კიბერსივრცეში პერსონალური მონაცემების დაცულობის უზრუნველყოფა

გამოწვევები და საჭიროებები საქართველოსთვის

ინფორმაციის თავისუფლების
განვითარების ინსტიტუტი

კვლევა მომზადდა ინფორმაციის თავისუფლების განვითარების ინსტიტუტის (IDFI) მიერ და მის შინაარსზე პასუხისმგებელია IDFI.

ავტორი: ნატა გოდერძიშვილი

შინაარსი

შესავალი 4

კიბერსივრცეში პერსონალურ მონაცემთა უსაფრთხოების ევროპული და ქართული მოდელების შედარებითი ანალიზი..... 5

პერსონალურ მონაცემთა კიბერუსაფრთხოება ევროპულ სამართლებრივ სისტემაში 5

პერსონალურ მონაცემთა კიბერუსაფრთხოება საქართველოს სამართლებრივ სისტემაში..... 9

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის NIS დირექტივასთან კრიტიკული შეუსაბამობები..... 12

პერსონალურ მონაცემთა კიბერუსაფრთხოების თვალსაზრისით „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ნაკლოვანებები..... 16

შეჯამება 19

რეკომენდაციები 20

შესავალი

კიბერინციდენტების მასშტაბურობა, სიხშირე და გავლენა ყოველდღიურად იზრდება და დიდ საფრთხეს უქმნის ქსელისა და ინფორმაციული სისტემების გამართულ ფუნქციონირებას, ტექნოლოგიების საშუალებით გადაცემული/დაცული ინფორმაციის მთლიანობას, ხელმისაწვდომობას, ავთენტურობასა და კონფიდენციალურობას. კრიტიკული ინფორმაციული სისტემების ფუნქციონირების შეფერხებამ, ინფორმაციული რესურსების კომპრომეტირებამ შესაძლოა მნიშვნელოვნად შეაფერხოს ან საერთოდ გააჩეროს სახელმწიფო თუ კერძო ორგანიზაციის საქმიანობა, მნიშვნელოვანი ფინანსური ზარალი გამოიწვიოს, შეამციროს მომხმარებლის ნდობა და დიდი ზიანი მიაყენოს როგორც ქვეყნის ეკონომიკას, ასევე ზოგადად, სამოქალაქო ბრუნვასა და საზოგადოების ნორმალურ ფუნქციონირებას.

ციფრული ტრანსფორმაციის ეპოქაში სულ უფრო მეტი ონლაინ ტრანზაქცია ხორციელდება, ელექტრონულ სახელმწიფო თუ კომერციულ სერვისებს მზარდი რაოდენობის მომხმარებლები ჰყავს. შესაბამისად, დღესდღეისობით პერსონალური მონაცემების უმეტესობა სწორედ ინფორმაციულ სისტემებში, ელექტრონულ რეესტრებსა და საკომუნიკაციო ქსელებში აკუმულირდება. ამიტომაც, პერსონალური მონაცემების დარღვევა ყველაზე ხშირად სწორედ ამ მოწყობილობების კომპრომეტირებით მასიური კიბერშეტევების გზით ხორციელდება. შედეგად კი ვიღებთ კიბერსივრცეში მოქალაქეთა ციფრული უფლებების, მათ შორის პერსონალური მონცემების დარღვევის ფაქტებს. აქვე მნიშვნელოვანია აღვნიშნოთ, რომ პერსონალური მონაცემების დაცულობა პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზებასთან პირდაპირ კავშირშია და კიბერსივრცეში პერსონალური მონაცემების უსაფრთხოების უზრუნველყოფა უპირობოდ გაუმჯობესების კუთხით ახდენს გავლენას ჩვენი ციფრული პრივატულობის/ხელშეუხებლობის ხარისხზე.

კიბერუსაფრთხოება ხელშემწყოფი გარანტია ციფრულ სამყაროში ადამიანის ფუნდამენტური უფლებებისა და თავისუფლებების დასაცავად, მათ შორის პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის უფლების რეალიზებისთვის. ციფრული გარემოს უსაფრთხოება მნიშვნელოვანია არა მხოლოდ პირადი უსაფრთხოებისთვის, პერსონალური მონაცემების დაცვისა და ხელშეუხებლობისთვის, არამედ იგი ეკონომიკის, საზოგადოებისა და დემოკრატიის მიმართ ნდობის გამყარების მნიშვნელოვანი წინაპირობა და ქვეყნის დინამიური განვითარების ხელშემწყობი მოვლენაა.

პერსონალურ მონაცემთა უსაფრთხოება და ინტერნეტ სივრცეში პირადი ცხოვრების ხელშეუხებლობა აუცილებელია თანხვედრაში იყოს და ინტეგრირდეს კიბერუსაფრთხოების ხელშემწყობ ჩარჩოებსა და მის პრაქტიკულ უზრუნველყოფაში. მნიშვნელოვანია კიბერუსაფრთხოებისა და ციფრულ სამყაროში პერსონალურ მონაცემთა დაცვის საკითხების მიმართ ჰოლისტური, უნიფიცირებული მიდგომა, ამ თემების ურთიერთთავსებადად და არა

იზოლირებულად და ურთიერთკონფლიქტური ფორმით განვითარება. პერსონალურ მონაცემთა დაცვის ინტეგრირება კიბერუსაფრთხოების მართვის სისტემაში დადებითი უკუშედეგის მატარებელია როგორც კიბერუსაფრთხოების გაძლიერების, ასევე პერსონალურ მონაცემთა დაცვის თვალსაზრისით.

მოცემული კვლევის მიზანია კიბერსივრცეში პერსონალური მონაცემების დაცვისა და კიბერუსაფრთხოების მარეგულირებელი სამართლებრივი გარემოს შესწავლა, არსებული გამოწვევებისა და ნაკლოვანებების გამოვლენა და საუკეთესო ევროპულ სამართლებრივ ჩარჩოებზე დაყრდნობით, მტკიცებულებებზე დაფუძნებული რეკომენდაციების შემუშავება.

კიბერსივრცეში პერსონალურ მონაცემთა უსაფრთხოების ევროპული და ქართული მოდელების შედარებითი ანალიზი

პერსონალურ მონაცემთა კიბერუსაფრთხოება ევროპულ სამართლებრივ სისტემაში

ციფრული ბაზრის უსაფრთხოდ ფუნქციონირება, დიჯიტალიზაციის პროცესის ეფექტიანობა და ეფექტურობა, ელ-მმართველობისა და ელ-კომერციის სერვისების ფართომასშტაბიანად დანერგვა, ისევე როგორც ინფორმაციული საზოგადოების მხრიდან ახალი ტექნოლოგიური გადაწყვეტილებების მიმართ ნდობის ჩამოყალიბება და ტექნოლოგიური გადაწყვეტილებებით სარგებლობის ინტერესი დიდწილად არის დამოკიდებული ციფრული კონიუნქტურის, კიბერსივრცის უსაფრთხოებაზე, დაცულობასა და რისკებისა და საფრთხეების მიმართ მედეგობაზე.

სწორედ ამ მიზნის უზრუნველსაყოფად, ევროკავშირის ფარგლებში თითქმის ერთდროულად ორი პარალელური პროცესი წარიმართა:

1) 2016 წელს ევროპარლამენტმა მიიღო ქსელებისა და ინფორმაციული სისტემების უსაფრთხოების შესახებ NIS დირექტივა,[1] რომელიც მიზნად ისახავს ევროკავშირის წევრ ქვეყნებს შორის **კიბერუსაფრთხოების ერთიანი და ერთგვაროვანი სტანდარტების დანერგვა**ს, ჰორიზონტალურ დონეზე ყოვლისმომცველი უსაფრთხოების ნორმებისა და სავალდებულოდ შესასრულებელი მინიმალური მოთხოვნების ჩამოყალიბებას, იმისთვის რომ ევროკავშირის წევრმა ქვეყნებმა უზრუნველყონ ქსელებისა და ინფორმაციული სისტემების მაღალი დონის დაცულობა და შედეგად გაუმჯობესდეს ევროპული ერთიანი ციფრული ბაზრის ფუნქციონირება.

[1] "Directive 2016/1148. The Measures for a high common level of security of network and information systems across the Union," accessed November 11, 2021, http://data.europa.eu/eli/dir/2016/1148/oj

ევროკავშირის წევრ სახელმწიფოებს დირექტივის ეროვნული ტრანსპოზიციისთვის საბოლოო ვადად 2018 წელი განესაზღვრათ.

