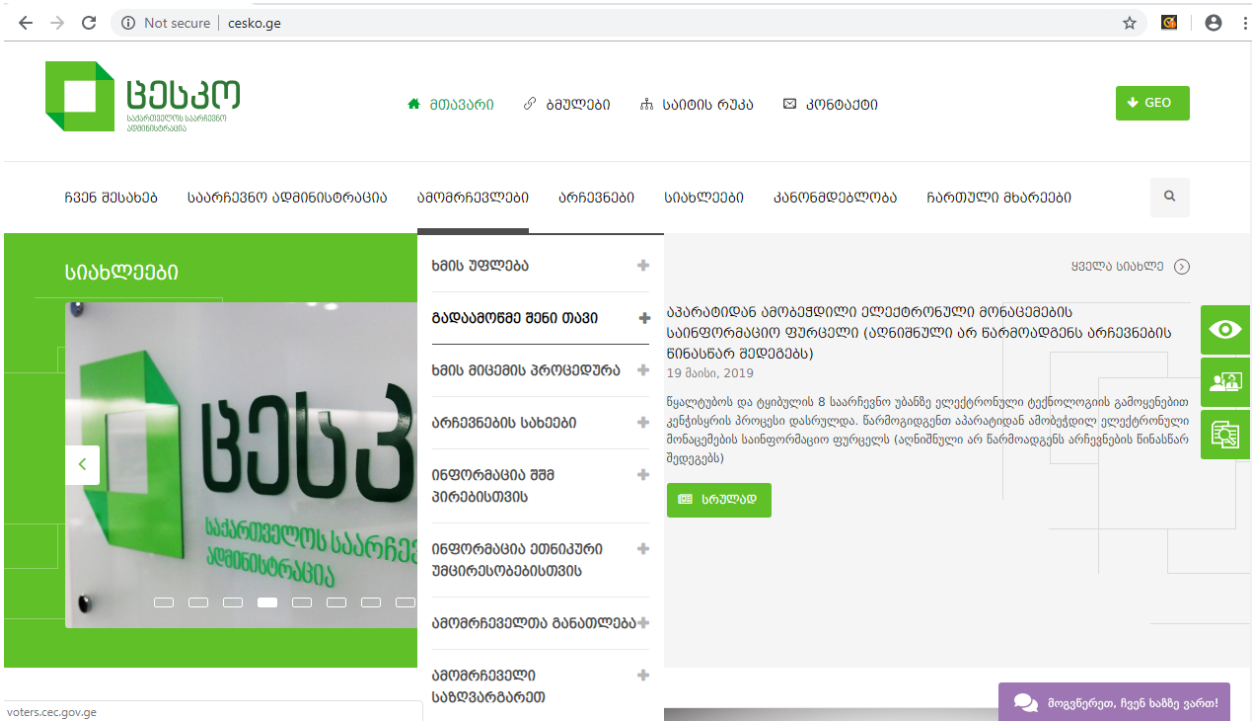
იცით თუ არა, როგორ დაიცვათ თქვენი პერსონალური მონაცემები ინტერნეტ სივრცეში?

