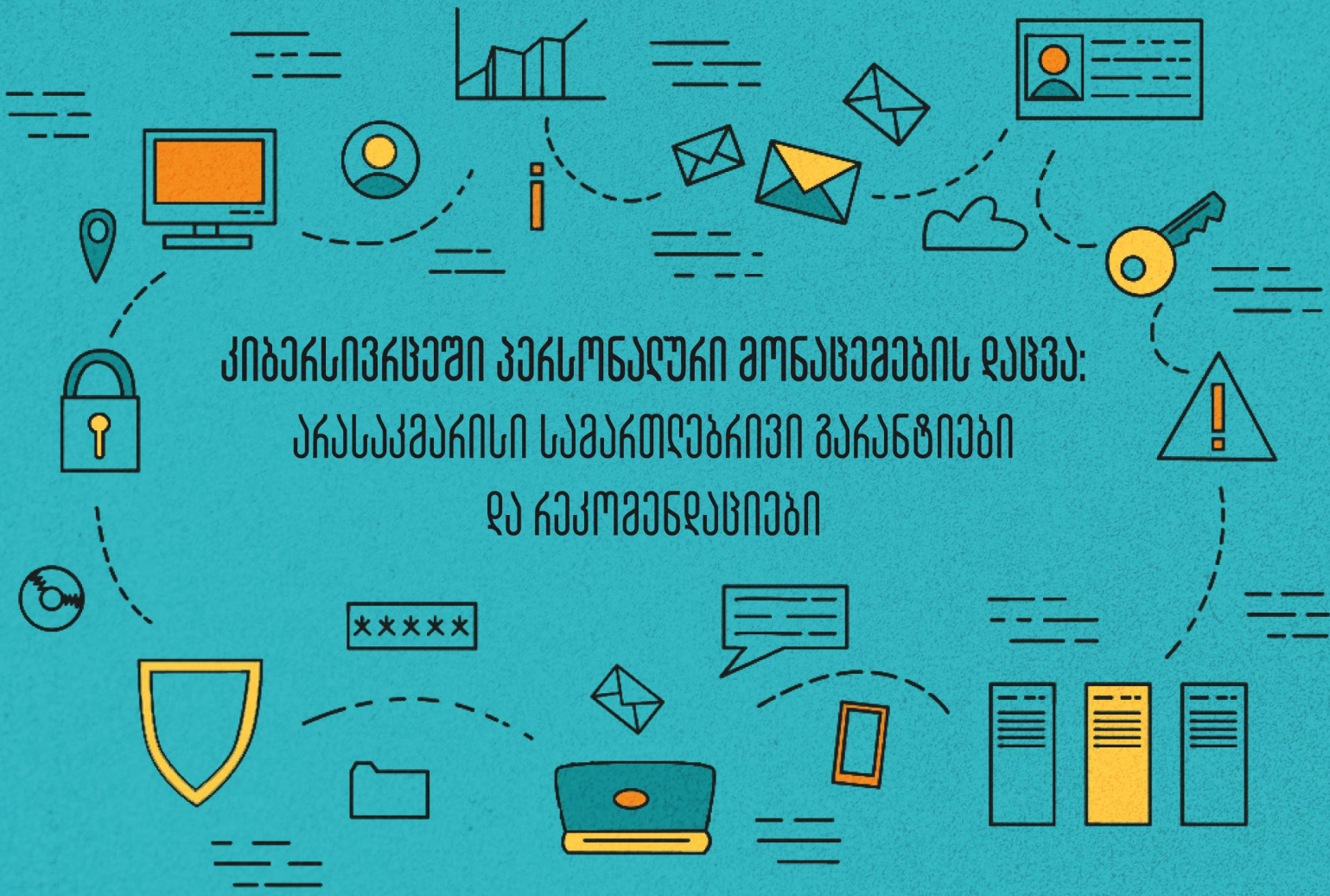
IDFI

ინფორმაციის თავისუფლების
განვითარების ინსტიტუტი



კიბერსივრცეში პერსონალური მონაცემების დაცვა: არასაკმარისი სამართლებრივი გარანტიები და რეკომენდაციები

თბილისი, 2022

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

2022

შესავალი

ციფრული ტრანსფორმაციის ეპოქაში იზრდება როგორც სახელმწიფო და კომერციული ელექტრონული სერვისების, ასევე მათი მომხმარებელთა რაოდენობა. მოქალაქეების პერსონალური მონაცემების მნიშვნელოვანი ნაწილი სწორედ ამგვარ ინფორმაციულ სისტემებში, ელექტრონულ რეესტრებსა და საკომუნიკაციო ქსელებში გროვდება. მათში დაცული მონაცემების მოცულობის გამო ამგვარი სისტემები და მოწყობილობები ყველაზე ხშირად ხდებიან კიბერშეტევების ობიექტები.