ქსელების და ინფორმაციული სისტემების უსაფრთხოების შესახებ ევროკავშირის NIS დირექტივა სპეციალურად შეიქმნა ინფორმაციული სისტემებისა და ქსელების უსაფრთხოების რეგულირებისათვის. მისი **მიზანია დაიცვას ინფორმაციულ სისტემები, ტექნოლოგიური გარემო, კომპიუტერული ინფრასტრუქტურა, კიბერსივრცეში ქსელებსა და ინფორმაციულ სისტემებში მონაცემების (მათ შორის, პერსონალური მონაცემების) მთლიანობა, ავტენტურობა, ხელმისაწვდომობა და კონფიდენციალურობა.** მიუხედავად იმისა, რომ NIS დირექტივის მოქმედების არეალი უფრო ფართოა, ვიდრე პერსონალურ მონაცემთა დაცვის უზრუნველყოფა, NIS დირექტივით მოთხოვნილი ინფორმაციული და კიბერპოლიტიკა, უსაფრთხოების სამართლებრივი, პროცედურული, ორგანიზაციულ-ტექნიკური ნორმები მეტწილად იზიარებს როგორც ევროკავშირის მონაცემების დაცვის ზოგადი რეგულაციის (GDPR), ასევე ინფორმაციული უსაფრთხოების კუთხით საერთაშორისო სტანდარტების (ISO, NIST) მიდგომებს მონაცემთა უსაფრთხოების შესახებ და მნიშვნელოვნად უწყობს ხელს პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების ხელშეუხებლობისათვის უსაფრთხო კიბერგარემოს შექმნას.

2) დაახლოებით ანალოგიური პროცესი წარიმართა მონაცემთა დაცვის ჩარჩო რეგულაციასთან დაკავშირებით (GDPR)[2], რომელიც ევროპარლამენტმა ასევე 2016 წელს მიიღო და მისი შესრულება წევრი ქვეყნებისთვის სავალდებულო 2018 წლიდან გახდა. რეგულაცია მიზნად ისახავს ინდივიდების პერსონალური მონაცემების დაცვას და განსაზღვრავს, რომ **უსაფრთხოება არის პერსონალური მონაცემების დამუშავებასთან მიმართებით ერთ-ერთი მთავარი პრინციპი და ასევე მონაცემთა დამმუშავებლის მნიშნველოვანი ვალდებულება.** უფრო კონკრეტულად კი, მონაცემების დამუშავებისას უზრუნველყოფილი უნდა იყოს მათი დაცვა უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვის, განადგურებისა და დაზიანებისგან. რეგულაციას პერსონალურ მონაცემთა დაცვა უფრო მაღალ დონეზე აჰყავს და მიზნად ისახავს ციფრული ტრანსფორმაციისა და ახალი ტექნოლოგიების დანერგვის პირობებში ინდივიდების უფლებების სათანადო დაცვას. რეგულაცია ამკვიდრებს ისეთ ახალ პრინციპებს, როგორიცაა **მონაცემთა დამმუშავებელი ორგანიზაციების ანგარიშვალდებულება, მონაცემთა დამუშავებისას რისკებზე დაფუძნებული მეთოდებისა და პოლიტიკის მიღება, მონაცემთა უსაფრთხოების დარღვევის შეტყობინების ვალდებულება** და სხვა. რეგულაციასთან თანხვედრითად, კიბერსაფრთხეების პრევენციის, გამოვლენის, გამკლავებისთვის გამოყენებული კიბერუსაფრთხოების სისტემები/სერვისები უნდა აკმაყოფილებდეს პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის შესახებ ევროპულ სტანდარტებს და, რა თქმა უნდა, ჩარჩო რეგულაციას.

[2] "Regulation 2016/679. Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," accessed November 11, 2021, http://data.europa.eu/eli/reg/2016/679/oj

მიუხედავად იმისა, რომ GDPR-ის მთავარი ამოსავალია პერსონალური მონაცემებისა და მონაცემთა სუბიექტის უფლებების დაცვა, ამ მიზნის მიღწევა შეუძლებელია უსაფრთხო გარემოს შესაქმნელად აუცილებელი ტექნოლოგიური და ორგანიზაციული ზომების გარეშე. GDPR ქმნის პერსონალური მონაცემების დაცვასთან დაკავშირებით უსაფრთხოების ვალდებულებების ერთობლიობას, რაც პირდაპირ თუ არაპირდაპირ ასახვას ჰპოვებს/უნდა აისახოს კიბერუსაფრთხოების სტრატეგიულ და სამართლებრივ ჩარჩოებში.

ორივე სამართლებრივ ჩარჩოს აქვს საკუთარი ხედვები და მიზნები და ადგენს მათი მიღწევის შესაბამის მექანიზმებს. მათი გავრცელების არეალიც ასევე არსებითად განსხვავდება: თუკი NIS დირექტივა მხოლოდ მნიშვნელოვანი და ციფრული სერვისების მიმწოდებლებზე ვრცელდება, GDPR-ის გავრცელების სუბიექტები გაცილებით ფართოა: ვრცელდება ევროკავშირში რეგისტრირებულ ნებისმიერ ორგანიზაციაზე, რომელიც საქმიანობის ფარგლებში ამუშავებს პერსონალურ მონაცემებს, გარდა ამისა, იმ ორგანიზაციებზეც, რომლებიც არ არიან რეგისტრირებული ევროკავშირში, თუმცა ამუშავებენ ევროკავშირში მყოფი პირების მონაცემებს. თუკი NIS დირექტივა კიბერსივრცეში ყველა ტიპის მონაცემების დაცვაზეა ორიენტირებული, GDPR-ი მხოლოდ პერსონალური მონაცემების ყველა სივრცეში/მედიუმში (ავტომატური, ნახევრადავტომატური, არაავტომატური) დამუშავების შემთხვევებს არეგულირებს.

GDPR-ის მიხედვით, პერსონალური მონაცემების დაცვის უზრუნველსაყოფად, მონაცემთა დამმუშავებლებს ეკისრებათ მონაცემთა უსაფრთხოებასთან დაკავშირებული ვალდებულებების ჩარჩო, რომლებიც მოიცავს როგორც ტექნიკურ, ისე ორგანიზაციულ-პროცედურულ ზომებს, რაც პირდაპირ თუ არაპირდაპირ ხელს უწყობს კიბერუსაფრთხოების გაძლიერებას. კიბერსივრცეში უსაფრთხოების თვალსაზრისით, მონაცემთა დამმუშავებლების ვალდებულებაა მაგალითად მონაცემთა მინიმიზაცია და მონაცემთა შენახვის ვადის შეზღუდვა, მონაცემთა კონფიდენციალურობის უზრუნველყოფა, რისკების შეფასებაზე დაფუძნებული უსაფრთხოების ზომების მიღება, მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში (privacy by design) და მონაცემთა დაცვა პირველად პარამეტრად (privacy by default), უსაფრთხოების ზომების ეფექტიანობის რეგულარული შეფასება, მონაცემთა კომპრომეტირების დროს შეტყობინებებისა და ანგარიშგების, ზიანის შემცირების და გამოსწორების ვალდებულება, ბიზნესუწყვეტობა, მედეგობის ზრდა.

GDPR არ მოიცავს უსაფრთხოების ზომების კონკრეტულ ჩამონათვალს, არამედ მოითხოვს მონაცემების დამმუშავებლებისგან პერსონალური მონაცემების დასაცავად რელევანტური, შესაფერისი, რისკების მართვაზე დაფუძნებული ტექნიკური და ორგანიზაციული ზომების მიღებას. თავად მონაცემთა დამმუშავებლებმა და უფლებამოსილმა პირმა უნდა შეაფასონ დამუშავების ბუნებიდან და მიზნებიდან გამომდინარე არსებული გარემო პირობები, კონტექსტი და პირობები, განსაზღვრონ უსაფრთხოების ზომების გასაწევად აუცილებელი დანახარჯები, მონაცემთა სუბიექტების უფლებათა შეზღუდვის/დარღვევის ალბათობა/სიმწვავე და ყოველივე აღნიშნულის საფუძველზე შეიმუშაონ პეროსნალურ მონაცემთა უსაფრთხოების პოლიტიკა. მაგალითისთვის, GDPR მონაცემთა უსაფრთხოების უზრუნველსაყოფად რამდენიმე ტექნოლოგიური გადაწყვეტილების გამოყენების რეკომენდაციას იძლევა, ასეთია პერსონალურ მონაცემთა ფსევდონიმიზაცია, მონაცემთა დაშიფვრა, ორგანიზაციული კუთხით -

შესაბამისობის სერთიფიცირებისა და შიდაუწყებრივი უსაფრთხოების პოლიტიკის ჩამოყალიბება, ღონისძიებათა ეფექტიანობის რეგულარულ ტესტირება და შეფასება მონაცემთა დამუშავების უსაფრთხოებისათვის.

