IDFI-ის მოსაზრებები კანონპროექტზე –
„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი

“კანონის მიზანია, ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორის უფლება–მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.”

პირველ რიგში, უნდა აღინიშნოს, რომ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტს“ (IDFI) გამართლებულად და დროულად მიაჩნია საკანონმდებლო ინიციატივის განხილვა. ვფიქრობთ, რომ ის რისკები რომლებიც არსებობს ინფორმაციული ტექნოლოგიების მზარდი ტემპით განვითარებისა და გამოყენების კუთხით შესაბამისად უნდა იყოს ასახული საქართველოს კანონმდებლობაშიც. მიუხედავად საკანონმდებლო ინიციატივისადმი ჩვენი დადებითი დამოკიდებულებისა, არსებული კანონპროექტი ბევრ კითხვას ბადებს და ჩვენი აზრით დახვეწას საჭიროებს.

კანონპროექტის საორჭოფო დებულებები ორ ძირითად საკითხად შეიძლება დაიყოს:

1. **საჯარო ინფორმაციის ხელმისაწვდომობის ახალი მარეგულირებელი ნორმები**;
2. **კერძო სექტორის საქმიანობაზე სახელმწიფო კონტროლის დამატებითი მექანიზმების დაწესება**.

- **საჯარო ინფორმაციის ხელმისაწვდომობის ახალი მარეგულირებელი ნორმები**

ჩვენთვის, როგორც არასამთავრობო ორგანიზაციისთვის, რომელიც მუშაობს საჯარო ინფორმაციის ხელმისაწვდომობის საკითხებზე, პირველ რიგში მნიშვნელოვანია ახალი კანონპროექტის მიღების შემთხვევაში შესაძლო შეზღუდვების დაწესება საჯარო ინფორმაციის გაცემის კუთხით.

აღსანიშნავია, რომ ახალი კანონპროექტი ამკვიდრებს „საჯარო ინფორმაციის“ სრულიად ახალ დეფინიციასა და სახეობებს. დღეის მდგომარეობით, საქართველოს კანონმდებლობაში საჯარო ინფორმაციის განმარტება განსაზღვრულია საქართველოს ზოგადი ადმინისტრაციული კოდექსის მიხედვით. კერძოდ სზაკ-ის მე-2 მუხლის პირველი ნაწილის „მ“ ქვეპუნქტის თანახმად საჯარო ინფორმაცია არის:

„ოფიციალური დოკუმენტი (მათ შორის, ნახაზი, მაკეტი, გეგმა, სქემა, ფოტოსურათი, ელექტრონული ინფორმაცია, ვიდეო და აუდიოჩანაწერები) ანუ საჯარო დაწესებულებაში დაცული, აგრეთვე საჯარო დაწესებულების ან მოსამსახურის მიერ სამსახურებრივ საქმიანობასთან დაკავშირებით მიღებული, დამუშავებული, შექმნილი ან გაგზავნილი ინფორმაცია“

ახალი კანონპროექტის მე-2 მუხლის მიხედვით, კი მკვიდრდება **საჯარო ინფორმაციის** შემდეგი კლასიფიკაცია:

> თ) **კონფიდენციალური ინფორმაცია** – *საჯარო ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას სავარაუდოდ მოჰყვება მნიშვნელოვანი ზიანი კრიტიკული ინფრასტრუქტურის სუბიექტის ფუნქციებისათვის*;
>
> ი) **შეზღუდული ინფორმაცია** – *საჯარო ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფა სავარაუდოდ გამოიწვევს კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ მისი ფუნქციების განხორციელების მნიშვნელოვან შეფერხებას, ან ზიანს მიაყენებს სახელმწიფო ინტერესს ან კერძო პირის საქმიან რეპუტაციას*;
>
> კ) **არაკლასიფიცირებული ინფორმაცია** – *საჯარო ინფორმაცია, რომელიც განკუთვნილია მხოლოდ კრიტიკული ინფრასტრუქტურის სუბიექტის თანამშრომლების ან/და მასთან სახელშეკრულებო ურთიერთობაში მყოფი პირისათვის, და რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას შესაძლებელია მოჰყვეს უმნიშვნელო ზიანი ინფრასტრუქტურის სუბიექტის ან/და სახელმწიფო ხელისუფლების ორგანოს უსაფრთხოების, სახელმწიფო ინტერესებისა ან კერძო სუბიექტის საქმიანი რეპუტაციისათვის*;
>
> ლ) **ღია ინფორმაცია** – *ყველა სხვა საჯარო ინფორმაცია, გარდა კონფიდენციალური, შეზღუდული ან არაკლასიფიცირებული ინფორმაციისა*;