ციფრული გარემოს კიბერუსაფრთხოების უზრუნველყოფასთან დაკავშირებული გამოწვევები საქართველოსთვის ახალი არაა. 2008 წლის რუსეთ–საქართველოს ომის დროს განხორციელებულმა კიბერშეტევებმა, რომელთა მთავარ სამიზნესაც სამთავრობო უწყებები და მედია საშუალებები წარმოადგენდა, საგრძნობლად დააზიანა ქვეყნის კრიტიკული ინფრასტრუქტურა. საპასუხოდ, ქვეყანამ მიიღო კანონი „ინფორმაციული უსაფრთხოების შესახებ“, შექმნა კიბერუსაფრთხოებაზე პასუხისმგებელი უწყება და კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი. მნიშვნელოვანი პროგრესის მიუხედავად, ბოლო წლების კიბერშეტევებმა აჩვენა, რომ როგორც სამთავრობო, ასევე კერძო სექტორი კვლავაც მოწყვლადია კიბერშეტევების მიმართ. ერთ-ერთი ბოლო, საჯაროდ ცნობილი მასშტაბური შემთხვევა 2020 წლის სექტემბერში მოხდა, როდესაც უცხო ქვეყნიდან საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს კომპიუტერულ სისტემაზე განხორციელდა კიბერშეტევა.[1] მიზანი სამინისტროს ცენტრალურ აპარატსა და მის სტრუქტურულ ერთეულებში, მათ შორის, დაავადებათა კონტროლისა და რიჩარდ ლუგარის სახელობის საზოგადოებრივი ჯანდაცვის კვლევითი ცენტრის მონაცემთა ბაზებში დაცული სამედიცინო ხასიათის დოკუმენტაციისა და პანდემიის მართვასთან დაკავშირებული მნიშვნელოვანი ინფორმაციის დაუფლება და გამოყენება იყო. მანამდე, იმავე წლის მარტში მილიონობით საქართველოს მოქალაქის პირადი ინფორმაცია (მათ შორის, პირადი ნომრები, დაბადების თარიღი, მობილური ტელეფონი, მისამართი) აიტვირთა ჰაკერულ ფორუმზე. მოგვიანებით აღმოჩნდა, რომ აღნიშნული ბაზები 2011 წელს გაჟონილ ინფორმაციას მოიცავდა.[2] ეს გარემოებები ხაზს უსვამს, რამდენად მნიშვნელოვანია კიბერუსაფთხოების უზრუნველყოფაზე მიმართული სახელმწიფო პოლიტიკა ითვალისწინებდეს პერსონალური მონაცემების უსაფრთხოებისა და ინტერნეტ სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის გარანტიებს.

საკანონმდებლო ცვლილებები და კიბერუსაფრთხოების ახალი არქიტექტურა საქართველოში

ქვეყნის კიბერუსაფრთხოების გასაძლიერებლად, 2021 წელს, საქართველოში მნიშვნელოვანი საკანონმდებლო ცვლილებები განხორციელდა. კანონში - ინფორმაციული უსაფრთხოების

[1] ინფორმაციის თავისუფლების განვითარების ინსტიტუტი. „კიბერშეტევა ჯანდაცვის სამინისტროზე და რუსული კვალი“. სექტემბერი, 2020. ხელმისაწვდომია: https://idfi.ge/ge/strategy_of_russian_cyber_operations

[2] DFRLab. „GeorgiaLeaks: Data from 2011 causes confusion in 2020“. აპრილი, 2020. ხელმისაწვდომია: https://medium.com/dfrlab/georgialeaks-data-from-2011-causes-confusion-in-2020-54c9e0add6d2

შესახებ - ცვლილებების საფუძველზე, რადიკალურად შეიცვალა კიბერუსაფრთხოების არქიტექტურა. სახელმწიფო უსაფრთხოების სამსახურის საჯარო სამართლის იურიდიული პირი, ოპერატიულ - ტექნიკური სააგენტო (OTA) გახდა კიბერუსაფრთხოების უზრუნველყოფის მთავარი მაკოორდინირებელი, აღმასრულებელი და ზედამხედველი უწყება.

კრიტიკული ინფორმაციული სუბიექტები დაიყო 3 კატეგორიად:

ა) პირველი კატეგორიის სუბიექტებში მოხვდნენ სახელმწიფო ორგანოები, დაწესებულებები, საჯარო სამართლის იურიდიული პირები და სახელმწიფო საწარმოები;

ბ) მეორე კატეგორიის სუბიექტებში მოხვდნენ ელექტრონული კომუნიკაციების კომპანიები;

გ) მესამე კატეგორიის სუბიექტებში მოიაზრებიან კერძო სამართლის იურიდიული პირები, მაგალითად, ბანკები, სადაზღვევო კომპანიები და ფინანსური ინსტიტუტები.