NIS დირექტივაც GDPR-ის მსგავსად აცხადებს, რომ წევრმა ქვეყნებმა კრიტიკული ინფრასტრუქტურებისთვის (მნიშვნელოვანი სერვისებისა და ციფრული მომსახურების მიმწოდებლები) უსაფრთხოების უზრუნველსაყოფად **თავად უნდა განსაზღვრონ ეფექტური, მორგებული, თავსებადი, პროპორციული, კონკრეტული, გადამოწმებადი და ინკლუზიური ტექნიკური და ორგანიზაციული ზომები**, რათა მართონ ქსელისა და ინფორმაციული სისტემების უსაფრთხოების წინაშე არსებული გამოწვევები, რისკები და საფრთხეები. მათ შორის კი გაითვალისწინონ შემდეგი კომპონენტები: სისტემებისა და მოწყობილობების უსაფრთხოება, ინციდენტების დამუშავება, ბიზნესის უწყვეტობის მენეჯმენტი, მონიტორინგი, აუდიტი და ტესტირება, საერთაშორისო სტანდარტებთან შესაბამისობა.

როგორც NIS დირექტივის, ასევე GDPR-ის ანალიზისას შთაბეჭდილება იქმნება, თითქოს ეს ორივე ჩარჩო ერთმანეთისგან სრულიად დამოუკიდებლად და დაუკავშირებლად განვითარდა. NIS დირექტივის მხოლოდ რამდენიმე მუხლში ვხვდებით ზოგადად მითითებას, რომ ინფორმაციული და კიბერუსაფრთხოების უზრუნველყოფისას პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობა და პერსონალურ მონაცემთა დაცვა GDPR-ის მოთხოვნების შესაბამისად უნდა განხორციელდეს. ასევე მხოლოდ ზოგადი ჩანაწერით შემოიფარგლება კიბერუსაფრთხოების კომპეტენტური ორგანოებისა და მონაცემთა დაცვაზე პასუხისმგებელი უწყების თანამშრომლობის, ინფორმაციის გაცვლის საკითხი კიბერინციდენტის დროს პერსონალური მონაცემების კომპრომეტირებისას. რაც შეეხება GDPR-ს, რეგულაციის ტექსტშიც ასევე ზოგადი ჩანაწერია, რომ ქსელებისა და ინფორმაციული სისტემების უსაფრთხოების, მათზე უნებართვო წვდომის აღკვეთის, მავნე კოდის გავრცელების თავიდან აცილების, და შესაბამისად, ამგვარ სისტემებში არსებული პერსონალური მონაცემების დაცვის მიზნით, CERT/CSIRT-ებს ეძლევათ მონაცემთა დამუშავების ლეგიტიმური ინტერესი და საფუძველი.

მიუხედავად იმის, რომ ორივე სამართლებრივ აქტში ურთიერთმითითებითი ნორმები მწირედ და ისიც ზოგადი ფორმულირებით მოიძებნება, ეს არ ნიშნავს რომ მათი თანაკვეთა პრაქტიკული გამოყენებისას არ ხდება. პირიქით, თუკი ქსელებისა და ინფორმაციული სისტემების საშუალებით პერსონალურ მონაცემთა დამუშავება ხორციელდება, ამ შემთხვევებში გამოიყენება როგორც NIS დირექტივა, ასევე GDPR რეგულაცია. მაგალითისთვის, თუკი კიბერინციდენტისას პერსონალურ მონაცემთა უსაფრთხოების დარღვევას აქვს ადგილი, შეტყობინების ვალდებულება დადგება როგორც მონაცემთა დაცვის უწყებისთვის, ასევე კიბერკომპეტენტური ორგანოს, CERT/CSIRT-სთვის. ამასთანავე ინციდენტმა შესაძლოა გამოიწვიოს როგორც NIS დირექტივის, ასევე GDPR-ის მოთხოვნების დარღვევა და დადგეს სამართალდარღვევისა და სანქციის დაკისრების აუცილებლობა ორივე სამართლებრივი აქტის შესაბამისად.

ვინაიდან ორივე სამართლებრივი აქტი ჯერჯერობით ახალია და მათი იმპლემენტაციის მაგალითებით ევროპული პრაქტიკა ამჟამად ყალიბდება, რთულია პასუხის გაცემა ისეთ

მნიშვნელოვან კითხვაზე, როგორიცაა NIS დირექტივის კონტექსტში განსაზღვრული უსაფრთხოების მოთხოვნების საკმარისობა GDPR-ის მიზნებისთვის პერსონალურ მონაცემთა კიბერსივრცეში დასაცავად. მიუხედავად იმის, რომ ამ საკითხზე დადებითი პასუხის გაცემა ევროპული სამართლებრივი სისტემის წარმატების უპირობო დასტური იქნებოდა, ალბათ მიზანშეწონილი იქნება კიბერსივრცეში პერსონალურ მონაცემთა დასაცავად NIS დირექტივის უსაფრთხოების მოთხოვნების ინდივიდუალურ შემთხვევებზე დაკვირვებით გაანალიზება და ყოველ კონკრეტულ შემთხვევაზე ხარვეზის თუ შესაბამისობის გამოვლენა.

და ბოლოს, უნდა აღინიშნოს, რომ ევროპულ სამართალთან პერსონალურ მონაცემთა დაცვისა და კიბერუსაფრთხოების საკანონმდებლო ბაზის ჰარმონიზაცია და კონსოლიდაცია საქართველოს მიერ ევროპის კავშირთან ასოცირების შეთანხმებითა და ასოცირების დღის წესრიგით ნაკისრ ვალდებულებას წარმოადგენს. ასოცირების შეთანხმების I დანართის თანახმად, საქართველო ვალდებულია უზრუნველყოს პერსონალურ მონაცემთა დაცვის კანონმდებლობის შესაბამისობა ევროკავშირის No 95/46/EC დირექტივასთან, ევროპის საბჭოს 108 კონვენციასთან და მის დამატებით ოქმთან, ასევე, ევროკავშირის 2008 წლის 27 ნოემბრის 2008/977/JHA ჩარჩო გადაწყვეტილებასთან და ევროპის საბჭოს მინისტრთა კომიტეტის 1987 წლის 15 ნოემბრის No R (87)15 რეკომენდაციასთან. რაც შეეხება კიბერუსაფრთხოებას, საქართველოსა და ევროკავშირს შორის ასოცირების დღის წესრიგის შესაბამისად, საქართველო იღებს საშუალოვადიან ვალდებულებას (2022 წელი), რომ მოახდინოს ქსელებისა და ინფორმაციული სისტემების (Network and Information Systems (NIS) უსაფრთხოების შესახებ ევროკავშირის 2016 წლის 6 ივლისის 2016/1148 დირექტივასთან „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ჰარმონიზაცია.

პერსონალურ მონაცემთა კიბერუსაფრთხოება საქართველოს სამართლებრივ სისტემაში

„ინფორმაციული უსაფრთხოების შესახებ“ და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონების ურთიერთმიმართება პერსონალური მონაცემების კიბერსივრცეში დაცვის თვალსაზრისით კვლევისთვის მნიშვნელოვანი მიმართულებაა.

ისევე როგორც NIS-ისა და GDPR-ის შემთხვევაში, საქართველოს საკანონმდებლო აქტებს კიბერუსაფრთხოებისა და პერსონალური მონაცემთა დაცვის შემთხვევაში საკუთარი სამოქმედო არეალი, მიზნები, ამოცანები, პრინციპები, კომპეტენტური ორგანოები და იმპლემენტაციის მეთოდები გააჩნიათ.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი კრიტიკული ინფორმაციული სისტემის სუბიექტებზე ვრცელდება, რომლებიც ამ ეტაპზე მხოლოდ საჯარო სექტორის უწყებებით, ხოლო 2022 წლის 1-ლი იანვრიდან ასევე კერძო სექტორის რიგი წარმომადგენლებებით (სავარაუდოდ ენერგეტიკა, საფინანსო-საბანკო, ჯანდაცვის სფეროს

ორგანიზაციები) შემოიფარგლება. რაც შეეხება „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის გავრცელების სფეროს, იგი პერსონალურ მონაცემთა ყველა დამმუშავებელზე ვრცელდება, როგორც საჯარო, ისე კერძო სამართლის იურიდიულ პირებზე და რიგ შემთხვევებში ფიზიკურ დამმუშავებლებზეც. ამრიგად ამ ეტაპზე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის აღსრულების პერიმეტრი „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონთან შედარებით გაცილებით ფართოა. რაც შეეხება დაცვის ობიექტს, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ამოსავალია კიბერსივრცეში ინფორმაციისა და ინფორმაციული სისტემების უსაფრთხოების, მათი კონფიდენციალობის, ხელმისაწვდომობისა და მთლიანობის უზრუნველყოფა. ინფორმაციული უსაფრთხოება კიბერსივრცეში ყველა ტიპის ინფორმაციული აქტივის და მათ შორის, პერსონალური მონაცემების, უსაფრთხოებას უზრუნველყოფს. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის დაცვის ობიექტია მონაცემთა სუბიექტის პირადი ცხოვრების ხელშუხებლობა და მისი პერსონალური მონაცემები.