აღნიშნული კლასიფიკაცია ვრცელდება კრიტიკული ინფრასტრუქტურის სუბიექტების (მათზე საუბარი შემდგომში გვექნება, თუმცა აქვე გვინდა დავაზუსტოთ, რომ კრიტკული ინფრასტრუქტურის სუბიექტებში სავარაუდოდ იგულისხმება მნიშვნელოვანი ფუნქციის საჯარო დაწესებულებები მაგ. ძალოვანი სტრუქტურები, სამოქალაქო რეესტრი, შესყიდვებისა და კონკურენციის სააგენტო , ეროვნული ბანკი და ა.შ.) **ინფორმაციულ აქტივებზე**. კანონპროექტის მე-2 მუხლის მ ქვეპუნქტის მიხედვით, კი ინფორმაციული აქტივი არის:

ინფორმაციული აქტივი - *ყველა ის ინფორმაცია და ცოდნა, რომელსაც გააჩნია ღირებულება კრიტიკული ინფრასტრუქტურის სუბიექტისათვის, როგორიცაა ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ;*

სწორედ, **ინფორმაციული აქტივების** ასეთი ფართო განსაზღვრება, ბადებს საფუძვლიან ეჭვს, რომ ზემოაღნიშნული კლასიფიკაცია გავრცელდება არა მხოლოდ ინფორმაციულ სისტემებზე, ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნილოგიური საშუალებების მართვაზე, არამედ მოიცავს საჯარო ინფორმაციის უფრო ფართო სპექტრსაც, რადგან კონკრეტულ საჯარო დაწესებულებაში არსებული ინფორმაცია, რომელსაც „გააჩნია ღირებულება“ ამ საჯარო დაწესებულებისთვის, ინტერპრეტაციის ფართო ასპარეზს ტოვებს.

აღნიშნულ ეჭვებს აძლიერებს კანონპროექტის მე-5 მუხლის **(ინფორმაციული აქტივების მართვა)** მესამე პუნქტი:

ინფორმაციული აქტივის შექმნის დროს, კრიტიკულობის შესაბამის კლასს ადგენს აქტივის ავტორი ან/და აქტივზე პასუხისმგებელი პირი.

აღნიშნული დებულებით კრიტიკული ინფრასტრუქტურის სუბიექტები თვითონ მიანიჭებენ საჯარო ინფორმაციას ოთხი კლასიფიკაციიდან ერთ-ერთს, ანუ წყვეტენ თუ რომელი საჯარო ინფორმაცია რომელ კატეგორიას განეკუთვნოს – კონფიდენციალური, შეზღუდული, არაკლასიფიცირებული ან ღია.

საქართველოს საკონსტიტუციო სასამართლომ 2008 წლის 30 ოქტომბრის №2/3/406,408 გადაწყვეტილებით მოახდინა საჯარო ინფორმაციის რამდენიმე კატეგორიად დაყოფა:

ა) *ინფორმაცია, რომელიც საჯარო ინფორმაციის მიღების მსურველ პირს შეეხება*;

ბ) *ინფორმაცია, რომელის შეიცავს სახელმწიფო, კომერციულ ან პროფესიულ საიდუმლოებას*;

გ) *ინფორმაცია, რომელიც საჯარო ინფორმაციის მიღების მსურველს არ შეეხება, მაგრამ მათი გაცემა დასაშვებია საქართველოს კანონმდებლობით გათვალისწინებული შემთხვევებისას*;

დ) *ინფორმაცია, რომელიც კერძო პირის კერძო საკითხებს შეეხება.*

კანონპროექტის მიხედვით, ზემოთ ჩამოთვლილ განსაზღვრებათა რიცხვს ემატება კიდევ ოთხი: კონფიდენციალური, შეზღუდული, არაკლასიფიცირებული და ღია ინფორმაცია.
განვიხილოთ თითოეული მათგანი:

კონფიდენციალური ინფორმაცია - კანონის მე-2 მუხლის „თ“ ქვეპუნქტის თანახმად, იგი წარმოადგენს მონაცემებს, რომლის კონფიდენციალურობის ხელყოფას კრიტიკული ინფრასტრუქტურის სუბიექტის ფუნქციონირების ზიანი მოჰყვება. რას ნიშნავს ფუნქციონირების ზიანი? კანონპროექტის მიხედვით, სუბიექტი შეიძლება იყოს კერძო სამართლის იურიდიული პირიც. მაგალითად, მისი საქმიანობისთვის მნიშვნელოვანია გაასაიდუმლოოს კონკრეტული ინფორმაცია. თუ მან ეს მონაცემები გასცა, ზიანი მიადგება მის კონკურენტუნარიანობას, ანუ მოხდება მისი ფუნქციონირების შეფერხება. როგორც ვხედავთ, იკვეთება ორი ურთიერთგამომრიცხავი შინაარსის მქონე ნორმა: ერთი მხრივ, სზაკ-ის 27[2] მუხლის პირველი ნაწილის მიხედვით, სახეზეა კომერციული საიდუმლოება, ხოლო მეორე მხრივ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-2 მუხლის „თ“ ქვეპუნქტით, კონფიდენციალური ინფორმაცია. ორივე შეიცავს ერთნაირი შინაარსის შემცველ დათქმას.

