ინფორმაციის თავისუფლების
განვითარების ინსტიტუტი

რისკები და გამოწვევები „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების კანონპროექტში

ნოემბერი, 2019

შესავალი

„ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ (IDFI) ეხმიანება საქართველოს პარლამენტში 2019 წლის 2 ოქტომბერს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ ინიცირებულ კანონპროექტს.

უპირველეს ყოვლისა ხაზი უნდა გავუსვათ იმ ფაქტს, რომ ინფორმაციული ტექნოლოგიების სწრაფი განვითარება ზრდის ერთი მხრივ საზოგადოების თითოეული წევრის დამოკიდებულებას თანამედროვე ელექტრონულ სისტემებზე, ხოლო მეორე მხრივ აძლიერებს სახელმწიფო სერვისების, სტრუქტურების და უსაფრთხოების სისტემების დამოკიდებულებას მუდმივად განახლებად ციფრულ ტექნოლოგიებზე, რაც ბუნებრივად წარმოშობს როგორც საგარეო, ასევე, საშინაო რისკებს. ასეთი რისკების განსაზღვრა და მათი დაცვის შესაბამისი ღონისძიებების დანერგვა აუცილებელია. თუმცა, გასათვალისწინებელია ის ფაქტი, რომ საქართველო ახალგაზრდა დემოკრატიაა, სადაც არ არის ჩამოყალიბებული კარგი და ანგარიშვალდებული სახელმწიფო მმართველობის სისტემები, შესაბამისად, უსაფრთხოების სექტორის მაკონტროლებელი უფლებამოსილებების პოტენციური, და ამ ეტაპზე დაუსაბუთებელი, ზრდა არ უნდა განხორციელდეს თავისუფლების შეზღუდვის ხარჯზე.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი დაფუძნებული იყო ინფორმაციული უსაფრთხოების სფეროში კერძო და საჯარო სექტორის კოორდინაციის და ურთიერთთანამშრომლობის პრინციპზე. ახალი კანონპროექტის მიზანი ხდება ინფორმაციული უსაფრთხოების სფეროში უფრო მკაცრი რეგულირების დაწესება სახელმწიფო უსაფრთხოების სამსახურის ოპერატიულ-ტექნიკური სააგენტოს კოორდინირებით, მათ შორის არა მხოლოდ საჯარო სექტორს მიკუთვნებული სუბიექტების, არამედ კერძო სამართლის იურიდიული პირების მიმართაც, რაც შეიძლება განვიხილოთ, როგორც კიბერუსაფრთხოების სფეროს კარდინალური რეფორმა.

2019 წლის 2 ოქტომბერს ინიცირებულ კანონპროექტში, IDFI ხედავს რისკებს, რომელიც სხვადასხვა დასაბუთებულ ფაქტორებზე დაყრდნობით შეიძლება შემდეგნაირად ჩამოყალიბდეს:

1. ინფორმაციული უსაფრთხოების სისტემის კარდინალური რეფორმა

დღეს არსებული რეგულირებისა და საქართველოს მთავრობის მიერ დამტკიცებული კიბერ უსაფრთხოების 2016-2018 წლების სტრატეგიის მიხედვით საქართველოში ინფორმაციული და კიბერ-უსაფრთხოების არქიტექტურა განსაზღვრული იყო შემდეგნაირად:

2010 წელს ჩამოყალიბდა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში შემავალი სსიპ - მონაცემთა გაცვლის სააგენტო, რომელსაც დაევალა ქვეყნის კრიტიკული ინფორმაციული სისტემების დაცვა და ინფორმაციული უსაფრთხოების სტანდარტების დანერგვა. სააგენტო ასევე ახორციელებს ერთიანი სამთავრობო ქსელი მონიტორინგს და ინფორმაციული სისტემების აუდიტს. მონაცემთა გაცვლის სააგენტოს დაქვემდებარებაში ფუნქციონირებს კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი, რომელიც საკუთარი კომპეტენციის ფარგლებში პასუხისმგებელია კიბერ ინციდენტების გამოვლენასა და მათ აღკვეთაზე.