GDPR-ის მსგავსად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მონაცემთა დამმუშავებლის მიერ მონაცემთა უსაფრთხოების უზრუნველსაყოფად კონკრეტული ზომების ჩამონათვალის ნაცვლად ზოგად ვალდებულებად დამუშავებასთან დაკავშირებული რისკების (მაგ.: მონაცემების უნებართვო ან უკანონო დამუშავება, შემთხვევითი დაკარგვა, განადგურება და დაზიანება.) შესაბამისი ორგანიზაციულ-ტექნიკური ზომების მიღებას განსაზღვრავს. კანონი ასევე იძლევა კონკრეტულ ინსტრუქციას, მონაცემებთან დაკავშირებული ქმედებების ლოგირების/აღრიცხვის თვალსაზრისით და დამუშავებისას უფლებამოსილების ფარგლების მკაცრი კონტროლის შესახებ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი კიბერგარემოში ტექნოლოგიური საშუალებებით მონაცემთა დამუშავებაზე ნაკლებად არის მორგებული.

თუნდაც 2019 წელს მომზადებული და საქართველოს პარლამენტში რეგისტრირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში ცვლილებების პროექტი[3], მიუხედავად მასში გათვალისწინებული ნოვატორული მიდგომებისა, მონაცემთა დამუშავების უსაფრთხოების თვალსაზრისით კვლავ ზოგადია და ფართო განმარტების საშუალებას უტოვებს ყველა დაინტერესებულ პირს: მონაცემთა სუბიექტს, მონაცემთა დამმუშავებელს, საზედამხედველო ორგანოსაც კი. კანონპროექტის მიხედვით, მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას დამმუშავებელმა და უფლებამოსილმა პირმა უნდა გაითვალისწინონ მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები. ასევე, პერიოდულად შეაფასონ მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით მიღებული ტექნიკური და ორგანიზაციული ზომების ეფექტიანობა და საჭიროების შემთხვევაში, უზრუნველყონ მონაცემთა უსაფრთხოების დაცვისათვის ადეკვატური ზომების მიღება ან/და არსებულის განახლება.

[3] “კანონპროექტი : „პერსონალურ მონაცემთა დაცვის შესახებ,” სახელმწიფო ინსპექტორის სამსახური, მაისი, 2019, https://info.parliament.ge/#law-drafting/18184

2019 წელს მომზადებული და საქართველოს პარლამენტში რეგისტრირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში ცვლილებების პროექტი ასევე პროგრესსულია მონაცემთა კომპრომეტირების შეტყობინების ნაწილში დ შეესაბამება GDPR-ის მოთხოვნებს. კერძოდ, მონაცემთა დამმუშავებელი/უფლებამოსილი პირი ვალდებულია აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები და ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა შეატყობინოს სახელმწიფო ინსპექტორის სამსახურს.

საგულისხმოა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (მუხლი 17.5) პერსონალურ მონაცემთა უსაფრთხოების დაცვის ზომების განსასაზღვრად მითითებას საქართველოს კანონმდებლობაზე აკეთებს. მიუხედავად იმის, რომ ამ მითითებით ნორმაში ზოგადად საქართველოს კანონმდებლობაზე და არა კონკრეტულად ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონზეა აპელირება, ამ უკანასკნელის სამოქმედო არეალიდან გამომდინარე უნდა მივიჩნიოთ, რომ კიბერსივრცეში ინფორმაციულ სისტემებსა და ქსელებში არსებული/დაცული პერსონალური ინფორმაციის უსაფრთხოებისთვის გამოიყენება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით გათვალისწინებული ზომები.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი მონაცემთა უსაფრთხოების უზრუნველსაყოფად ინფორმაციული და კიბერუსაფრთხოების მთელ რიგ ორგანიზაციულ, პროცედურულ და ტექნოლოგიურ მოთხოვნებს ითვალისწინებს, როგორიცაა მაგალითად ინფორმაციული აქტივების ინვენტარიზაცია მათი კრიტიკულობის/სენსიტიურობის გამოვლენისა და შესაბამისი კატეგორიებისთვის (კონფიდენციალური, შინასამსახურებრივი გამოყენების, საჯარო) მართვის (მათ შორის, წვდომის კონტროლის) სისტემის ჩამოყალიბების მიზნით, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შინასამსახურებრივი ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტით განსაზღვრა, ინსტიტუციურ დონეზე უფლებამოსილი/დელეგირებული რგოლის იდენტიფიცირება, ინფორმაციული და კიბერუსაფრთხოების უფლებამოსილი ერთეულების სერტიფიცირება, ინფორმაციული უსაფრთხოების პერიოდული აუდიტი, სისტემებისა და სერვისების შეღწევადობის ტესტირება, ინციდენტების მართვის სისტემა/შეტყობინების ვალდებულება და აშ.

შეჯამებისთვის, როდესაც მონაცემთა დამმუშავებელი ამავდროულად არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, აუცილებელია რომ ინფორმაციულ სისტემებსა/სერვისებში გამოყენებული პერსონალური მონაცემები მკაფიოდ დაიდენტიფიცირდეს (მათ შორის IP მისამართები, მოწყობილობების მაიდენტიფიცირებული მონაცემები, ქსელის ლოგ-ფაილები, წვდომის კონტროლის ლოგ-ფაილები და სხვა) და მათი დაცვისა და უსაფრთხოებისთვის გამოყენებულ იქნას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული დამუშავების პრინციპები და უსაფრთხოების მოთხოვნები (მაგ.: დამუშავების მიზნის შეზღუდვა, შენახვის ვადის შეზღუდვა, მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში (privacy by design) და მონაცემთა დაცვა პირველად პარამეტრად (privacy by default), ისევე როგორც „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული უსაფრთხოების ზომები (მაგ.: უსაფრთხოების პერიოდული აუდიტი,

შეღწევადობის/პენეტრაციის ტესტირება, აქტივების ინვენტარიზაცია და წვდომის კონტროლის განსაზღვრა და ა.შ.).

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის NIS დირექტივასთან კრიტიკული შეუსაბამობები

საქართველოს ევროინტეგრაციასა და ევროპის ერთიანი ციფრული ბაზრისკენ სწრაფვა გულისხმობს ციფრული სფეროს მარეგულირებელი ევროკავშირის უსაფრთხოების მოთხოვნების, NIS დირექტივის ტრანსპოზიციის, ევროპულ სტანდარტებთან და კანონმდებლობასთან ჰარმონიზების ვალდებულებას.

კიბერუსაფრთხოების ევროპული მიდგომების ანალიზისას განსაკუთრებული აქცენტები უნდა გაკეთდეს კიბერუსაფრთხოების თვალსაზრისით ევროკავშირის ძირითად მიდგომებზე, როგორებიცაა:
სახელმწიფოებრივი მიდგომა უნდა აქცენტირდეს კიბერუსაფრთხოების მარეგულირებელი სტანდარტიზებული, ჰორიზონტალური ჩარჩოს, უნიფიცირებული მოთხოვნების დანერგვის სასარგებლოდ და არა ფრაგმენტული, სექტორული, ქაოტური გადაწყვეტილებების მხარდასაჭერად. ევროკავშირის კიბერუსაფრთხოების რეგულირება, უპირველეს ყოვლისა, გულისხმობს კიბერუსაფრთხოების უნიფიცირებულ მიდგომას როგორც მისი წევრი ქვეყნების მიმართ, ასევე რეგულირებას დაქვემდებარებული სექტორების თვალსაზრისითაც.

კიბერსაფრთხეების წინაშე მედეგობის გასაძლიერებლად ევროპული მოდელი გულისხმობს არა რეგულირებადი სექტორების საქმიანობაში ფართომასშტაბიან კონტროლსა და ოპერაციულ დონეზე საზედამხედველო სუბიექტების ჩარევას, არამედ პირიქით, ევროპული მიდგომა დამყარებულია კრიტიკული ინფორმაციული სისტემის სუბიექტების მხრიდან ძლიერი თვითკონტროლის, პრევენციის, დისკრეციის შესაძლებლობებზე და საზედამხედველო ორგანოების მხრიდან ნაკლები ოპერატიული ფუნქციებისა და მეტი სტრატეგიული ამოცანების გადაწყვეტაზე.