შეზღუდული ინფორმაცია - ამავე კანონის „ი“ ქვეპუნქტი. ეს ტერმინი ერთგვარი ნოვაციაა ქართულ კანონმდებლობაში, მაგრამ ირიბად იგი ყოველთვის გამოიყენებოდა. ყველა ის ინფორმაცია, რომელიც გასაჯაროებას არ ექვემდებარებოდა შეზღუდული, ხშირ შემთხვევაში, დახურული ინფორმაციის სახით მოიაზრებოდა და აღნიშნული მოწესრიგებული არის სახელმწიფო საიდუმლოების შესახებ საქართველოს კანონით. კანონპროექტში ვხვდებით განმარტებას, რომლის მიხედვითაც, შეზღუდული ინფორმაცია სახეზეა, თუ მისი კონფიდენციალურობის ხელყოფა, სუბიექტის საქმიანობის შეფერხებას (მათ შორის სავარაუდო შეფერხებას) გამოიწვევს, ან ზიანს მიაყენებს სახელმწიფო ან კერძო ინტერესს, ან კერძო პირის საქმიან რეპუტაციას. კერძო პირის საქმიანი რეპუტაციის შემლახველი შეიძლება იყოს ყველა მონაცემები, რომელიც მის პირად საკითხებს ეხება. ამ შემთხვევაში, შეიძლება სახეზე იყოს პირადი მონაცემების შემცველი ინფორმაცია, რომლის გასაიდუმლოების ვალდებულება ეკისრება საჯარო დაწესებულებას. ამასთან, კერძო ინტერესისთვის ზიანის მიყენება შეიძლება გამოიწვიოს ასევე პროფესიული თუ კომერციული საიდუმლოების გაცემამ, რომელიც ასევე სზაკ-ითაა მოწესრიგებული.

არაკლასიფიცირებული ინფორმაცია - ანალოგიური შინაარსის მქონე დათქმაა ჩამოყალიბებული ამავე კანონის მე-2 მუხლის „კ“ ქვეპუნქტში, რომლის მიხედვითაც, არაკლასიფიცირებული ინფორმაცია არის ყველა ის მონაცემი, რომლის

გასაჯაროებითაც შეიძლება **უმნიშვნელო** ზიანი მიადგეს კერძო პირთა თუ სახელმწიფოს ინტერესებს.
პირველ რიგში გასარკვევია, თუ რას ნიშნავს უმნიშვნელო ზიანი და როგორ უნდა განისაზღვროს მისი ხარისხი? ვის ეკისრება მტკიცების ტვირთი და ვინ იქნება ამ საკითხზე პასუხისმგებელი პირი?

ღია საჯარო ინფორმაცია - იგულისხმება კონფიდენციალური, შეზღუდული ან არაკლასიფიცირებული ინფორმაციის გარდა ყველა სხვა სახის საჯარო ინფორმაცია. აქ, კიდევ ერთხელ, უნდა აღინიშნოს, რომ თუ მონაცემები საჯარო ხასიათისაა და მისი გაცნობა ნებისმიერ მსურველს შეუძლია, მაშინ რა საჭიროა საერთოდ საჯარო ინფორმაციის დამცავი ნორმა? ანუ თუ ინფორმაციის მიღება ნებისმიერ მსურველს შეუძლია, მაშინ რატომ უნდა გადაუგზავნოს იგი კონკრეტულმა სუბიექტმა სსიპ - მონაცემთა გაცვლის სააგენტოს მავალდებულებელი ნორმის საფუძველზე?

აქ კიდევ ერთხელ იკვეთება, თუ რა შეუსაბამობაში მოდის წინამდებარე კანონპროექტი ქვეყნის მოქმედ კანონმდებლობასთან. თითოეული განხილული საკითხი სზაკ-ში ცალკე სახითაა მოწესრიგებული. კანონპროექტიდან და დღევანდელი პრაქტიკიდან გამომდინარე, საჯარო ინფორმაცია, ნაცვლად ოთხი სახისა, რვა სახედ იყოფა:

ა) ინფორმაცია, რომელიც საჯარო ინფორმაციის მიღების მსურველ პირს შეეხება;

ბ) ინფორმაცია, რომელის შეიცავს სახელმწიფო, კომერციულ ან პროფესიულ საიდუმლოებას;

გ) ინფორმაცია, რომელიც საჯარო ინფორმაციის მიღების მსურველს არ შეეხება, მაგრამ მათი გაცემა დასაშვებია საქართველოს კანონმდებლობით გათვალისწინებული შემთხვევებისას;

დ) ინფორმაცია, რომელიც კერძო პირის კერძო საკითხებს შეეხება. განვიხილოთ, თუ რომელი მათგანია სახეზე წინამდებარე საქმის მიხედვით:

ე) კონფიდენციალური ინფორმაცია;

ვ) შეზღუდული ინფორმაცია;

ზ) არაკლასიფიცირებული ინფორმაცია;

თ) ღია ინფორმაცია.