2012 წლის დეკემბერში საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელიც ახორციელებს კიბერინციდენტების გამოძიებას მთელი ქვეყნის მასშტაბით. სამმართველო ასევე წარმოადგენს საერთაშორისო საკონტაქტო პუნქტს, რომელიც ასრულებს საერთაშორისო საპოლიციო თანამშრომლობასთან დაკავშირებულ ფუნქციებს „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის შესაბამისად.

თავდაცვის სფეროში კიბერუსაფრთხოების უზრუნველყოფის მიზნით, 2014 წელს შეიქმნა თავდაცვის სამინისტროს სისტემაში შემავალი სსიპ - კიბერუსაფრთხოების ბიურო, რომელიც ახორციელებს საქართველოს სამხედრო ინფრასტრუქტურის წინააღმდეგ მიმართული კიბერინციდენტების აღკვეთასა და პრევენციას. აღნიშნულ ფუნქციათა ეფექტური აღსრულების მიზნით, ბიურო უზრუნველყოფს თავდაცვის სფეროში არსებული ინფრასტრუქტურის შესწავლას, უსაფრთხოების მექანიზმების დანერგვასა და განვითარებას.

საქართველოს პრემიერ-მინისტრის დაქვემდებარებაში 2014 წელს შეიქმნა სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო, რომელიც თავის გაუქმებამდე უზრუნველყოფდა კიბერუსაფრთხოების პოლიტიკის ძირითადი ჩარჩოს შემუშავებას. ამასთან, საბჭო კოორდინაციას უწევდა შესაბამის უწყებებს კიბერ საფრთხეების გამოვლენის პროცესში და ასევე შეიმუშავებდა სათანადო ზომებს. ამასთან, საბჭო მართავდა კიბერუსაფრთხოებასთან დაკავშირებული ეროვნული მასშტაბის ნებისმიერ კრიზისულ სიტუაციას.

სახელმწიფო უსაფრთხოების სამსახური პასუხისმგებელია **ეროვნული უსაფრთხოების** წინააღმდეგ კიბერსივრცეში განხორციელებული აქტივობების გამოვლენაზე, პრევენციასა და აღკვეთაზე. ამასთან, მოქმედი კანონმდებლობით სახელმწიფო უსაფრთხოების სამსახური წარმოადგენს ორგანოს, რომელსაც გაჩნია კიბერსივრცეში ფარული საგამოძიებო საქმიანობის განხორციელების ექსკლუზიური უფლებამოსილება.

კანონპროექტით შემოთავაზებულ ვერსიაში კარდინალურად იცვლება არსებული კიბერ უსაფრთხოების არქიტექტურა. სახელმწიფო უსაფრთხოების სამსახურის სსიპ ოპერატიულ - ტექნიკური სააგენტო ფაქტობრივად ხდება საინფორმაციო და კიბერუსაფრთხოების უზრუნველყოფის მთავარი მაკოორდინირებელი და ზედამხედველი უწყება, რომლის უფლებამოსილება გავრცელდება არა მხოლოდ კრიტიკულ ინფრასტრუქტურას მიკუთვნებულ საჯარო დაწესებულებებზე, არამედ კერძო სექტორზეც. კანონპროექტში არ ჩანს, თუ როგორ მოხდება კოორდინაციის გაძლიერება უწყებებს შორის. პირიქით, კოორდინაციის სახელმწიფო ღერძს ემატება უწყება, რომელმაც არა

მხოლოდ უნდა განახორციელოს შესაბამისი სუბიექტების ზედამხედველობა, არამედ უნდა ითანამშრომლოს უკვე არსებულ სახელმწიფო უწყებასთან (მათ შორის ერთობლივი ბრძანებების გამოცემის სახით), რაც კიბერ-უსაფრთხოების მენეჯმენტს კიდევ უფრო გაართულებს. კოორდინაციის კუთხით კანონპროექტით მკაფიოდ არ არის განსაზღვრული არც თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროსა და შინაგან საქმეთა სამინისტროს შესაბამისი სტრუქტურული ქვედანაყოფის როლი ახალ მოწესრიგებაში.