კიბრუსაფრთხოების ევროპული მოდელი გულისხმობს კიბერკომპეტენტური ორგანოების მიმართ დელეგირებული უფლებამოსილებების შესრულების პროცესის მკაფიო და განჭვრეტადი სისტემის, ხელისუფლების დანაწილების, კონტროლისა და ბალანსის (checks and balance) არსებობას. კიბერუსაფრთხოების კომპეტენტურ უფლებამოსილებათა საქმიანობის დაბალანსება მხოლოდ გამჭვირვალე, ანგარიშვალდებული, ღია საზედამხედველო ბერკეტებით არის შესაძლებელი.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის NIS დირექტივასთან შესაბამისობის თვალსაზრისით არაერთი შეუსაბამობა ვლინდება,[4] თუმცა აღნიშნულ ანგარიშში გამოვყოფთ რამდენიმე ყველაზე მნიშვნელოვანი შეუთავსებლობის შემთხვევებს:

1) მმართველობითი ჩარჩო არის ხარვეზიანი, არ შეესაამება არანაირ საერთაშორისო მოდელს და კონკრეტული უფლებამოსილი რგოლების ინტერესებზეა მორგებული. ჰორიზონტალურ და ვერტიკალურ დონეებზე უფლებამოსილებების, კომპეტენციებისა და სამოქმედო არეალის გამიჯვნის, კოორდინაციისა და თანამშრომლობის, ინფორმაციის ურთიერთგაცვლის გაურკვეველი, ქაოტური და რთული სურათი, რომელიც აუცილებლად გამოიწვევს უფლებამოსილებებს შორის კონფლიქტს და ასევე, შეიქმნება შემთხვევები, როდესაც ვერ დაინდენტიფიცირდება კონკრეტულ შემთხვევაზე პასუხისმგებელი ორგანო/პირი.

მაგალითი 1: არ არის განსაზღვრული როგორ ახდენენ სექტორული საზედამხედველი ორგანოები ურთიერთთანამშრომლობას და ინფორმაციის ურთიერთგაცვლას. არსებობს თუ არა ქვეყანაში ეროვნულ დონეზე ინციდენტების რეპოზიტორი და ვინ არის მის მართვაზე პასუხისმგებელი? ვინ არის სახელმწიფოს დელეგირებული წარმომადგენელი (SPOC-Single Point of Contact)? ვინ იღებს გადაწყეტილებას მასშტაბური კიბერშეტევების დროს სახელმწიფო კომპეტენტური ორგანოების მობილიზება/საქმიანობის კოორდინაციაზე? ვინ არის პასუხისმგებელი საერთაშორისო არენაზე საქართველოს წარმომადგენლობის კუთხით? ვინ აკეთებს სახელმწიფო აქტორების მიერ საქართველოს წინააღმდეგ მიმართული შეტევების ატრიბუციას? და აშ.

მაგალითი 2: საქართველოს ეროვნული ბანკი, როგორც საბანკო-საფინანსო სექტორზე საზედამხედველო ორგანო, კანონის მიხედვით, იღებს გარკვეულ კვაზი-მარეგულირებელ ფუნქციას კიბერსივრცეში. თუ ეს მოდელი წესია და არა გამონაკლისი, მაშინ რა როლი აქვთ კიბერუსაფრთხოების თვალსაზრისით საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელ ეროვნულ კომისიას (სემეკი), კომუნიკაციების მარეგულირებელ კომისიას, როგორც სექტორულ ზედამხედველებს?

2) კიბერუსაფრთხოების მიმართ ერთიანი სახელმწიფოებრივი მიდგომის (whole-of-nation principle) არარსებობა. ასევე, გაურკვეველია საკანონმდებლო ბაზისა და ეროვნული სტრატეგიული ჩარჩოს ურთიერთმიმართება.

სხვადასხვა კატეგორიის კრიტიკული ინფრასტრუქტურის სუბიექტების მიმართ საზედამხედველო ორგანოები აწესებენ სექტორულ ინფორმაციულ და კიბერუსაფრთხოების მოთხოვნებს, როგორებიცაა მაგალითად, აუდიტის ჩატარების წესი, ინციდენტების კლასიფიცირება და აშ. თუკი ამ კანონქვემდებარე აქტების პროექტების შექმნის პროცესში არ მოხდა კოორდინირებული მუშაობა და მეტ-ნაკლებად სტანდარტული ინფორმაციული და კიბერუსაფრთხოების მოთხოვნების ჩამოყალიბდა, შედეგად მივიღებთ განსხვავებულ რეჟიმებს

[4] “კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები | IDFI,” აგვისტო, 2020, https://idfi.ge/public/upload/GG/CyberN222.pdf

და პრაქტიკას. იმ დროს როცა ევროკავშირი არათუ სექტორებს შორის ჰარმონიზებულ მიდგომას, არამედ ქვეყნებს შორის ერთიანი სტრატეგიული, ოპერატიული და პროცედურული ჩარჩოს დანერგვას ავალდებულებს წევრ სახელმწიფოებს.

NIS დირექტივის მიხედვით, ქვეყნების სტრატეგიული და საკანონმდებლო ჩარჩოები ურთიერთმიმართებით და ურთიერთმითითებით უნდა შემუშავდეს და აღსრულდეს. როგორც NIS დირექტივა, ისევე მისი განახლების შესახებ ევროკავშირის ახალი პროექტი (NIS 2) პირდაპირ უთითებს, სულ მცირე, რა საკითხები უნდა იქნას დაფარული სტრატეგიით. საქართველოს „ინფორმაციული უსაფრთხოების შესახებ“ კანონი კიბერუსაფრთხოების სტრატეგიაზე და მის აუცილებელ კომპონენტებზე მითითებას არ აკეთებს. აქვე საყურადღებოა, რომ კიბერუსაფრთხოების ეროვნული სტრატეგია, როგორც ქვეყნის ერთიანი ხედვისა და ხელისუფლების ნების გამომხატველი მთავარი პოლიტიკური დოკუმენტი, სამწლიანი პაუზის შემდეგ, მხოლოდ ზემოხსენებულ კანონში შეტანილი ცვლილებების შემდეგ დამტკიცდა.[5] თუმცა, ინსიტუციულ-ორგანიზაციული მმართველობითი მოდელის განსაზღვრა არც ამ ახალი სტრატეგიით მომხდარა. არსებული მდგომარეობა კიდევ უფრო ართულებს კანონისა და სტრატეგიის ურთიერთშესაბამისობის და თანხვედრადობის საკითხს, ვინაიდან კანონი სწორედ რომ ერთ-ერთი მექანიზმია სტრატეგიული ხედვების, მიზნებისა და ამოცანების გადასაწყვეტად და სტრატეგიაში მმართველობითი მოდელის არარსებობის ფონზე „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ახალი რედაქციის დამტკიცება არაერთ მნიშვნელოვან საკითხს ბუნდოვანს ტოვებს.

3) კრიტიკული ინფორმაციული სისტემის სუბიექტების შესაბამის საზედამხედველო სტრუქტურებთან მიკუთვნების არსებული მოდელითა და განსხვავებული სექტორული სტანდარტების/მოთხოვნების დაწესებით, ქვეყანაში **კიბერუსაფრთხოების არაერთგვაროვანი სურათის/შედეგების მიღების საფრთხე.**

NIS დირექტივის მიხედვით, კრიტიკული ინფორმაციული სისტემის სუბიექტების იდენტიფიცირება ხდება არა მათი სამართლებრივი ფორმით (საჯარო სამართლის თუ კერძო სამართლის იურიდიული პირი), არამედ მათი სექტორული მიკუთვნების მიხედვით.[6] ასევე მათი საზედამხედველო რეჟიმი უნიფიცირებულია და არა სექტორულად დაყოფილი.
მაგალითად: თუკი სემეკი გახდა კიბერშეტევის სამიზნე, მასზე გავრცელდება პირველი კატეგორიის სუბიექტისთვის განსაზღვრული რეჟიმი და იგი დაექვემდებარება სახელმწიფო უსაფრთხოების სამსახურის დაქვემდებარებაში მყოფი, ოპერატიულ-ტექნიკური სააგენტოს (OTA) რეგულირებას. ამავე დროს ენერგეტიკული კომპანიის მიმართ (მაგ.: თელასი) ანალოგიურ

[5] “საქართველოს მთავრობის დადგენილება №482 საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ,” სექტემბერი, 2021, https://matsne.gov.ge/document/view/5263611?publication=0

[6] NIS დირექტივის მიხედვით, მნიშვნელოვანი სერვისის მიმწოდებლების იდენტიფიცირებისთვის განსაზღვრულია როგორც ჰორიზონტალური კრიტერიუმები (ინფორმაციული სისტემის კომპრომეტირებისას ზიანის/ზარალის მოცულობა, ბაზრის წილი, გეოგრაფიული გავრცელების არეალი, მომხმარებელთა რაოდენობა), ასევე სპეციფიური სექტორული განზომილებების დაწესების შესაძლებლობა.