არ უნდა დაგვავიწყდეს, შემდეგი ფაქტორიც, საქართველოს კონსტიტუცია ინფორმაციის გასაიდუმლოების ოთხ სახეს იცნობს: პირად, სახელმწიფო, პროფესიულ და კომერციულ საიდუმლოებას. საქართველოს კანონმდებლობა კრძალავს კონკრეტულ საკითხებს მიკუთვნებული მონაცემების გასაჯაროებას. „სახელმწიფო საიდუმლოების შესახებ“ საქართველოს კანონის მიხედვით „სახელმწიფო საიდუმლოება“ არის:

„ინფორმაციის სახეობა, რომელიც მოიცავს სახელმწიფო საიდუმლოების შემცველ მონაცემებს თავდაცვის, ეკონომიკის, საგარეო ურთიერთობის, დაზვერვის, სახელმწიფო უსაფრთხოების და მართლწესრიგის დაცვის სფეროებში, რომელთა გამჟღავნებას ან დაკარგვას შეუძლია ზიანი მიაყენოს საქართველოს ან საერთაშორისო ხელშეკრულებებისა და შეთანხმებების მონაწილე მხარის სუვერენიტეტს, კონსტიტუციურ წყობილებას, პოლიტიკურ და ეკონომიკურ ინტერესებს, რაც ამ კანონით ან/და საერთაშორისო ხელშეკრულებით ან შეთანხმებით დადგენილი წესით აღიარებულია სახელმწიფო საიდუმლოებად და ექვემდებარება სახელმწიფო დაცვას.“

ამავე დროს, საქართველოს კანონმდებლობა აწესებს არა მარტო ინფორმაციის გასაიდუმლოების სტანდარტებს, არამედ ადგენს მათი გაცნობის, მათი შემდგომი გასაჯაროების, მათზე ხელმისაწვდომობის პროცედურებსაც. ამავე დროს, საჯარო ინფორმაციის ხელმისაწვდომობა განსაზღვრულია საქართველოს ზოგადი ადმინისტრაციული კოდექსით. ხოლო, კანონპროექტის მეორე თავის, მე-5 მუხლის, მე-4 პუნქტით დგინდება კლასიფიცირებული ინფორმაციის (მათ შორის **ღია ინფორმაციის**) წვდომის, გაცემის (გამოქვეყნების), შეცვლის ან განადგურების ახალი წესები:

ინფორმაციული აქტივების აღწერის, კლასიფიცირების, მასზე წვდომის, მისი გაცემის (გამოქვეყნების), მისი შეცვლის ან განადგურების წესს ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო.

ვფიქრობთ ზემოთ აღნიშნული მუხლი შეუსაბამობაში მოდის საქართველოს ზოგად ადმინისტრაციულ კოდექსთან და საქართველოს იუსტიციის სამინისტროს საჯარო სამართლის იურიდიულ პირს - მონაცემთა გაცვლის სააგენტოს ანიჭებს მაკონტროლებელი ორგანოს უფლებამოსილებებს.

შესაბამისად აუცილებალად მიგვაჩნია რიგი ტერმინების დაზუსტება, მაგ.:

ინფორმაციული აქტივი - კრიტიკული ინფრასტრუქტურის სუბიექტში დაცული ყველა ის ინფორმაცია და ცოდნა, რომელიც უკავშირდება კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციული სისტემების ფუნქციონირებას,

როგორიცაა ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ;
ჩვენ ასევე ვთვლით, რომ არ არსებობს **საჯარო ინფორმაციის** კანონპროექტში არსებული ინტერპრეტაციის დამკვიდრების აუცილებლობა და იმ შემთხვევაში, თუ აუცილებელი ხდება კონკრეტულ საჯარო ინფორმაციაზე ხელმისაწვდომობის შეზღუდავა, შესაბამისმა საჯარო დაწესებულებებმა უნდა იხელმძღვანელონ საქართველოს კანონით „სახელმწიფო საიდუმლოების“ და საქართველოს ზოგადი ადმინისტრაციული კოდექსის შესაბამისად.

ზოგადად, კანონპროექტის განმარტებითი ბარათიდან გამომდინარე იკვეთება, რომ ახალი კანონის მიღების ძირითადი მიზანია კრიტიკული ინფრასტრუქტურის სუბიექტთა **საინფორმაციო სისტემების** (ინფო-საკომუნიკაციო ტექნოლოგიების) უსაფრთხოების დაცვა, პირველ რიგში კიბერ-სივრცეში. კერძოდ:

*„სააგენტოს ევალება „უზრუნველყოს ინფორმაციული უსაფრთხოება, მათ შორის, განახორციელოს საგანმანათლებლო საქმიანობა როგორც საჯარო, ისე სამოქალაქო სექტორში“, რა მიზნითაც მას შეუძლია „შეიმუშაოს **ინფორმაციული ტექნოლოგიების (სისტემების) სფეროს** მარეგულირებელი სამართლებრივი აქტების პროექტები“ (იმავე მუხლის „მ“ ქვეპუნქტი). **შემოთავაზებული კანონპროექტი სწორედ ამ უფლებამოსილებათა განხორციელებას ემსახურება.**“*