2021 წლის 30 დეკემბრიდან ამოქმედდა კრიტიკული ინფორმაციული სისტემების სუბიექტების ახალი ნუსხა, რომლითაც განისაზღვრა პირველი, მეორე და მესამე კატეგორიების სუბიექტები.[3] პირველ კატეგორიაში მოცემულია ჯამში 61 საჯარო დაწესებულება. მანამდე არსებული ნუსხა მოიცავდა 39 საჯარო უწყებას, რომელიც აერთიანებდა საქართველოს მთავრობისგან ინსტიტუციურად სრულიად დამოუკიდებელ ადმინისტრაციულ ორგანოებს, კერძოდ: საქართველოს პარლამენტს, პრეზიდენტის ადმინისტრაციას, ქალაქ თბილისის მერიას, ცენტრალურ საარჩევნო კომისიას, საქართველოს ეროვნულ ბანკს, საქართველოს რკინიგზას, შპს საქაერონავიგაციასა და სხვა.

ახალ რედაქციაში დამატებულია ისეთი უწყებები, როგორიცაა: სახელმწიფო ინსპექტორის სამსახური (აღნიშნული 2022 წელს გაუქმდა და მის ნაცვლად ორი ახალი უწყება შეიქმნა - სპეციალური საგამოძიებო სამსახური და პერსონალურ მონაცემთა დაცვის სამსახური), გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო, კულტურის, სპორტისა და ახალგაზრდობის სამინისტრო, იუსტიციის სამინისტროს დაქვემდებარებული სსიპ-ები: ეროვნული არქივი, საკანონმდებლო მაცნე, ნოტარიუსთა პალატა, აღსრულების ეროვნული ბიურო, ასევე, სსიპ საჯარო სამსახურის ბიურო, სსიპ საპენსიო სააგენტო, შპს საქართველოს ფოსტა. მუნიციპალური ორგანოებიდან დამატებულია ქალაქ თბილისის მუნიციპალიტეტის საკრებულო და თბილისის მერიის ა(ა)იპ მუნიციპალური სერვისების განვითარების სააგენტო. დამატებულია ასევე აჭარის ავტონომიური რესპუბლიკის საკანონმდებლო და აღმასრულებელი ორგანოები - უმაღლესი საბჭო და მთავრობის აპარატი.

მეორე კატეგორიის სუბიექტები მოიცავს რვა ორგანიზაციას - ინტერნეტ სერვის პროვაიდერებს - შპს მაგთიკომი, სს სილქნეტი, შპს ვიონი-საქართველო, შპს ახალი ქსელები, შპს დელტა-კომი, შპს ოპტიკურ-ბოჭკოვანი ტელეკომუნიკაციის ქსელი - ფოპტნეტი, შპს კავკასუს ონლაინი და შპს სისტემ ნეტი. სუბიექტებში არ არიან შესული მცირე ოპერატორები.

მესამე კატეგორიის სუბიექტები 29 ორგანიზაციას აერთიანებენ, რომელთა შორის არიან მსხვილი დასაზღვევო კომპანიები, ბანკები, ასევე, მნიშვნელოვანი ენერგო, წყალმომარაგებისა და ელექტრომიმწოდებელი კომპანიები (კერძო სამართლის იურიდიული პირები), როგორიცაა, სს თელასი, შპს ჯორჯიან უოთერ ენდ ფაუერი, შპს თბილისის ელექტრომიმწოდებელი კომპანია (თელმიკო), შპს სოკარ ჯორჯია გაზი და ა.შ.

[3] საქართველოს მთავრობის დადგენილება №646 პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ. ხელმისაწვდომია: https://matsne.gov.ge/ka/document/view/5346058?publication=0
დანართი 1-ში მოცემულია პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ჩამონათვალი

ოპერატიულ-ტექნიკური სააგენტო (OTA) კოორდინირებას გაუწევს პირველ და მეორე კატეგორიაში შესულ ორგანიზაციებს, ციფრული მმართველობის სააგენტოს (ყოფილი, მონაცემთა გაცვლის სააგენტოს) რეგულირების სფეროში კი ნაწილობრივ რჩება მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები, რამდენადაც კომერციული ბანკების ინფორმაციული უსაფრთხოების უზრუნველყოფის ზედამხედველობასა და რეგულირებას კოორდინაციას გაუწევს ეროვნული ბანკი.