შემთხვევაში გავრცელდება ციფრული მმართველობის სააგენტოს საზედამხედველო მოთხოვნები, ხოლო თუკი ენერგეტიკული კომპანია სახელმწიფო წილობრივი მონაწილეობითი ფორმისაა (მაგ.: სახელმწიფო ელექტროსისტემა), მასზე ასევე OTA-ს რეჟიმი გამოიყენება. ასეთი მმართველობითი ჩარჩოთი კონკრეტულ ერთ სექტორშიც კი იქმნება ინფორმაციის დროული გაცვლისა და სექტორული კიბერმედეგობის შესუსტების რისკი.

თუკი კატეგორიების მიხედვით დაწესდება განსხვავებული მოთხოვნები და აღსრულების მექანიზმები, ეს რა თქმა უნდა, გამოიწვევს სექტორებს შორის ინფორმაციული და კიბრუსაფრთხოების დანერგვის განსხვავებულ შედეგს. შესაბამისად, საზედამხედველო უწყებების საქმიანობის ეფექტიანობა და წარმატებაც განსხვავებული იქნება მათი კონტროლისა და მონიტორინგის ბერკეტების პროპორციულად. და რაც მთავარია, ეს ყოველივე გავლენას მოახდენს ქვეყანაში კიბერუსაფრთხოების მდგრადი, ერთიანი და პროგნოზირებადი გარემოს შექმნაზე, რაც ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მთავარი მიზანია.

4) გადამეტებული კონტროლისა და ზედამხედველობის რეჟიმი

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული საზედამხედველო მოდელი კრიტიკული ინფრასტრუქტურების კიბერმედეგობისა და თვითგაძლიერების ნაცვლად ხშირ შემთხვევაში ზედამხედველი სუბიექტის მიერ პირდაპირ ოპერატიულ საქმიანობაში ჩარევას და სადავეების საკუთარ ხელში აღებას გულისხმობს. საზედამხედველო ორგანოების მხრიდან ზედამხედველობის რეჟიმი დასულია ყოველდღიურ ოპერატიულ დონეზე, კრიტიკული ინფორმაციული სისტემების წვდომისა და კონტროლის აქტივობებზე. NIS-ის შემთხვევაში მთავარი აქცენტი არის სუბიქტების მხარდაჭერა, გაძლიერება და არა მათ ნაცვლად კიბერშეტევების მართვა. NIS დირექტივა ემყარება დაბალანსებულ და პროპორციულ ტექნიკურ და ორგანიზაციულ ღონისძიებებს. შესაბამისად, საზედამხედვლო ორგანოების მხრიდან რეგულირების დროს ასევე უნდა იყოს დაცული პროპორციულობის, ბალანსისა და აუცილებლობის პრინციპები.

5) რისკების მართვაზე დაფუძნებული მიდგომის არარსებობა

„ინფორმაციული უსაფრთხოების შესახებ“ შეცვლილი კანონის, ისევე როგორც მანამდე არსებული რედაქციის შემთხვევაში, ინფორმაციული აქტივების მართვის, თუ ინფორმაციული და კიბერუსაფრთხოების პოლიტიკის წარმართვისას არ იყო და ახლაც არ არის გათვალისწინებული რისკებზე დაფუძნებული მიდგომა. ამ დროს, NIS დირექტივაც, ევროკავშირის ახალი NIS2 შემოთავაზებაც რისკებზე დაფუძნებით გადაწყვეტილებების მიღებისა და მართვის პროცესს ინფორმაციული უსაფრთხოების მართვის სისტემების მთავარ ქვაკუთხედად მიიჩნევს.

პერსონალურ მონაცემთა კიბერუსაფრთხოების თვალსაზრისით „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ნაკლოვანებები

საქართველოს კანონში „ინფორმაციული უსაფრთხოების შესახებ“ არ იძებნება ჩანაწერი, სადაც საუბარია პირადი ცხოვრების ხელშეუხებლობასა და პერსონალურ მონაცემთა დაცვაზე. კანონით არ არის მოწესრიგებული საზედამხედველო უწყების თუ კრიტიკული ინფორმაციული სისტემის სუბიექტის ვალდებულება მონაცემებზე წვდომის თუ სხვაგვარი დამუშვებისას პერსონალურ მონაცემთა დაცვის შესაბამისი ზომების მიღების/ეფექტური მექანიზმების დანერგვის შესახებ.

1) ქსელური მონიტორინგის სისტემა

„ინფორმაციის უსაფრთხოების შესახებ“ საქართველოს კანონი კითხვებს აჩენს პერსონალურ მონაცემთა დაცვის შესაძლო დარღვევის შესახებ ქსელურ სენსორთან მიმართებით. ქსელური სენსორი, მისი მახასიათებლების - წვდომის შესაძლებლობის - გათვალისწინებით, სენსიტიური ტექნოლოგიაა, ვინაიდან მისი გამოყენებით პერსონალურ მონაცემთა დამუშავების წესების დარღვევის შესაძლებლობა მაღალია. შესაბამისად ქსელური სენსორის კონფიგურირების წესები უნდა განსაზღვრავდეს ყველა აუცილებელ გარანტიას, რომ სენსორული მოწყობილობების გამოყენებისას მონაცემთა დამუშავების ყველა წესი იქნება შესაბამისად დაცული.

ერთი მხრივ, „ინფორმაციული უსაფრთხოების კანონის” მე-2 მუხლის განმარტება გულისხმობს, რომ ქსელური სენსორის მიზანი არ არის სისტემის საშუალებით შენახულ ან გადაცემულ ინფორმაციაზე წვდომა, არამედ იგი გამიზნულია უმთავრესად ინფორმაციული სისტემების წინააღმდეგ მიმართული კომპიუტერული ინციდენტების გამოსავლენად. ეს მიდგომა ასევე განმტკიცებულია მე-4 მუხლის მე-4 პუნქტითაც, რომელიც ადგენს, რომ „ოპერატიულ-ტექნიკურ სააგენტოს, ციფრული მმართველობის სააგენტოს და კიბერუსაფრთხოების ბიუროს ხელი არ მიუწვდებათ კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციასა და ინფორმაციულ აქტივზე (გარდა ამ კანონით გათვალისწინებული შემთხვევებისა)“. თუმცა, მეორე მხრივ, სამართლიანად აღსანიშნავია, რომ კანონის ჩანაწერი - ,,ქსელური სენსორი კომუნიკაციის შინაარსობრივი მონაცემის ხელმისაწვდომობის შესაძლებლობას უნდა გამორიცხავდეს“ - არ წარმოადგენს სამართლებრივ გარანტიას, რომ ქსელური სენსორების დაყენებისთანავე მათი ბოროტად გამოყენება არ მოხდება/შეუძლებელი იქნება პერსონალურ ინფორმაციაზე ხელმისაწვდომობის მოპოვება. აგრეთვე, ქსელური სენსორის კონფიგურირების წესების კანონქვემდებარე აქტით სამომავლოდ განსაზღვრა ამ საკითხებს პასუხგაუცემლად ტოვებს.

აღნიშნული საკითხების რეგულირება უნდა მოხდეს მკაფიო და არაორაზროვანი ნორმებით, რომლებიც კოდიფიცირდება კანონით და არა კანონის მიღების შემდეგ მის საფუძველზე სამომავლოდ შესამუშავებელი კანონქვემდებარე აქტების ქოლგის ქვეშ. მნიშვნელოვანია აღინიშნოს, რომ კანონქვემდებარე აქტებით დადგენილი წესები შესაძლოა ხშირად, მარტივად

და არაპროგნოზირებადად შეიცვალოს გარეშე პირთა მიერ დეტალური ანალიზისა და კრიტიკის ნაკლები შესაძლებლობით. გარდა ამისა, ქსელური მონიტორინგის სისტემის ფუნქციონირებაზე დამოუკიდებელი და მიუკერძოებელი საზედამხედველო რგოლის არსებობა კრიტიკულად მნიშვნელოვანია.