*„დღეს არსებული მდგომარეობით თითოეული სამინისტრო და სახელმწიფო უწყება თავისი არსებული რესურსების გამოყენებით ზრუნავს **კიბერ უსაფრთოების დაცვაზე**. რესურსებიდან გამომდინარე დაცვის დონე განსხვავებულია უწყებს შორის. ხშირად ეს დონე არ შეესაბამება დაცვის მინიმალურ დონესაც. რაც შეეხება სამოქალაქო სექტორს ან მოქალაქეებს, ამ მიმართულებით თითქმის არავითარი ნაბიჯები არ არის გადადგმული.*“

იგივე დასკვნის გაკეთების საშუალებას გვაძლევს კრიტიკული ინფრასტრუქტურის განსაზღვრებაც:

*„კრიტიკული ინფრასტრუქტურა – ამ კანონით და კანონის საფუძველზე გამოცემული სხვა ნორმატიული აქტით განსაზღვრული იურიდიული პირების, სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, **რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება** მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის“*

აქედან გამომდინარე, ჩვენ მიგვაჩნია, რომ კანონპროექტის დებულებები მიმართული უნდა იყოს ინფორმაციული სისტემებისა და ამ სისტემების უსაფრთხოდ ფუნქციონირების უზრუნველსაყოფად, ხოლო საიდუმლოების საკითხი, საქართველოს კანონმდებლობით სწორედ იმიტომაა მოწესრიგებული, რომ უზრუნველყოს საჯარო დაწესებულების ინფორმაციული უსაფრთხოება.

- **კერძო სექტორის საქმიანობაზე სახელმწიფო კონტროლის დამატებითი მექანიზმების დაწესება**

არსებული კანონპროექტი საქართველოს სამართლებრივ სივრცეში ამკვიდრებს ისეთ ტერმინებს, როგორიცაა კრიტიკული ინფრასტრუქტურა და კრიტიკული ინფრასტრუქტურის სუბიექტი:

კრიტიკული ინფრასტრუქტურა *– ამ კანონით და კანონის საფუძველზე გამოცემული სხვა ნორმატიული აქტით განსაზღვრული* ***იურიდიული პირების****, სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის;*

კრიტიკული ინფრასტრუქტურის სუბიექტი *– სახელმწიფო ორგანო,* ***იურიდიული პირი****, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური უსაფრთხოების, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის;*

ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირზე და სახელმწიფო ორგანოზე, რომელიც წარმოადგენს კრიტიკული ინფრასტრუქტურის სუბიექტს. კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციზე ან უწყებაზე, რომელიც შედის კრიტიკული ინფრასტრუქტურის სუბიექტის დაქვემდებარებაში ან დაკავშირებულია სუბიექტთან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით, რომელიც უზრუნველყოფს წვდომას ინფორმაციულ აქტივზე ასეთი ურთიერთობის ფარგლებში.

სამწუხაროდ, **ჩვენ წინასწარ არ შეგვიძლია ვიცოდეთ, თუ ვინ იგულისხმება კრიტიკული ინფრასტრუქტურის სუბიექტებში**, რადგანაც მათი ჩამონათვალი უშიშროების საბჭოს წარდგინებით უნდა დაამტკიცოს საქართველოს პრეზიდენტმა კანონის მიღებიდან ექვსი თვის განმავლობაში.

თუმცა, შესაძლებელია, სავარაუდოდ, მაინც განისაზღვროს იმ სუბიექტთა ჩამონათვალი, რომლებზეც გავრცელდება „ინფორმაციული უსაფრთხოების“ კანონი. კერძოდ, იქიდან გამომდინარე, რომ კანონპროექტი შემუშავებული საერთაშორისო

პრაქტიკის გათვალისწინებით, ვფიქრობთ, რომ კრიტიკული ინფრასტრუქტურის სუბიექტებში იგულისხმება:

- საფინანსო სექტორი;
- კომუნიკაციების სექტორი;
- ინფორმაციული ტექნოლოგიების სექტორი;
- ენერგეტიკისა და წყალმომარაგების სექტორი;
- სატრანსპორტო სისტემების სექტორი;
- ჯანმრთელობის დაცვისა სექტორი;
- ინდუსტრიული, მათ შორის სამშენებლო და ქიმიური მრეწველობის სექტორი;
- თავდაცვისა და უსაფრთხოების სექტორი და ა.შ.