კიბერუსაფრთხოების გაზრდის მიზნით, კანონში მნიშვნელოვანი ცვლილებების მიუხედავად, ახალმა რეგულაციებმა სამოქალაქო საზოგადოების კრიტიკა დაიმსახურა. განსაკუთრებით პრობლემურად შეფასდა უსაფრთხოების სამსახურის გაზრდილი ძალაუფლება და კიბერსივრცეში პერსონალური მონაცემების დაცვის გარანტიების ნაკლებობა. კერძოდ, სამოქალაქო საზოგადოების ორგანიზაციების მოსაზრებით, OTA-ს გაუჩნდებოდა პირდაპირი წვდომა სახელმწიფო ორგანოებისა და სატელეკომუნიკაციო სექტორის ინფორმაციულ სისტემებზე და არაპირდაპირი წვდომა ამ სისტემებში დაცულ პერსონალურ და სხვა სენსიტიურ ინფორმაციაზე, რამდენადაც, ნორმათა ბუნდოვანება აჩენს პერსონალურ მონაცემთა არაკანონიერად და არაპროპორციულად დამუშავების რეალურ საშიშროებას.[4] ამავდროულად, მათი მოსაზრებით, კანონპროექტი არ შეესაბამებოდა ,,ქსელური უსაფრთხოების მაღალი სტანდარტისა და ინფორმაციული სისტემების დაცვის თაობაზე" **ევროპული** დირექტივის (ე.წ. NIS დირექტივა) მთელ რიგ პრინციპებს, რომლის გათვალისწინებაც საქართველოსთვის სავალდებულოა ევროკავშირთან ასოცირების ხელშეკრულების ფარგლებში.

მართალია, კანონის მიღებამდე მოხდა ცალკეული პრობლემური დეფინიციების დავიწროება,[5] ასევე, გათვალისწინებულ იქნა საბანკო სექტორის შენიშვნები, თუმცა, სამოქალაქო სექტორისთვის პრობლემური საკითხი, სახელმწიფო უსაფრთხოების სამსახური გაზრდილ უფლებამოსილებასთან დაკავშირებით, უცვლელი დარჩა. კანონში შეტანილი ცვლილებების კრიტიკის საპასუხოდ, მაშინდელმა პარლამენტის თავმჯდომარემ განაცხადა, რომ ევროდირექტივასთან ჰარმონიზაციისთვის დარჩენილი იყო რამდენიმე საკითხი, მუშაობა გაგრძელდებოდა სამუშაო ჯგუფის ფარგლებში და შემუშავდებოდა ახალი საკანონმდებლო ცვლილება, რომელსაც, საჭიროების შემთხვევაში, დაჩქარებული წესით მიიღებდნენ.[6] თუმცა, ამ დრომდე ცვლილებები არ დაინიცირებულა.

საგულისხმო იყო კანონპროექტის მიღების პროცესიც. საკანონმდებლო ცვლილებები წინ უსწრებდა ქვეყნის ახალი კიბერუსაფრთხოების ეროვნული სტრატეგიის დამტკიცებას, რომელიც სამწლიანი პაუზის შემდეგ განახლდა. შესაბამისად, ქვეყნის კიბერუსაფრთხოების არქიტექტურის რადიკალური ცვლილება დაეფუძნა არა ქვეყნის სტრატეგიულ დოკუმენტს, რომელიც ქვეყნის ერთიან ხედვასა და შემდეგი წლების განმავლობაში სტრატეგიულ მიზნებს განსაზღვრავს, არამედ პარლამენტის წევრის (ირაკლი სესიაშვილი) მიერ მომზადებულ საკანონმდებლო ცვლილებებს. აქვე უნდა აღინიშნოს, რომ სტრატეგიის მომზადებაში ჩართულნი იყვნენ სხვადასხვა უწყებები, მაშინ როცა საკანონმდებლო ცვლილებები წინასწარი კონსულტაციების გარეშე იქნა ინიცირებული.

---

[4] ინფორმაციის თავისუფლების განვითარების ინსტიტუტი. „X მოწვევის პარლამენტმა „ინფორმაციული უსაფრთხოების შესახებ" პრობლემური კანონპროექტი მესამე მოსმენით მიიღო". ივნისი 2021. ხელმისაწვდომია: https://bit.ly/3qDOY68

[5] ინფორმაციის თავისუფლების განვითარების ინსტიტუტი. „პარლამენტმა მხარი არ უნდა დაუჭიროს კანონპროექტს ინფორმაციული უსაფრთხოების შესახებ". მაისი, 2020. ხელმისაწვდომია: https://idfi.ge/ge/law-on-information-security

[6] საქართველოს პარლამენტი. „პარლამენტმა „ინფორმაციული უსაფრთხოების შესახებ" კანონში დაგეგმილი ცვლილებები მესამე მოსმენით მიიღო". ივნისი, 2021. ხელმისაწვდომია: https://bit.ly/3S0q3FS

კიბერუსაფრთხოების ახალი სტრატეგია და მიზნები

2021 წლის 30 სექტემბერს საქართველოს მთავრობის დადგენილებით მიღებულ იქნა საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა.[7]

სტრატეგიული დოკუმენტი ოთხ პრიორიტეტულ მიზანს განსაზღვრავს:

- მიზანი 1: ინფორმაციული საზოგადოებისა და ორგანიზაციების კიბერკულტურის განვითარება და შესაძლებლობების გაძლიერება კიბერსივრცეში საფრთხეებსა და ინციდენტებთან გამკლავების მიზნით;
- მიზანი 2: კიბერუსაფრთხოების მმართველობითი სისტემის მდგრადობა და საჯარო-კერძო თანამშრომლობის გაძლიერება;
- მიზანი 3: კიბერშესაძლებლობების განვითარება ძლიერი ადამიანური რესურსითა და სათანადო ტექნიკური უზრუნველყოფის საშუალებებით;
- მიზანი 4: კიბერუსაფრთხოების საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერება.