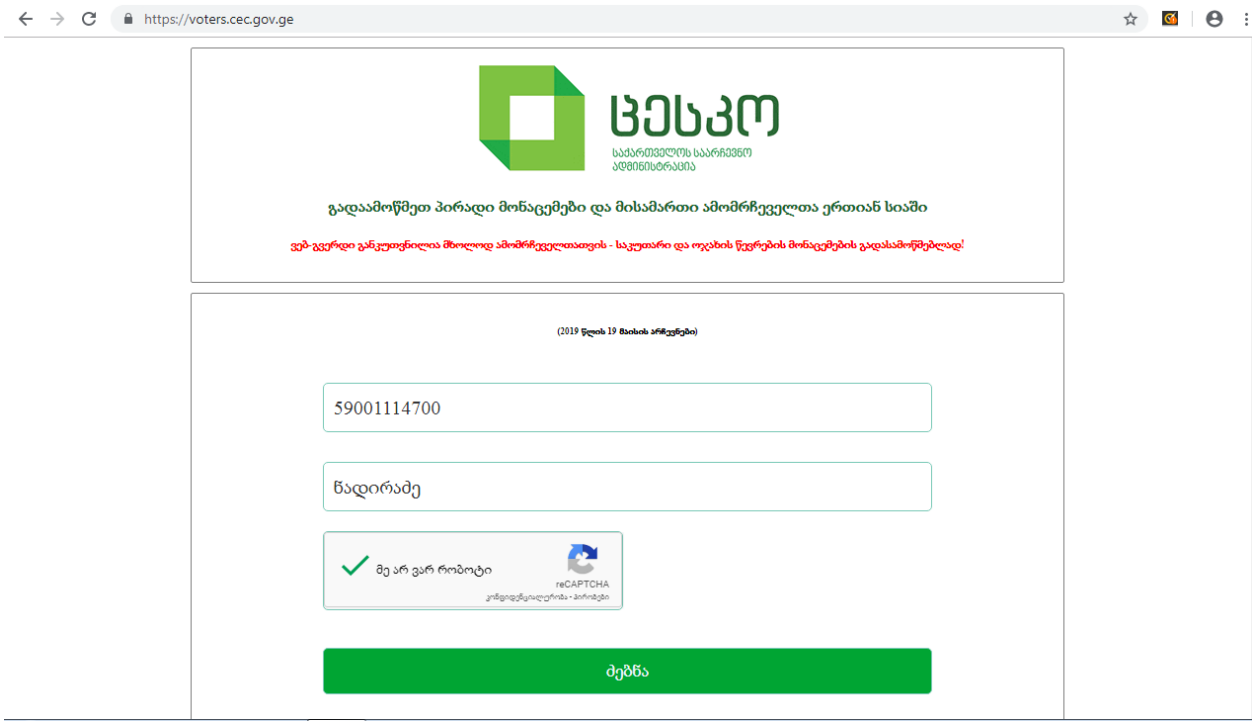


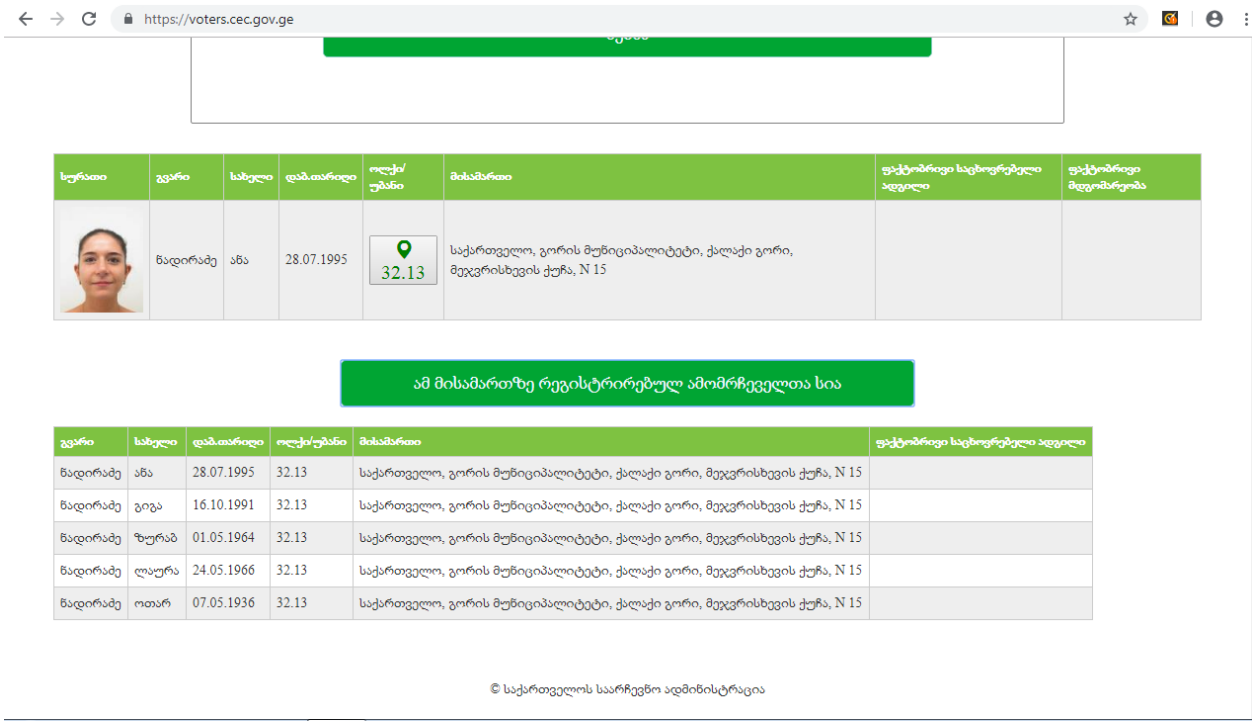
გსმენიათ რაიმე პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატზე?