თავისთავად, აღნიშნული სექტორები მოიცავენ საკმაოდ ფართო სპექტრს მიმართულებებისა, რომელიც შესაძლებელია მიჩნეულ იქნეს კრიტიკული ინფრასტრუქტურის სუბიექტებად. აღნიშნული ჩამონათვალი ფართოვდება შემდეგი ჩანაწერით:

ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირზე და სახელმწიფო ორგანოზე, რომელიც წარმოადგენს კრიტიკული ინფრასტრუქტურის სუბიექტს. ***კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციზე ან უწყებაზე, რომელიც შედის კრიტიკული ინფრასტრუქტურის სუბიექტის დაქვემდებარებაში ან დაკავშირებულია სუბიექტთან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით,*** *რომელიც უზრუნველყოფს წვდომას ინფორმაციულ აქტივზე ასეთი ურთიერთობის ფარგლებში.*

მაგალითად, ამერიკის შეერთებული შტატებში კრიტიკულ ინფრასტრუქტურად ითვლება მასობრივი საზოგადოებრივი თავშეყრის ადგილები. თუმცა, პარლამენტში ინიციირებულ კანონპროექტში ზუსტდება, რომ კრიტიკული ინფრასტრუქტურის სუბიექტია – „სახელმწიფო ორგანო, იურიდიული პირი, რომლის **ინფორმაციული სისტემების** უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური უსაფრთხოების, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის.“ შესაბამისად, საქართველოს შემთხვევაში იგულისხმება ზემოთჩამოთვლილი სექტორებში მოქმედი ის სუბიექტები, რომელთა საქმიანობაც მჭიდროდ არის დაკავშირებული ინფორმაციული სისტემების ფუნქციონირებასთან. მაგ.:

- საფინანსო სექტორში - ბანკები და სხვა ფინანსური ინსტიტუტები;
- კომუნიკაციების სექტორში - სამაუწყებლო და საკომუნიკაციო კომპანიები;
- ინფორმაციული ტექნოლოგიების სექტორში - ინტერნეტ პროვაიდერი კომპანიები და ა.შ.

ამავე დროს, აღნიშვნის ღირსია ის ფაქტი, რომ კრიტიკული ინფრასტრუქტურის სუბიექტების მნიშვნელოვან წილს (სავარაუდოდ 60-70%), საერთაშორისო პრაქტიკიდან გამომდინარე, შეადგენენ კერძო სექტორის წარმომადგენელი კომპანიები და ორგანიზაციები. ა ღნიშნული ფაქტორის გათვალისწინებით, **კანონპროექტის მიერ დაწესებული რეგულაციები და მოთხოვნები, უპირველეს ყოვლისა, სწორედ კერძო სექტორის წარმომადგენლებზე გავრცელდება**. ჩვენ მოვიყვანთ ახალი წესების იმ მაგალითებს რომლებიც, ჩვენის აზრით, კერძო სექტორის თავისუფლად საქმიანობის სახელმწიფოს მხრიდან კონტროლის გამკაცრებაზე მიუთითებს. კერძოდ:

კანონპროექტის მე-4 მუხლის (**ინფორმაციული უსაფრთხოების წესები**) მესამე პუნქტის მიხედვით:

> *„კრიტიკული ინფრასტრუქტურის სუბიექტი **ვალდებულია წარუდგინოს მონაცემთა გაცვლის სააგენტოს მიღებული ინფორმაციული უსაფრთხოების პოლიტიკა, ისევე როგორც მასში განხორციელებული ნებისმიერი ცვლილება.**“*

იურიდიული პირის უსაფრთხოების, მათ შორის ინფორმაციული უსაფრთხოების, პოლიტიკა მისი კომერციული საიდუმლოებაა (მ.შ. ინტელექტუალური საკუთრება, სამრეწველო საკუთრების ისეთ ობიექტებთან დაკავშირებული საიდუმლოება როგორიცაა გამოგონება, ე.წ. „ნოუ ჰაუ“ და ა.შ.). ამავე დროს, რთული წარმოსადგენია, რომ რომელიმე კერძო კომპანია ნებაყოფლობით ხელმისაწვდომს გახდიდა აღნიშნულ დოკუმენტს. მითუმეტეს, თუ მას არ აქვს იმის გარანტია, რომ დოკუმენტში მოცემული ინფორმაცია არ იქნება გამოყენებული მის წინააღმდეგ. კანონპროექტი ცალმხრივ ვალდებულებებს უწესებს კერძო სექტორის წარმომადგენლებს და თავის მხრივ მასში არ არის ასახული რაიმე სახის გარანტიები ინფორმაციის არ გამჟღავნების, დაცვის, მესამე მხარისთვის უნებართვოდ გადაცემის ან თუნდაც, იგივე ინფორმაციის კერძო მესაკუთრის წინააღმდეგ გამოყენების შესახებ.

ინფორმაციის თავისუფლების საკითხი თავისი ბუნებით სწორედ საჯარო სექტორს ეხება და მისი მავალდებულებელი ნორმები არ შეიცავენ კერძო საქმიანობის სფეროში ჩარევის მომწესრიგებელ დათქმას. გამონაკლისს წარმოადგენს მხოლოდ ის კერძო დაწესებულებები, რომლებიც სახელმწიფო ბიუჯეტიდან ფინანსდებიან და ასევე საჯარო სამართლებრივ უფლებამოსილებას ახორციელებენ. წინამდებარე კანონის მიხედვით კი, სახელმწიფო თავად განსაზღვრავს, თუ რომელი ორგანიზაციისკენ იქნება ეს ნორმა მიმართული და რომელი მათგანი გახდება ვალდებული, გასცეს ინფორმაცია სსიპ - მონაცემთა გაცვლის სააგენტოზე.