პერსონალური მონაცემთა დაცვის მიმართულებით სტრატეგიასა და მის სამოქმედო გეგმაში ცალკეული გარემოებებია ნახსენები. მიმოხილვის ნაწილში აღნიშნულია, რომ პერსონალურ მონაცემთა დაცვის სამსახური ახორციელებს ქვეყანაში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლს და პასუხისმგებელია მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულებაზე. ასევე, სამსახური კონტროლს უწევს კიბერსივრცეში ფარული საგამოძიებო მოქმედებების განხორციელების პროცესს.

სტრატეგიის განხორციელების პრინციპებში ხაზგასმულია, რომ კიბერუსაფრთხოების უზრუნველყოფა უნდა განხორციელდეს პროპორციულ, თანაზომიერ და აუცილებელ ღონისძიებათა ერთობლიობით ისე, რომ არ ილახებოდეს პირადი ცხოვრების ხელშეუხებლობა და უზრუნველყოფილი იყოს პერსონალურ მონაცემთა დაცვა.

პერსონალურ მონაცემთა დაცვის სამართლებრივი გარანტიების ჭრილში შეიძლება გამოვყოთ სტრატეგიით დაგეგმილი აქტივობები, რომლებიც ძირითადად კიბერუსაფრთხოების მმართველობითი სისტემის მედეგობის გასაზრდელად არის დაგეგმილი:

- ევროკავშირთან ასოცირების შეთანხმებით აღებული ვალდებულებებისა და ePrivacy დირექტივის შესაბამისად, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონში შესატანი ცვლილებების შესახებ შესაბამისი კანონპროექტის მომზადება;

- CERT/CSIRT-ებს, საქართველოს შინაგან საქმეთა სამინისტროს, კრიტიკული ინფორმაციული სისტემის სუბიექტებს, ინტერნეტ სერვის პროვაიდერებსა და სხვა პასუხისმგებელ უწყებებს შორის კიბერინციდენტებისა და კიბერსაფრთხეების შესახებ შეტყობინებისა და მათზე

[7] საქართველოს მთავრობის დადგენილება №482 საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ. ხელმისაწვდომია: https://matsne.gov.ge/ka/document/view/5263611?publication=1

რეაგირების სამართლებრივი მექანიზმის შემუშავება, ინფორმაციის ურთიერთგაცვლის ერთიანი პლატფორმის შექმნა და განვითარება;

- საგამოძიებო მოქმედებების განხორციელებისას მოპოვებული ელექტრონული (მათ შორის, პერსონალური მონაცემების შემცველი) მტკიცებულებების დამუშავებისა და მათთან მოპყრობის სამართლებრივი საფუძვლების ანალიზი და შესაბამისი საკანონმდებლო ცვლილებების მომზადება.

ხსენებული აქტივობების განხორციელება 2023-2024 წლებშია დაგეგმილი. მათი განხორციელების პროცესში პერსონალურ მონაცემთა დაცვის სამსახური პარტნიორ უწყებად არის დასახელებული.

ერთ-ერთი აქტივობა ასევე ეხება NIS დირექტივას, კერძოდ, განსაზღვრულია NIS დირექტივასთან სსიპ – ციფრული მმართველობის სააგენტოს მიერ მიღებული ნორმატიული აქტების ჰარმონიზაცია. თუმცა, საგულისხმოა, რომ აღნიშნული აქტივობა არ არის გათვალისწინებული კიბერუსაფრთხოებაზე პასუხისმგებელ სხვა უწყებებთან მიმართებითაც.