ინიცირებული კანონპროექტის მიხედვით, იუსტიციის სამინისტროს საჯარო სამართლის იურიდიულ პირს - მონაცემთა გაცვლის სააგენტოს, საკუთარი უფლებამოსილების განხორციელებისას სუს-ის ოპერატიულ-ტექნიკურ სააგენტოსთან კოორდინაციის ვალდებულება ეკისრება. კანონპროექტის თანახმად, მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი ოპერატიულ-ტექნიკურ სააგენტოსთან **კოორდინაციით** ახორციელებს: ა) ინფორმაციული უსაფრთხოების საკითხებზე საზოგადოებრივ საგანმანათლებლო და ინფორმაციულ უზრუნველყოფას; ბ) შესაძლო საფრთხეების შესახებ მოსახლეობის ფართო წრის გაფრთხილებას და მისთვის სათანადო ინფორმაციის მიწოდებას; გ) საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობას; დ) ინფორმაციული უსაფრთხოების საკითხებზე საზოგადოებრივი ცნობიერების ამაღლებას (მე-8^1 მუხლის 1-ლი პუნქტი). კანონპროექტის მე-6 მუხლის მე-2 პუნქტის მიხედვით მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების (ანუ კერძო სექტორის) ინფორმაციული უსაფრთხოების აუდიტის დასკვნები, რომელიც შეიძლება განხორციელებული იქნეს მონაცემთა გაცვლის სააგენტოს ან მათ მიერ ავტორიზებული პირის მიერ **სავალდებულოდ ეგზავნება** ოპერატიულ ტექნიკურ სააგენტოს.

მიუხედავად იმისა, რომ ორმა უწყებამ ერთობლივად უნდა გამოსცეს ინფორმაციული უსაფრთხოების მარეგულირებელი ბრძანებები და ნორმატიულ აქტები, ასეთი მოწესრიგების პირობებში, მონაცემთა გაცვლის სააგენტოს ზედამხედველობა აღარ გავრცელდება საჯარო სექტორზე და ის მთლიანად გადავა ოპერატიულ-ტექნიკური სააგენტოს კომპეტენციაში. მაგალითად, კანონპროექტის თანახმად, პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მენეჯერები ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენენ ოპერატიულ-ტექნიკურ სააგენტოს, ხოლო მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები - მონაცემთა გაცვლის სააგენტოს (მე-7 მუხლის მე-4 პუნქტი). ამავე დროს კერძო სექტორის ინფორმაციული უსაფრთხოების სტანდარტების ზედამხედველობაც მონაცემთა გაცვლის სააგენტომ უნდა განახორციელოს სუს-ის ოპერატიულ ტექნიკურ სააგენტოსთან შეთანხმებით და კოორდინაციით. **ასეთ პირობებში გაუგებარი რჩება ზოგადად მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის, როგორც ცალკე არსებული ერთეულის, დანიშნულება.**

მნიშვნელოვანია ასევე აღინიშნოს, რომ საინფორმაციო და კიბერ უსაფრთხოების სფეროს ასეთი კარდინალური და შინაარსობრივი რეფორმა ხორციელდება იმ პირობებში, როდესაც საქართველოს მთავრობას ჯერ კიდევ არ დაუმტკიცებია ახალი კიბერ უსაფრთხოების ეროვნული სტრატეგია და სამოქმედო გეგმა, ხოლო