საინტერესოა საკითხი, თუ რა სტანდარტებია დაწესებული იმ შემთხვევაში, თუ კერძო სექტორის წარმომადგენელი სუბიექტი კონკრეტულ ინფორმაციას კომერციულ საიდუმლოებად მიიჩნევს? კანონპროექტი ხაზგასმით აღნიშნავს, რომ კომერციული საიდუმლოების შემცველ მონაცემებთან მას კავშირი საერთოდ არ გააჩნია და იგი სზაკ-ით რეგულირდება. მაშინ საინტერესოა, რა სახის ქმედების განხორციელების შესაძლებლობა აქვს სსიპ - მონაცემთა გაცვლის სააგენტოს, თუ კონკრეტულმა სუბიექტმა, რომელიც კერძო სექტორს წარმოადგენს, შესაბამისი ინფორმაცია მასზე საერთოდ არ გასცა და მიზეზად კომერციული საიდუმლოების შემცველი მონაცემები მიუთითა.

კანონპროექტის მე-5 მუხლის (**ინფორმაციული აქტივების მართვა**) მეოთხე პუნქტის მიხედვით:

ინფორმაციული აქტივების აღწერის, კლასიფიცირების, მასზე წვდომის, მისი გაცემის (გამოქვეყნების), მისი შეცვლის ან განადგურების წესს ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო.

კანონპროექტის მე-6 მუხლის (**აუდიტი და ტესტირება**) 1-ლი, 4-ე და მე-6 პუნქტების მიხედვით:

*მონაცემთა გაცვლის სააგენტო ან, მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზირებულ პირთა წრიდან კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ შერჩეული პირი ან ორგანიზაცია, ატარებს კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციული უსაფრთხოების პოლიტიკის თავსებადობის შეფასებას მონაცემთა გაცვლის სააგენტოს მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან (ინფორმაციული უსაფრთხოების აუდიტი). **ინფორმაციული აუდიტის ჩატარების შედეგად დგება დასკვნა, რომელიც სავალდებულოა შესასრულებლად.***

*მონაცემთა გაცვლის სააგენტო ნორმატიული აქტით განსაზღვრავს ინფორმაციული უსაფრთხოების აუდიტის ჩატარებაზე უფლებამოსილ პირთა ან ორგანიზაციათა **ავტორიზაციის გავლის წესს, ავტორიზაციის პროცედურებსა და ავტორიზაციის საფასურს.***

*თუ აუდიტის ან ტესტირების შედეგად გამოვლინდა ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნებთან შეუსაბამობა, კრიტიკული ინფრასტრუქტურის სუბიექტი ატარებს შეუსაბამობის მიზეზის ანალიზს და, საჭიროების შემთხვევაში, განსაზღვრავს და ახორციელებს სათანადო გამოსასწორებელ ღონისძიებებს, **რომელთა გრაფიკსაც წარუდგენს მონაცემთა გაცვლის სააგენტოს.***

კანონპროექტის მე-7 მუხლის (**ინფორმაციული უსაფრთხოების ოფიცერი**) მეოთხე პუნქტის მიხედვით:

> *ინფორმაციული უსაფრთხოების ოფიცერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას, და **გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარდუგენს** ამ მუხლის მე–3 პუნქტით განსაზღვრულ პირს (პირებს) და **მონაცემთა გაცვლის სააგენტოს.***

ზემოთ აღნიშნული მუხლებით, სახელმწიფო კერძო სექტორს უწესებს მკაცრ შეზღუდვებსა და სავალდებულო ანგარიშგების რეგულაციებს მისი საქმიანობის ისეთ სასიცოცხლოდ მნიშვნელოვან სფეროში, როგორიც არის ინფორმაციული უსაფრთხოება. აღნიშნული წესები კანონის ამოქმედების შემდგომ იქნება შემუშავებული მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტით, შესაბამისად რთულია იმაზე მსჯელობა, თუ რა ხარისხისა და რა სახის შეზღუდვები დაწესდება, თუმცა ცალსახაა, რომ ხელისუფლების მიერ კერძო სექტორის საქმიანობაში ამგვარი სახის ჩარევა გარკვეულწილად ზღუდავს მათ თავისუფლებას და ეწინააღმდეგება საბაზრო ეკონომიკის პრინციპებს.