მართალია სტრატეგია შეიცავს ცალკეულ აქტივობებს პერსონალური მონაცემების სამართლებრივი გარანტიების გასაუმჯობესებლად, ასევე, ნახსენებია ის ევროკავშირის დირექტივები (NIS დირექტივა, ePrivacy დირექტივა), რომლებიც მნიშვნელოვანია ციფრული სფეროს მარეგულირებელი ევროკავშირის უსაფრთხოების მოთხოვნების დასაკმაყოფილებლად, მაგრამ ხაზგასმული არ არის ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის (General Data Protection Regulation – GDPR) მოთხოვნების დაკმაყოფილების მნიშვნელობა. ასევე, NIS დირექტივა და ePrivacy დირექტივების შემთხვევაშიც აქცენტი კეთდება კიბერუსაფრთხოებაზე პასუხისმგებელ მხოლოდ ცალკეულ უწყებებზე, და არ იკვეთება რამდენად იქნება გათვალისწინებული ამ კუთხით OTA-ს უფლებამოსილების კონტროლისა და ზედამხედველობის მექანიზმები. შესაბამისად, მართალია სტრატეგია პრინციპების დონეზე აღიარებს პერსონალური მონაცემების დაცვის აუცილებლობას, მაგრამ არასაკმარისია ამ მიზნის მისაღწევად დაგეგმილი აქტივობები. რაც უზრუნველყოფდა ერთი მხრივ, კიბერუსაფრთხოების გაზრდას და მეორე მხრივ, კიბერსივრცეში მოქალაქეთა პირადი ცხოვრების ხელშეუხებლობის დაცვას.

კიბერსივრცეში პერსონალური მონაცემების დაცვის სამართლებრივი გარანტიების ნაკლებობა

პერსონალურ მონაცემთა უსაფრთხოების საკითხის კიბერუსაფრთხოების ხელშემწყობ ჩარჩოსთან თანხვედრისა და ინტეგრირების აუცილებლობაზე მიანიშნებდა IDFI-ის ერთ-ერთი ბოლო კვლევა, სადაც გაანალიზდა აღნიშნულ საკითხებზე საქართველოს კანონმდებლობა, საუკეთესო ევროპული სამართლებრივი ჩარჩო, და გამოვლენილი ნაკლოვანებების საფუძველზე შემუშავდა რეკომენდაციები.[8]

ხსენებული დოკუმენტი ხაზს უსვამდა შემდეგ გამოწვევებსა და საჭიროებებს:

ა) გადამეტებული კონტროლისა და ზედამხედველობის რეჟიმი - ინფორმაციული უსაფრთხოების შესახებ ახალიკანონით განსაზღვრული საზედამხედველო მოდელი კრიტიკული ინფრასტრუქტურების კიბერმედეგობისა და თვითგაძლიერების ნაცვლად ხშირ

[8] "კიბერსივრცეში პერსონალური მონაცემების დაცულობის უზრუნველყოფა: გამოწვევები და საჭიროებები საქართველოსთვის" ნოემბერი, 2021. ხელმისაწვდომია: https://idfi.ge/ge/protection_of_personal_data_in_cyberspace

შემთხვევაში ზედამხედველი სუბიექტის მიერ პირდაპირ საქმიანობაში ჩარევას და სადავეების საკუთარ ხელში აღებას გულისხმობს. საზედამხედველო ორგანოების მხრიდან ზედამხედველობის რეჟიმი დასულია ყოველდღიურ ოპერატიულ დონეზე, კრიტიკული ინფორმაციული სისტემების წვდომისა და კონტროლის აქტივობებზე. მაშინ როცა, NIS დირექტივა მთავარ აქცენტს სუბიექტების მხარდაჭერაზე, გაძლიერებასა და არა მათ ნაცვლად კიბერშეტევების მართვაზე აკეთებს. საზედამხედველო ორგანოების მხრიდან რეგულირების დროს ასევე უნდა იყოს დაცული პროპორციულობის, ბალანსისა და აუცილებლობის პრინციპები.

ბ) ქსელური მონიტორინგის სისტემასთან დაკავშირებული კითხვები პერსონალური მონაცემების დაცვის ჭრილში - ქსელური სენსორი გახლავთ აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების ერთობლიობა, რომელიც გამიზნულია ქსელური ნაკადის მონიტორინგისთვის, ინფორმაციული სისტემის წინააღმდეგ მიმართული კომპიუტერული ინციდენტის გამოსავლენად. კანონის თანახმად, მისი კონფიგურირების წესები განისაზღვრება კანონქვემდებარე აქტით - პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით. მნიშვნელოვანია, რომ ამ საკითხის რეგულირება მოხდეს მკაფიო და არაორაზროვანი ნორმებით, რომლებიც კოდიფიცირდება კანონით, რადგან კანონქვემდებარე აქტებით დადგენილი წესები შესაძლოა ხშირად, მარტივად და არაპროგნოზირებადად შეიცვალოს გარეშე პირთა ჩართულობის ნაკლებობის პირობებში. გარდა ამისა, ქსელური მონიტორინგის სისტემის ფუნქციონირებაზე დამოუკიდებელი და მიუკერძოებელი საზედამხედველო რგოლის არსებობა კრიტიკულად მნიშვნელოვანია.