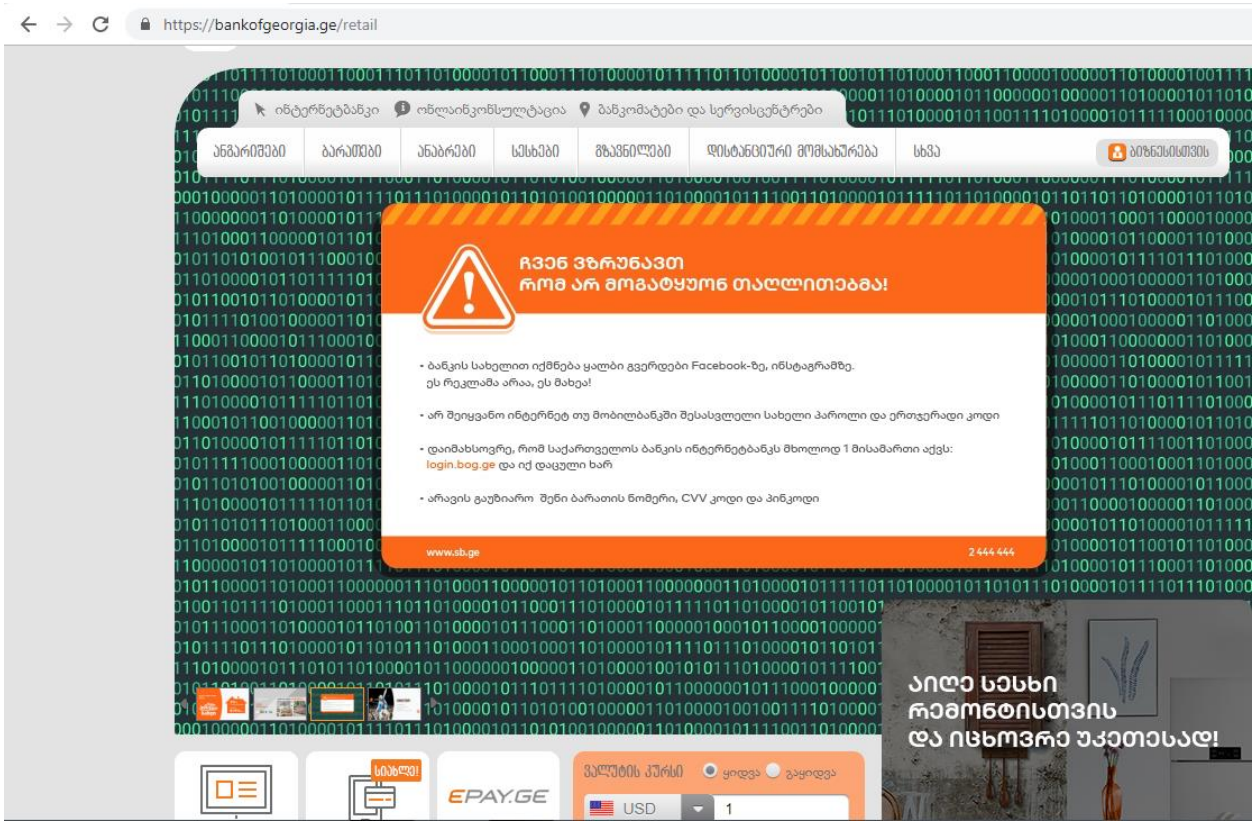
დანართი N3:


Not secure | cesko.ge
ცესკო
საქართველოს საარჩევნო ადმინისტრაცია
მთავარი
ბმულები
საიტის რუკა
კონტაქტი
GEO
ჩვენ შესახებ
საარჩევნო ადმინისტრაცია
ამომრჩევლები
არჩევნები
სიახლეები
კანონმდებლობა
ჩართული მხარეები
სიახლეები
ხმის უფლება
გადაამოწმე შენი თავი
ხმის მიცემის პროცედურა
არჩევნების სახეები
ინფორმაცია მშმ პირებისთვის
ინფორმაცია ეთნიკური უმცირესობებისთვის
ამომრჩეველთა განათლება
ამომრჩეველი საზღვარგარეთ
ყველა სიახლე
აპარატიდან ამობეჭდილი ელექტრონული მონაცემების საინფორმაციო ფურცელი (აღნიშნული არ წარმოადგენს არჩევნების წინასწარ შედეგებს)
19 მაისი, 2019
წყალტუბოს და ტყიბულის 8 საარჩევნო უბანზე ელექტრონული ტექნოლოგიის გამოყენებით კენჭისყრის პროცესი დასრულდა. წარმოგიდგენთ აპარატიდან ამობეჭდილ ელექტრონული მონაცემების საინფორმაციო ფურცელს (აღნიშნული არ წარმოადგენს არჩევნების წინასწარ შედეგებს)
სრულად
მოგვწერეთ, ჩვენ სამზე ვართ!
voters.cec.gov.ge


https://voters.cec.gov.ge
ცესკო
საქართველოს საარჩევნო ადმინისტრაცია
გადაამოწმეთ პირადი მონაცემები და მისამართი ამომრჩეველთა ერთიან სიაში
ვებ-გვერდი განკუთვნილია მხოლოდ ამომრჩეველთათვის - საკუთარი და ოჯახის წევრების მონაცემების გადასამოწმებლად!
(2019 წლის 19 მაისის არჩევნები)
59001114700
წადირაძე
მე არ ვარ რობოტი
reCAPTCHA
ძებნა


https://voters.cec.gov.ge
სურათი
გვარი
სახელი
დაბ.თარიღი
ოლქი/ უბანი
მისამართი
ფაქტობრივი საცხოვრებელი ადგილი
ფაქტობრივი მდგომარეობა
წადირაძე
ანა
28.07.1995
32.13
საქართველო, გორის მუნიციპალიტეტი, ქალაქი გორი, მეუკვრისხევის ქუჩა, N 15
ამ მისამართზე რეგისტრირებულ ამომრჩეველთა სია
გვარი
სახელი
დაბ.თარიღი
ოლქი/უბანი
მისამართი
ფაქტობრივი საცხოვრებელი ადგილი
წადირაძე ანა 28.07.1995 32.13 საქართველო, გორის მუნიციპალიტეტი, ქალაქი გორი, მეუკვრისხევის ქუჩა, N 15
წადირაძე გოგა 16.10.1991 32.13 საქართველო, გორის მუნიციპალიტეტი, ქალაქი გორი, მეუკვრისხევის ქუჩა, N 15
წადირაძე ზურაბ 01.05.1964 32.13 საქართველო, გორის მუნიციპალიტეტი, ქალაქი გორი, მეუკვრისხევის ქუჩა, N 15
წადირაძე ლაურა 24.05.1966 32.13 საქართველო, გორის მუნიციპალიტეტი, ქალაქი გორი, მეუკვრისხევის ქუჩა, N 15
წადირაძე ოთარ 07.05.1936 32.13 საქართველო, გორის მუნიციპალიტეტი, ქალაქი გორი, მეუკვრისხევის ქუჩა, N 15
© საქართველოს საარჩევნო ადმინისტრაცია

დანართი N4:


https://bankofgeorgia.ge/retail
ინტერნეტბანკი
ონლაინკონსულტაცია
ბანკომატები და სერვისცენტრები
ანგარიშები
ბარათები
ანაბრები
სესხები
გზავნილები
დისტანციური მომსახურება
სხვა
ბიზნესისთვის
ჩვენ ვზრუნავთ რომ არ მოგატყუონ თაღლითებმა!
• ბანკის სახელით იქმნება ყალბი გვერდები Facebook-ზე, ინსტაგრამზე. ეს რეკლამა არაა, ეს მახეა!
• არ შეიყვანო ინტერნეტ თუ მობილბანკში შესასვლელი სახელი პაროლი და ერთჯერადი კოდი
• დაიმახსოვრე, რომ საქართველოს ბანკის ინტერნეტბანკს მხოლოდ 1 მისამართი აქვს: login.bog.ge და იქ დაცული ხარ
• არავის გაუზიარო შენი ბარათის ნომერი, CVV კოდი და პინკოდი
www.sb.ge
2 444 444
EPAY.GE
USD
1
აიღე სესხი რემონტისთვის და იცხოვრე უკეთესად!