კანონპროექტში აგრეთვე არის რიგი სხვა დებულებებისა, რომლებიც ჩვენი აზრით კერძო სექტორის საქმიანობაში უხეში ჩარევად შეიძლება ჩაითვალოს. მაგ. ხელისუფლება არამარტო ითხოვს არასახელმწიფო (კერძო) ორგანიზაციებში ორი საშტატო ერთეულის იმპერატიულ არსებობას - **ინფორმაციული უსაფრთხოების ოფიცერი** და **კომპიუტერული უსაფრთხოების სპეციალისტი**, არამედ თავ ადვე განსაზღვრავს მათ ფუნქციებსა და კომპეტენციას, მათი ანგარიშვალდებულების ხარისხს და დისპოზიციას (მე-7 და მე-9 მუხლი). ამავე დროს, შესაძლებელი ხდება კერძო სექტორში დასაქმებულ პირთა (ამ შემთხვევაში საუბარია კომპიუტერული უსაფრთხოების სპეციალისტებზე) იძულებითი მობილიზაცია, მათ შორის **სავარაუდო** კიბერშეტევის დროს, რაც ჩვენი აზრით შრომის უფლებებისა და არჩევანის თავისუფლების შეზღუდვად შეიძლება მივიჩნიოთ:

> *იმ შემთხვევაში, როდესაც **მიმდინარე ან სავარაუდო კიბერშეტევა** წარმოადგენს განსაკუთრებულ საფრთხეს ქვეყნის თავდაცვისუნარიანობის, ეკონომიკური უსაფრთხოების, სახელმწიფო ხელისუფლებისა და საზოგადოების ნორმალური ფუნქციონირების წინააღმდეგ, მონაცემთა გაცვლის სააგენტო უფლებამოსილია, **განახორციელოს კრიტიკული ინფრასტრუქტურის სუბიექტების კომპიუტერული უსაფრთხოების სპეციალისტების დროებითი მობილიზაცია** (კოორდინაცია) შეტევის პრევენციის, მოგერიების ან/და შედეგების აღმოფხვრის მიზნით.*

გასათვალისწინებელია, აგრეთვე, ისეთი საკითხი, როგორც ქსელური სენსორის დანერგვა იურიდიული პირების ინფორმაციულ სისტემებში. შესაძლებელია, რომ მისი მეშვეობით მონაცემთა გაცვლის სააგენტოს ნებისმიერ დროს ჰქონდეს წვდომა

გარკვეულ ინფორმაციაზე, მათ შორის კონფიდენციალურ ინფორმაციაზე. შესაბამისად აუცილებელია ქსელური სენსორის ფუნქციონალური შესაძლებლობების მეტად დაკონკრეტება. ზოგადად, იგი შეიძლება მართლაც სასარგებლო აღმოჩნდეს, თუმცა ყველა სისტემას, აპლიკაციას თუ ვებ-გვერდს სჭირდება ინდივიდუალური მიდგომა, რადგან სისტემები მკვეთრად განსხვავდებიან ერთმანეთისაგან, როგორც ლოგიკით, ასევე ხარვეზებით. ქსელურ სენსორს უნდა ჰქონდეს საერთაშორისო ლიცენზია, რათა გარანტირებული იყოს ის, რომ იგი მართლაც იმ საქმესთვის არის მიმართული რისთვისაც შეიქმნა. იგი უნდა იყოს Open Source-ი, რათა კერძო კომპანიების IT სფეროს წარმომადგენლები დარწმუნდნენ, რომ სენსორში სხვა ფუნქციები, რაც კონფიდენციალური ინფორმაციას შეუქმნის საფრთხეს, არ იქნება დანერგილი.

ზოგადად შეიძლება ითქვას, რომ ერთი დაცვის მოდელის ჩამოყალიბება ყველა სისტემისთვის ვერასდროს იქნება ისეთი ეფექტური, როგორც ინდივიდუალური პოლიტიკა და მიდგომა. ამავე დროს, კერძო სექტორს გაცილებით უფრო დიდი ფინანსური რესურსები და მაღალკვალიფიცირებული კადრები ჰყავს ვიდრე საჯარო სექტორს. საკუთარი ინფორმაციული სისტემების უსაფრთხოება მნიშვნელოვანია, პირველ რიგში კერძო სექტორის სუბიექტებისთვის. უსაფრთხოების სისტემები და კერძო სექტორის სუბიექტთა უსაფრთხოების პოლიტიკა შესაძლებელია განსხვავებული იყოს ერთმანეთისაგან ისევე, როგორც საჯარო სექტორის სპეციფიკა ვერ იქნება იდენტური. მიუხედავად, იმ ფაქტორისა, რომ სახელმწიფოში უნდა არსებობდეს კიბერ-უსაფრთხოების კონსოლიდირებული სისტემა და სტრატეგია, სასურველია, რომ აღნიშნული განხორციელდეს თავისუფალი ეკონომიკის პრინციპებზე დაყრდნობით და მაკონტროლებელი ინსტიტუტების კერძო სექტორის საქმიანობაში ჩარევის მინიმალიზაციით.

ჩვენ ვფიქრობთ, რომ კერძო სექტორთან მიმართებაში სახელმწიფოს მაკონტროლებელი ფუნქცია, უნდა შეიცვალოს მაკოორდინირებელი, დამხმარე და სარეკომენდაციო ფუნქციით, ხოლო შესაბამისი სამართლებრივი ნორმები ზედმიწევნით კონკრეტული და არაბუნდოვანი უნდა იყოს.