გ) პერსონალურ მონაცემთა კომპრომეტირებისას შეტყობინებების ვალდებულება - კიბერშეტევის დროს ხდება პერსონალური მონაცემების კომპრომეტირება. იმისთვის, რომ კიბერსივრცეში არ მოხდეს პერსონალური მონაცემთა ხელყოფა, აუცილებელია კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებელმა უწყებებმა ითანამშრომლონ პერსონალური მონაცემების დაცვაზე მომუშავე საჯარო დაწესებულებასთან, გაცვალონ ინფორმაცია ინცინდენტის შედეგად პერსონალური მონაცემების ხელყოფის შესახებ და ერთობლივად იმუშაონ მძიმე შედეგების მინიმიზაციისა და ზიანის შემსუბუქებისთვის. შედარებისთვის, ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის (General Data Protection Regulation – GDPR) 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. „ინფორმაციული უსაფრთხოების შესახებ“ კანონი არ განსაზღვრავს პერსონალურ მონაცემთა დაცვის სამსახურთან ინფორმაციის ურთიერთგაცვლისა და თანამშრომლობის რაიმე ფორმების შესაძლებლობებს.

დ) კრიტიკული ინფორმაციული სისტემის სუბიექტებიდან ინფორმაციის გამოთხოვისას, ინფორმაციაზე წვდომის მოპოვებისას მიზნობრიობის, პროპორციულობისა და აუცილებლობის დაცვა - შეცვლილი 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. მაშინ როცა, ევროკავშირის დირექტივის (NIS დირექტივა) მიხედვით, „ინფორმაციის ან მტკიცებულების მოთხოვნისას კომპეტენტურმა ორგანომ უნდა დაასაბუთოს მოთხოვნის მიზანი და დააკონკრეტოს ინფორმაცია, რომლის გამოთხოვაც საჭიროდ მიაჩნია“.[9]

[9] The Directive on security of network and information systems (the NIS Directive) Article 15(2)

მნიშვნელოვანია, რომ კანონით განსაზღვრული იყოს პროცედურული თუ სამართლებრივი პროტოკოლი, რომელთა დაკმაყოფილების შემთხვევაში, დაშვების აუცილებლობა დასაბუთებული იქნება საზედამხედველო სუბიექტების მიერ და მხოლოდ შემდეგ განხორციელდება წვდომა.

ე) კიბერუსაფრთხოების კომპეტენტური ორგანოების საზედამხედველო მექანიზმების სისუსტე - კანონი ღიად ტოვებს OTA-ს უფლებამოსილების კონტროლისა და ზედამხედველობის მექანიზმებს, და არ განსაზღვრავს კონკრეტული გარანტიებსა და პროცედურულ ბერკეტებს. ინფორმაციული და კიბერუსაფრთხოების სფეროებში დელეგირებული უფლებამოსილებების განხორციელებისას, 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.

რეკომენდაციები

გამოვლენილი გამოწვევებისა და საკანონმდებლო ხარვეზების საპასუხოდ, IDFI-ის კვლევის ფარგლებში შემუშავდა ცალკეული რეკომენდაციები, რომლებიც დღემდე აქტუალურია ხელისუფლების მიერ დააანონსებული პოტენციური საკანონმდებლო ცვლილებების ჭრილში. ასევე, აღნიშნული რეკომენდაციების გათვალისწინება მნივშენლოვანია კიბერუსაფრთხოების ეროვნული სტრატეგიით გათვალისწინებული აქტივობების განხორციელების დროსაც.

- ✓ „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 პერსონალურ მონაცემების დაცვის სამსახურთან.** ჩამოყალიბდეს **ინფორმაციის ურთიერთგაცვლის პროტოკოლი და სამართლებრივ-პროცედურული ნორმები**.
- ✓ 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.

- ✓ გაანალიზდეს, 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 იყოს იდენტიფიცირებული კიბერსივრცეში პერსონალური მონაცემების უსაფრთხოების უზრუნველყოფისთვის რა სტანდარტებით უნდა იხელმძღვანელონ.**

✓ მნიშვნელოვანია პერსონალურ მონაცემთა დაცვისა და კიბერუსაფრთხოების 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 და ა.შ.