2) პერსონალურ მონაცემთა კომპრომეტირებისას შეტყობინებების ვალდებულება

ხშირ შემთხვევაში, კიბერინციდენტების შედეგად ხდება პერსონალური მონაცემების კომპრომეტირება. შესაბამისად, ოპერატიულ-ტექნიკურმა სააგენტომ და ციფრული მმართველობის სააგენტომ, ისევე როგორც კანონით გათვალისწინებულმა კიბერუსაფრთხოების სხვა კომპეტენტურმა ორგანოებმა, უნდა ითანამშრომლონ სახელმწიფო ინსპექტორის სამსახურთან, რათა თავიდან იქნეს აცილებული კიბერსივრცეში პერსონალურ მონაცემთა ხელყოფა, დროულად და ეფექტიანად გაცვალონ ინფორმაცია ინციდენტის შედეგად პერსონალურ მონაცემთა ხელყოფის შესახებ და ერთობლივად იმუშაონ მძიმე შედეგების მინიმიზაციისა და ზიანის შემსუბუქებისთვის.

შედარებისთვის GDPR-ის მიხედვით, თუ ირღვევა პერსონალურ მონაცემთა უსაფრთხოება, დამმუშავებელმა დარღვევის აღმოჩენიდან არაუგვიანეს 72 საათისა უნდა შეატყობინოს პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელ ორგანოს და იმ პირებს, რომელთაც შეეხოთ აღნიშნული ინციდენტი. ამასთან, იმ შემთხვევაში, თუ პერსონალურ მონაცემთა უსაფრთხოების დარღვევას თან ახლავს კიბერინციდენტი, მისი შეტყობინება ხორციელდება NIS დირექტივით გაწერილი პროცედურების შესაბამისად. დამმუშავებლები ვალდებულნი არიან აღრიცხონ მონაცემთა უსაფრთხოების დარღვევის ყველა შემთხვევა და მიღებული ზომები. მათ ასევე ევალებათ მონაცემთა უსაფრთხოების პოლიტიკის შემუშავება, ინციდენტების გამოვლენისა და მათზე რეაგირების გეგმები. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი არ ცნობს კიბერინციდენტისას პერსონალურ მონაცემთა დარღვევის ფაქტების შემთხვევაში ამგვარ რეგულირებებს და ზოგადად, არ განსაზღვრავს სახელმწიფო ინსპექტორის აპარატთან ინფორმაციის ურთიერთგაცვლისა და თანამშრომლობის სხვა ფორმების შესაძლებლობებს.

გარდა ამისა, NIS დირექტივა ხაზგასმით აღნიშნავს, რომ კრიტიკული სუბიექტების მიერ CERT/CSIRT-ებისთვის ინციდენტების შეტყობინება შესაძლოა მოითხოვდეს პერსონალური ინფორმაციის დამუშავებას და ასეთი დამუშავება შესაბამისობაში უნდა მოდიოდეს GDPR-ის და ePrivacy დირექტივის მოთხოვნებთან. გაცვლილი ინფორმაცია უნდა შემოიფარგლებოდეს მხოლოდ იმ მონაცემებით, რომელიც შესაბამისი და პროპორციულია ამგვარი გაცვლის მიზნისათვის. ინფორმაციის ასეთი გაცვლისას შენარჩუნებული უნდა იყოს ინფორმაციის კონფიდენციალურობა, მისი დამმუშავებლების უსაფრთხოება და კომერციული ინტერესები. ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი ასევე არ ცნობს კიბერინციდენტის CERT/CSIRT-ებისთვის შეტყობინებისას ამგვარ დანაწესს.

3) კანონის უზენაესობის უზრუნველყოფა, კრიტიკული ინფორმაციული სისტემის სუბიექტებიდან ინფორმაციის (მათ შორის, პერსონალური მონაცემების) გამოთხოვისას, **ინფორმაციაზე წვდომის მოპოვებისას მიზნობრიობის, პროპორციულობისა და აუცილებლობის პრინციპების დაცვა**

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის არაერთი ნორმა ოპერატიულ-ტექნიკური სააგენტოს, ციფრული მმართველობის სააგენტოსა და კიბერუსაფრთხოების ბიუროს საკუთარ საზედამხედველო სექტორებში ინფორმაციულ აქტივზე პირდაპირი წვდომისა და ინფორმაციის სავალდებულო წესით გამოთხოვის ბერკეტებს აძლევს. მაგალითად: ისინი უფლებამოსილი არიან კრიტიკული ინფორმაციული სისტემის სუბიექტისგან მოიპოვონ არა მხოლოდ ინფორმაციული უსაფრთხოების პოლიტიკა შესაბამისი შინასამსახურებრივი წესებით, არამედ ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებასთან, დანერგვასთან, მონიტორინგსა და გაუმჯობესებასთან დაკავშირებული ნებისმიერი სხვაგვარი ინფორმაცია, ხოლო მათი დამუშავების შემდეგ გასცენ სავალდებულოდ შესასრულებელი მითითებები. მიუხედავად იმის, რომ საზედამხედველო უფლებამოსილების განხორციელებისას წვდომა-დაშვება არ ახალია როგორც მოქმედი NIS დირექტივისთვის, ასევე მისი გაუმჯობესების მიზნით შემუშავებული NIS2 დირექტივის პროექტით, ეს უფლებამოსილებები შესაბამისი კონტროლისა და საზედამხედველო ბერკეტების გარეშე არ არსებობს. უფრო კონრეტულად, NIS დირექტივის მე-15 (2) მუხლში მითითებულია, რომ: „ინფორმაციის ან მტკიცებულების მოთხოვნისას კომპეტენტურმა ორგანომ უნდა დაასაბუთოს მოთხოვნის მიზანი და დააკონკრეტოს ინფორმაცია, რომლის გამოთხოვაც საჭიროდ მიაჩნია“. ყველა ასეთი მოთხოვნა უნდა ითვალისწინებდეს ევროკავშირის ფუნდამენტური უფლებების ქარტიის მოთხოვნებს, მათ შორის ეფექტური სასამართლო დაცვის, პროპორციულობისა და ინდივიდუალურად საქმის გარემოებების შეფასების პრინციპებს. ამგვარი წესრიგი ვრცელდება კიბერსივრცეში ყველა ტიპის სამეთვალყურეო მექანიზმსა და აღსრულების ღონისძიებებზე.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მიერ OTA-სთვის მინიჭებული მანდატით, იზრდება პირველი (საჯარო დაწესებულებები) და მეორე კატეგორიის (სატელეკომუნიკაციო კომპანიები) სუბიექტების ინფორმაციულ აქტივებზე დაუსაბუთებელი წვდომისა და დაცული ინფორმაციის დამუშავების რისკი, რამდენადაც, OTA-ს ენიჭება სამართლებრივი ბერკეტი, სასამართლოს ნებართვის გარეშე ჰქონდეს პირდაპირი წვდომა სახელმწიფო ორგანოებისა და სატელეკომუნიკაციო სექტორის ნებისმიერ წარმომადგენლის ინფორმაციულ სისტემებზე და არაპირდაპირი წვდომა სისტემებში დაცულ პერსონალურ და სხვაგვარად სენსიტიურ ინფორმაციაზე.

მნიშვნელოვანია, რომ კანონით განსაზღვრული იყოს პროცედურული თუ სამართლებრივი პროტოკოლი, რომელთა დაკმაყოფილების შემთხვევაში, დაშვების აუცილებლობა დასაბუთებული იქნება საზედამხედველო სუბიექტების მიერ და მხოლოდ შემდეგ განხორციელდება წვდომა. წინააღმდეგ შემთხვევაში, OTA-ს მიერ მხოლოდ ზოგადი გაცხადებით, რომ არსებობს საფრთხე და მას ესაჭიროება წვდომის განხორციელება, პირველი კატეგორიის სუბიექტებს ამ მოთხოვნის დაუყოვნებლივ აღსრულება მოუწევთ.