კანონპროექტის ავტორი და ინიციატორი არა საქართველოს მთავრობა, არამედ პარლამენტის წევრი ირაკლი სესიაშვილია. გაურკვეველია ასევე რამდენად მონაწილეობდა საქართველოს ეროვნული უსაფრთხოების საბჭოს აპარატი კანონპროექტის შემუშავებაში, მაშინ როდესაც სწორედ მისი წინამორბედი უწყება, სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო, უზრუნველყოფდა კიბერუსაფრთხოების პოლიტიკის ძირითადი ჩარჩოს შემუშავებას. უცნობია აგრეთვე რამდენად იყო განხილული და შეჯერებული საინფორმაციო უსაფრთხოების არქიტექტურის ახალი ხედვა ყველა დაინტერესებულ მხარესთან, მათ შორის კერძო სექტორის იმ წარმომადგენლებთან, ვიზეც სავარაუდოდ გავრცელდება ახალი მკაცრი რეგულაციები.

2. სუბიექტებად დაყოფის კატეგორიზაციის პრობლემურობა და დაცულ უფლებებში ჩარევის მომეტებული რისკი

განმარტებითი ბარათის მიხედვით, საკანონმდებლო ცვლილებების მთავარ მიმართულებას წარმოადგენს კრიტიკული ინფორმაციული სისტემების სუბიექტების ახალი კატეგორიზაცია და მათ მიმართ კონტროლისა და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დიფერენცირებული მიდგომების გამოყენება.

კანონპროექტით გათვალისწინებული ცვლილების შესაბამისად, კრიტიკული ინფორმაციული სისტემის სუბიექტები დაიყოფიან 3 კატეგორიად:

ა) **პირველი კატეგორიის** სუბიექტებში მოხვდებიან სახელმწიფო ორგანოები, დაწესებულებები, საჯარო სამართლის იურიდიული პირები (გარდა რელიგიური და პოლიტიკური გაერთიანებებისა) და სახელმწიფო საწარმოები;

ბ) **მეორე კატეგორიის** სუბიექტებში მოხვდებიან ელექტრონული კომუნიკაციების კომპანიები;

გ) **მესამე კატეგორიის** სუბიექტებში მოიაზრებიან ისეთი კერძო სამართლის იურიდიული პირები, როგორებიც არიან მაგალითად ბანკები და ფინანსური ინსტიტუტები.

ყველა სუბიექტისთვის ზოგადი ვალდებულებების (მაგ. ინფორმაციული უსაფრთხოების მენეჯერის ყოლა და აუდიტის ჩატარების ვალდებულება) გარდა, კანონპროექტს შემოაქვს ასევე დიფერენცირებული მიდგომები სხვადასხვა კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ მათი კონტროლისა და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის თვალსაზრისით.

ყველაზე მკაცრი რეგულაციები უწესდებათ პირველი კატეგორიის სუბიექტებს. ამ კატეგორიის სუბიექტები ვალდებული იქნებიან:

ა) ჰქონდეთ ქსელური სენსორები და მისცენ წვდომა ოპერატიულ-ტექნიკურ სააგენტოს აღნიშნულ ქსელურ სენსორებზე;

ბ) მოთხოვნისთანავე მისცენ წვდომა ოპერატიული ტექნიკურ სააგენტოს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის.

გ) მათ მიმართ სავალდებულო წესით გავრცელდება საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმების პროცედურაც, რომელიც შეიძლება განხორციელდეს ოპერატიულ-ტექნიკური სააგენტოს მიერ ნებისმიერ დროს, გეგმიური ან არაგეგმიური სახით.

დ) ასეთი შემოწმების შედეგად შემუშავებული დასკვნა შესასრულებლად სავალდებულოა აღნიშნული სუბიექტისთვის და მისი შეუსრულებლობა ან დასკვნით გათვალისწინებული მოთხოვნების დარღვევა გამოიწვევს ადმინისტრაციულ სამართლებრივ პასუხისმგებლობას.

„კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის 2014 წლის 29 აპრილის დადგენილებით, პირველი კატეგორიის დღეს მოქმედ ნუსხაში შედიან სხვადასხვა დაწესებულებები, მათ შორის საქართველოს მთავრობისგან ინსტიტუციურად სრულიად დამოუკიდებელი ადმინისტრაციული ორგანოები: საქართველოს პარლამენტი, პრეზიდენტის ადმინისტრაცია, ქალაქ თბილისის მერია, ცენტრალური საარჩევნო კომისია, საქართველოს ეროვნული ბანკი, აგრეთვე სააქციო საზოგადოება საქართველოს რკინიგზა, შპს საქაერონავიგაცია და სხვა. **შესაბამისად, შემოთავაზებული მოწესრიგებით ოპერატიულ ტექნიკური სააგენტოს ეძლევა საშუალება ჰქონდეს სრული წვდომა პირველი კატეგორიას მიკუთვნებული დაწესებულებების ინფორმაციულ აქტივებზე, ინფორმაციული სისტემებსა და ინფრასტრუქტურაზე. ხოლო კანონპროექტის მე-10 მუხლის მე-4 პუნქტის მიხედვით კომპიუტერული ინციდენტების იდენტიფიცირებისთვის თავად აკონტროლებდეს ამ დაწესებულებაში განთავსებულ სენსორს და ქსელს.**

მნიშვნელოვანია აღინიშნოს, რომ მოქმედი კანონმდებლობით ტერმინი **ინფორმაციული აქტივი** საკმაოდ ფართოდ განისაზღვრება, როგორც ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის. კრიტიკული ინფორმაციული სისტემის სუბიექტი ატარებს ინფორმაციული სისტემების ინვენტარიზაციას, რის შედეგადაც ყოველ ინფორმაციულ აქტივს ენიჭება კრიტიკულობის შესაბამისი კლასი – **კონფიდენციალური ან შინასამსახურებრივი** გამოყენების. „ინფორმაციული უსაფრთხოების შესახებ“ კანონის დღეს მოქმედი რედაქცია ითვალისწინებს აღნიშნული ტერმინების განმარტებას, თუმცა ზოგადი ადმინისტრაციული კოდექსით არ არის განსაზღვრული კონფიდენციალური ან შინასამსახურებრივი გამოყენების ინფორმაციის დეფინიცია. სზაკ ამომწურავად ითვალისწინებს საჯარო ინფორმაციის ხელმისაწვდომობიდან გამონაკლის შემთხვევებს, კერძოდ, საჯარო ინფორმაცია ღიაა, გარდა კანონით გათვალისწინებული შემთხვევებისა და დადგენილი წესით სახელმწიფო, კომერციული ან პროფესიული საიდუმლოებისთვის ან პერსონალური მონაცემებისთვის მიკუთვნებული ინფორმაციისა. შესაბამისად,

არსებობს წინააღმდეგობა „ინფორმაციული უსაფრთხოების შესახებ“ კანონსა და ზოგად ადმინისტრაციულ კოდექსს შორის და დღემდე ბუნდოვანია კონფიდენციალური ან შინასამსახურებრივი გამოყენების ინფორმაციის კლასიფიკაცია. ამავე დროს, ასეთი ფართო განმარტება, განუზომლად ზრდის უფლებაში თვითნებურად, გადამეტებულად ჩარევისა და ინფორმაციის ხელმისაწვდომობის დაუსაბუთებელი შეზღუდვის რისკებს.

„ქსელური სენსორის კონფიგურაციის წესების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის ბრძანების მიხედვით, ქსელურ სენსორში იგულისხმება ორგანიზაციის კომპიუტერულ სერვერზე გამართული პროგრამული უზრუნველყოფა, რომელიც ახდენს ქსელის/ქსელის სეგმენტის მდგომარეობის და კავშირების შესახებ ინფორმაციის ჩაწერას და უსაფრთხო კავშირის გამოყენებით ამ ინფორმაციის გადაგზავნას ცენტრალურ შემგროვებელ სერვერზე, რომელიც განთავსდება მონაცემთა გაცვლის სააგენტოში. ამავე ბრძანების მიხედვით ქსელის მონიტორინგის დროს ქსელური სენსორის საშუალებით შემგროვებელ სერვერზე იგზავნება ისეთი მონაცემები, როგორიც არის: ა) შემავალი და გამავალი კავშირების მიმართულება: კონკრეტული IP მისამართები; ბ) კავშირების დამყარების და დასრულების თარიღი და სხვა. **თუმცა, თანამედროვე ტექნოლოგიები საშუალებას იძლევა ასეთი სენსორების კონფიგურირებას იმგვარად, რომ მათ გაცილებით უფრო დიდი მოცულობის და შინაარსის ინფორმაცია დაამუშაონ, მათ შორის საშუალებას, რომ მოხდეს გზავნილების შინაარსის კონტროლიც რეალურ რეჟიმში.**

ზემოთჩამოთვლილი ფაქტორები ზრდის რისკს იმისა, რომ სახელმწიფო უსაფრთხოების სამსახური, თანამედროვე ტექნოლოგიების გამოყენებით, მოიპოვებს პირადი ხასიათის ინფორმაციას განუსაზღვრელ პირთა წრის შესახებ. მართალია, არსებობს პრეზუმფცია, რომ შესაბამისი უფლებამოსილების მქონე ორგანო ბოროტად არ ისარგებლებს ამ ტექნიკური საშუალებებით, თუმცა რეალურ დროში პირადი ხასიათის ინფორმაციის მოპოვების ტექნიკური შესაძლებლობის ფლობა, ადმინისტრირება და პირადი ხასიათის ინფორმაციაზე პირდაპირი წვდომის შესაძლებლობა, ასევე მაიდენტიფიცირებელი მონაცემების (მეტადატის) დამუშავება ისეთი უწყების მიერ, რომელიც არის პროფესიულად დაინტერესებული ამ ინფორმაციის გაცნობით, ქმნის პირად ცხოვრებაში დაუსაბუთებელი ჩარევის მომეტებულ საფრთხეს. დაცულ უფლებებში ჩარევის სწორედ ასეთი მომეტებული რისკი დაინახა საქართველოს საკონსტიტუციო სასამართლომ, როდესაც შეუზღუდა სახელმწიფო უსაფრთხოების სამსახურს მიყურადებისა და მოსმენების ტექნიკურ საშუალებებზე წვდომა.

სუბიექტების კატეგორიზაციაში განსაკუთრებით პრობლემურია მეორე და მესამე კატეგორიის სუბიექტები, რომლებიც კერძო სუბიექტებს წარმოადგენენ. განსაკუთრებით მეორე კატეგორიის სუბიექტები, რომლებიც კანონპროექტის 1-ლი მუხლის „ზ²“ ქვეპუნქტის თანახმად წარმოადგენენ „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით განსაზღვრულ ელექტრონული კომუნიკაციის კომპანიებს.

ამ შემთხვევაში, გაუგებარია რა პრინციპით არიან ისინი გაყოფილნი მეორე და მესამე კატეგორიად და რატომ უწესდებათ ელექტრონული კომუნიკაციის კომპანიებს ოპერატიულ ტექნიკურ სააგენტოსთან ანგარიშვალდებულების უფრო მაღალი სტანდარტი. კანონპროექტის მე-4 მუხლის მე-3 პუნქტის მიხედვით მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტმა, ანუ სატელეკომუნიკაციო კომპანიამ, ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები

განსახილველად უნდა წარუდგინოს ოპერატიულ ტექნიკურ სააგენტოს, ასევე უნდა აცნობონ ამ წესებში შეტანილი ნებისმიერი ცვლილება. ასეთივე ვალდებულება ვრცელდება მესამე კატეგორიის სუბიექტებზეც, რომლებმაც აღნიშნული ინფორმაცია უნდა მიაწოდონ მონაცემთა გაცვლის სააგენტოს.

ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია კომპიუტერული ინციდენტის განმეორების საფრთხის თავიდან აცილების მიზნით იმპერატიულად მოსთხოვოს ელექტრონული კომუნიკაციის კომპანიას მის ინფრასტრუქტურაში მსგავსი კომპიუტერული ინციდენტების იდენტიფიცირებისა და ნეიტრალიზებისთვის აუცილებელი ღონისძიებების განხორციელება. აღსანიშნავია, რომ ამ ვალდებულების შეუსრულებლობა იწვევს ადმინისტრაციულ-სამართლებრივ პასუხისმგებლობას, რამაც თავის მხრივ, შესაძლებელია მეორე კატეგორიის სუბიექტები უფრო მოწყვლადი გახადოს ოპერატიულ-ტექნიკურ სააგენტოსთან ურთიერთობაში და ჯარიმის თავიდან აცილების მიზნით, მათ საკუთარი ნებით მისცენ ოპერატიულ ტექნიკურ სააგენტოს წვდომა საკუთარ ინფრასტრუქტურასთან, მათ შორის ქსელურ სენსორებთან.

სუბიექტების განსაზღვრაში, რომელზედაც ვრცელდება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის დებულებები, განსაკუთრებით პრობლემურია ასეთი დაყოფის განსაზღვრა საქართველოს მთავრობის დადგენილებით, რასაც ითვალისწინებს კანონპროექტის მე-2 მუხლის 1-ლი პუნქტი. აღნიშნული შესაძლებლობას მისცემს საქართველოს მთავრობას დაინტერესებული მხარეების მოსაზრებების მოსმენის გარეშე, გადაწყვიტოს, რომელი სუბიექტი უნდა იყოს შედარებით მკაცრ ან ნაკლებად მკაცრი კონტროლის რეჟიმის ქვეშ.

3. კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ მონაცემების მიღებისა და დამუშავების სტანდარტის განსაზღვრა საქართველოს მთავრობის დადგენილებით

პრობლემურია კანონპროექტის მე-8[2] მუხლის 1-ლი პუნქტი, რომელიც ითვალისწინებს კრიტიკული ინფორმაციული სისტემის როგორც პირველი, ისე მესამე კატეგორიის (მაგალითად ბანკები) სუბიექტების მიერ მონაცემების მიღების, დამუშავების, შენახვის და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების **მწარმოებლებთან** დაკავშირებული მოთხოვნების საქართველოს მთავრობის დადგენილებით განსაზღვრას. ამ მუხლის შესაბამისად საქართველოს მთავრობას ეძლევა საშუალება დაუდგინოს კერძო კომპანიებს გარკვეული შეზღუდვები საკუთარი IT ინფრასტრუქტურისა და პროგრამული უზრუნველყოფის შეძენის, განახლების ან გამოყენების კუთხით. აღსანიშნავია, რომ მთავრობის დადგენილებით გათვალისწინებული მოთხოვნების შეუსრულებლობა გამოიწვევს ამ სუბიექტების დაჯარიმებას 5000 ლარით. ასეთი მიდგომა თავის მხრივ ეწინააღმდეგება თავისუფალი ბაზრისა და კონკურენციის პრინციპებს.

კიბერუსაფრთხოების სფეროში ქვეყნის წინაშე არსებული გამოწვევების ფონზე „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი საჭიროებს გადახედვას და ცვლილებებს, განსაკუთრებით აღსრულების მექანიზმების დახვეწის მიმართულებით. თუმცა, IDFI-ის მიერ იდენტიფიცირებული რისკებისა და პრობლემების გათვალისწინებით, **მოვუწოდებთ საქართველოს პარლამენტს:**

1. მხარი არ დაუჭიროს ინიცირებულ კანონპროექტს;
2. საქართველოს საინფორმაციო და კიბერუსაფრთხოების სისტემის რეფორმა განხორციელდეს საქართველოს მთავრობის მიერ კიბერუსაფრთხოების სტრატეგიისა და სამოქმედო გეგმის დამტკიცების შემდგომ;
3. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში შესატანი ცვლილებების მომზადების პროცესში უზრუნველყოს ყველა დაინტერესებული მხარის, საერთაშორისო და ადგილობრივი არასამთავრობო ორგანიზაციების, კერძო სექტორის ჩართულობა.