4) კიბერუსაფრთხოების კომპეტენტური ორანოების მიერ საქმიანობის განხორციელებისას **უფლებამოსილების გადამეტების შემთხვევებზე მკაფიო და ჩამოყალიბებული საზედამხედველო მექანიზმებისა და მაკონტროლებელი ჩარჩოები**

კანონი ღიად ტოვებს OTA-ს უფლებამოსილების კონტროლისა და ზედამხედველობის მექანიზმებს, და არ განსაზღვრავს კონკრეტული გარანტიებსა და პროცედურულ ბერკეტებს. ინფორმაციული და კიბერუსაფრთხოების სფეროებში დელეგირებული უფლებამოსილებების განახორციელებისას, დეტალურად შესასწავლი და გასაანალიზებელია OTA-ს მიმართ ზედამხედველობის ყველა არსებული და შესაძლო მექანიზმი (საპარლამენტო, სასამართლო, საპროკურორო, სახელმწიფო ინსპექტორის მიერ შემოწმება, შიდა აუდიტი თუ სხვა შესაძლო ბერკეტები), იმისთვის რომ უზრუნველყოფილ იქნას მისი სრულყოფილი და ეფექტური ზედამხედველობა. აქვე მნიშვნელოვანია აღინიშნოს, რომ მხოლოდ და მხოლოდ მითითებითი ნორმების დამატება კანონში ამა თუ იმ საზედამხედველო მანდატზე არ არის ამ ამოცანის გადაწყვეტა. არამედ, აუცილებელია გაიწეროს ყველა ის პროცედურული, ორგანიზაციული თუ ტექნიკური ბერკეტები, რომლებიც დასაბუთებულად და არაორაზროვნად გახდის OTA-ს ზედამხედველობისა და კონტროლის ობიექტად, ხოლო ამ უკანასკნელის მხრიდან არ დარჩება სამართლებრივი თუ სხვაგვარი საშუალება უფლებამოსილების გადამეტების, კომპეტენციის ბოროტად გამოყენების და ინფორმაციული უსაფრთხოების მანდატის ქვეშ სხვაგვარი უკანონო საქმიანობის.

შეჯამება

საქართველოში ბოლო ათწლეულის განმავლობაში კიბერუსაფრთხოებისა და პერსონალური მონაცემების დაცვის სტანდარტები როგორც საკანონდებლო, ასევე, პრაქტიკული იმპლემენტაციის დონეზე, მნიშვნელოვნად განვითარდა. ორივე მიმართულებით ქვეყანაში ჩამოყალიბდა ორგანიზაციულ-ინსტიტუციური ჩარჩო, ამაღლდა ამ დარგებში მოღვაწე სპეციალისტების კვალიფიკაცია, შეიქმნა შესაბამისი სტრატეგიული და საკანონმდებლო ჩარჩოები, რომლებმაც რეგულირებასთან ერთად კიბერუსაფრთხობისა და პერსონალურ მონაცემთა დაცვის განვითარებისთვის ხელსაყრელი გარემო პირობები უნდა შექმნას.

კიბერუსაფრთხოებისა და პერსონალური მონაცემების დაცვის სტანდარტების განვითარების მიუხედავად, გლობალური გამოწვევების, კიბერუსაფრთოებისა და პერსონალურ მონაცემთა დაცვის მიმართულებების დინამიურობის გათვალისწინებით, ამ სფეროებში კვლავ რჩება მრავალი გამოწვევა, როგორც კერძო, ასევე, საჯარო სტრუქტურებში. აღნიშნულის საილუსტრაციოდ, ნათელი მაგალითია სახელმწიფო ინსპექტორის აპარატის 2020 წლის საქამიანობის ანგარიში, რომლის მიხედვითაც მონაცემთა უსაფრთხოების ზომებთან დაკავშირებული დარღვევები 2019 წელთან შედარებით 10%ით გაიზარდა.[7]

[7] პერსონალურ მონაცემთა დაცვის სფეროში ბოლო პერიოდში განვითარებული მოვლენების მოკლე მიმოხილვა | IDFI," მაისი, 2021, https://bit.ly/3oEGcn8

საქართველომ, როგორც ევროპული სამართლებრივი კულტურისა და ევროპული ინტეგრაციის პროცესში მყოფმა ქვეყანამ, ევროპულ მარეგულირებელ სტანდარტებთან შიდა კანონმდებლობის დაახლოების გზა უფრო მეტი ძალისხმევით უნდა განაგრძოს. კიბერუსაფრთხოებისა და პერსონალურ მონაცემთა დაცვის ევროპული სტანდარტების დანერგვა საქართველოსთვის კიდევ ერთი წინგადადგმული ნაბიჯი იქნება ევროპის ერთიან ციფრულ ბაზარზე ინტეგრაციისთვის, საქართველოს მოქალაქეები კი კიბერსივრცეში უზრუნველყოფილნი იქნებიან უსაფრთხოების მაღალი სტანდარტით, პერსონალური მონაცემის დამუშავებისას ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის ეფექტიანი და ქმედითი დაცვის მექანიზმებით.

რეკომენდაციები

● „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში **მკაფიოდ უნდა განისაზღვროს,** რომ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულ საკითხებზე, მათ შორის პერსონალურ მონაცემთა უსაფრთხოების დარღვევის ან/და კიბერინციდენტის დროს, **თუ როგორ თანამშრომლობს კიბერუსაფრთხოების კომპეტენტური ორგანო სახელმწიფო ინსპექტორის აპარატთან.** ჩამოყალიბდეს **ინფორმაციის ურთიერთგაცვლის პროტოკოლი და სამართლებრივ-პროცედურული ნორმები**. ინციდენტთან დაკავშირებული პერსონალური მონაცემების კომპრომეტირების შესახებ შეტყობინების პროცესის სწორად დასაგეგმად, მნიშვნელოვანია ე.წ. „table top” სავარჯიშოებითა და შესაბამისი ტრენინგებით უფლებამოსილი ორგანოების გაძლიერება.

● ,,„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში **კრიტიკული ინფორმაციული სისტემების სუბიექტების იდენტიფიცირების მკაფიო და განსაზღვრული წესი/კრიტერიუმები უნდა არსებობდეს**, რომელსაც შესაძლოა სექტორული მახასიათებლები ემატებოდეს. კანონმდებლობის დონეზე მეტი სიცხადე სუბიექტური დისკრეციის ნაკლებ შესაძლებლობას დაუტოვებს უფლებამოსილ ორგანოებს და სექტორებს მდგრადობის და განჭვრეტადობის მეტ შესაძლებლობას მისცემს. კრიტიკული სექტორების კანონის დონეზე განსაზღვრა ევროკავშირის არაერთი ქვეყნის, მაგალითად ესტონეთის, დადგენილ პრაქტიკას წარმოადგენს.

● მიზანშეწონილია, რომ საქართველოს სამართლებრივ სისტემაში („ინფორმაციული უსაფრთხოების შესახებ“ ან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონებით) **დაკონკრეტდეს ორგანიზაციულ-ტექნიკური ზომების ჩამონათვალი,** მათი დანიშნულება (მაგ.: მონაცემთა მთლიანობის, ხელმისაწვდომობისა და კონფიდენციალობის უზრუნველყოფა) ან უფრო დეტალური მოთხოვნები (მაგ.: სერტიფიცირებული სისტემების

გამოყენება, მონაცემთა დაცვის შიდა პოლიტიკის დოკუმენტების - შინაგანაწესის შემუშავება), რომელთა დანერგვაც უზრუნველყოფს პერსონალურ მონაცემთა კიბერუსაფრთხოებას.

● მნიშვნელოვანია დეტალური ანალიზის განხორციელება იმის შესახებ, თუ რამდენად პასუხობს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნებს მონაცემთა კიბერსივრცეში უსაფრთხოების ჭრილში „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი და აღნიშნული ანალიზის საფუძველზე, სულ მცირე, **კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის, მკაფიოდ იქნება იდენტიფიცირებული კიბერსივრცეში პერსონალური მონაცემების უსაფრთხოების უზრუნველყოფისთვის რა სტანდარტებით უნდა იხელმძღვანელონ.** კერძოდ, საკმარისი არის თუ არა ISO 27001, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების და კიბერუსაფრთხოების სერვისების დანერგა კიბერსივრცეში პერსონალური მონაცემების დაცვისთვის.

● ვინაიდან კიბერსივრცეში პერსონალურ მონაცემთა დაცვის თვალსაზრისით „პერსონალურ მონაცემთა დაცვის შესახებ“ და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონებს, მათი მიზნებისა და სამოქმედო არეალის განსხვავებულობის მიუხედავად, მნიშვნელოვანი სამართლებრივი და პრაქტიკული თანაკვეთა აქვს, მიზანშეწონილია ამ სფეროების უფლებამოსილი ორგანოების საქმიანობის ურთიერთდაახლოება, მეტი ინტენსივობით **თანამშრომლობა და ქმედებების კოორდინირებულად წარმართვა.** თანამშრომლობისთვის პირველად დონეზე აუცილებელი სფეროებია: აუდიტის პროცესის კონკრეტული მიმართულებების კოორდინირება, ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების სპეციალისტების, პერსონალურ მონაცემთა დაცვის თანამშრომლების გადამზადება ურთიერთთანაკვეთ საკითხებში, ცოდნის ამაღლება პერსონალური მონაცემების დამუშავების მიმართ მოთხოვნების შესახებ, ინფორმაციის ურთიერთგაცვლა.