დანართი 1: პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ჩამონათვალი

I კატეგორიის სუბიექტები:	**II კატეგორიის სუბიექტები**	**III კატეგორიის სუბიექტები**
პასუხიმგებელი უწყება: ოპერატიულ-ტექნიკური სააგენტო	**პასუხიმგებელი უწყება:** ოპერატიულ-ტექნიკური სააგენტო	**პასუხისმგებელი უწყება:** ციფრული მმართველობის სააგენტო (ეროვნული ბანკი ბანკებთან მიმართებაში)
საქართველოს პარლამენტი	შპს „მაგთიკომი“	სს „დაზღვევის საერთაშორისო კომპანია ირაო“
საქართველოს პრეზიდენტის ადმინისტრაცია	სს „სილქნეტი“	სს „სადაზღვევო კომპანია ჯი პი აი ჰოლდინგი“
საქართველოს მთავრობის ადმინისტრაცია	შპს „ვიონი-საქართველო“	სს „პსპ დაზღვევა“
აჭარის ა/რ უმაღლესი საბჭო	შპს „ახალი ქსელები“	სს „სადაზღვევო კომპანია იმედი ელ“
აჭარის ა/რ მთავრობის აპარატი	შპს „დელტა-კომმი“	სს „არდი დაზღვევა“
საქართველოს ეროვნული ბანკი	შპს „ოპტიკურ-ბოჭკოვანი ტელეკომუნიკაციის ქსელი – ფოპტნეტი“	სს „სადაზღვევო კომპანია ალდაგი“
საქართველოს პროკურატურა	შპს „კავკასუს ონლაინი“	სს „თიბისი დაზღვევა“
ეროვნული უსაფრთხოების საბჭოს აპარატი	შპს „სისტემ ნეტი“	ა(ა)იპ – სავალდებულო დაზღვევის ცენტრი
ცენტრალური საარჩევნო კომისია		შპს „აღმოსავლეთის ენერგოკორპორაცია“

სახელმწიფო ინსპექტორის სამსახური		სს „თელასი“
სახელმწიფო დაცვის სპეციალური სამსახური		შპს „თბილისი ენერჯი“
საქართველოს სახელმწიფო უსაფრთხოების სამსახური		შპს „საქართველო-ურბან ენერჯი“
სსიპ საქართველოს ოპერატიულ-ტექნიკური სააგენტო		შპს „აჭარ ენერჯი-2007“
შინაგან საქმეთა სამინისტრო		შპს „ჯორჯიან უოთერ ენდ ფაუერი“
სსიპ საქართველოს სასაზღვრო პოლიცია		შპს „სოკარ ჯორჯია გაზი“
სსიპ მომსახურების სააგენტო		შპს „თბილისის ელექტრომიმწოდებელი კომპანია“ (თელმიკო)
სსიპ საზოგადოებრივი უსაფრთხოების მართვის ცენტრი „112“		სს „ენერგო-პრო ჯორჯია“
სსიპ დაცვის პოლიციის დეპარტამენტი		სს „საქართველოს ბანკი“
საგარეო საქმეთა სამინისტრო		სს „თიბისი ბანკი“
ეკონომიკისა და მდგრადი განვითარების სამინისტრო		სს „ლიბერთი ბანკი“
სსიპ სახმელეთო ტრანსპორტის სააგენტო		შპს „ბათუმის ნავთობტერმინალი“
სსიპ საზღვაო ტრანსპორტის სააგენტო		შპს „ფოთის ახალი საზღვაო ნავსადგური“
იუსტიციის სამინისტრო		შპს „ბათუმის საერთაშორისო საკონტეინერო ტერმინალი“
სპეციალური პენიტენციური სამსახური		შპს „შავი ზღვის ტერმინალი“
სსიპ საქართველოს ეროვნული არქივი		სს „საქართველოს მილსადენის კომპანიის საქართველოს ფილიალი“
სსიპ საქართველოს საკანონმდებლო მაცნე		სს „კორპორაცია ფოთის საზღვაო ნავსადგური“
სსიპ საჯარო რეესტრის ეროვნული სააგენტო		შპს „ჯორჯიან ეარვეის“
სსიპ სახელმწიფო სერვისების		შპს „ლასარე“

განვითარების სააგენტო		
სსიპ საქართველოს ნოტარიუსთა პალატა		შპს „თბილისი კარგო სერვისი“
სსიპ აღსრულების ეროვნული ბიურო		
სსიპ დანაშაულის პრევენციის, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის ეროვნული სააგენტო		
განათლებისა და მეცნიერების სამინისტრო		
სსიპ განათლების მართვის საინფორმაციო სისტემა		
სსიპ შეფასებისა და გამოცდების ეროვნული ცენტრი		
სსიპ განათლების ხარისხის განვითარების ეროვნული ცენტრი		
რეგიონული განვითარებისა და ინფრასტრუქტურის სამინისტრო		
კულტურის, სპორტისა და ახალგაზრდობის სამინისტრო		
ფინანსთა სამინისტრო		
სსიპ შემოსავლების სამსახური		
სსიპ საფინანსო-ანალიტიკური სამსახური		
გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო		
სსიპ სურსათის ეროვნული სააგენტო		
სსიპ გარემოს ეროვნული სააგენტო		
სსიპ გარემოსდაცვითი ინფორმაციისა და განათლების ცენტრი		
ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო		
სსიპ ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი		
სსიპ დევნილთა, ეკომიგრანტთა და საარსებო წყაროებით უზრუნველყოფის სააგენტო		

სსიპ საგანგებო სიტუაციების კოორდინაციისა და გადაუდებელი დახმარების ცენტრი		
სსიპ სამედიცინო და ფარმაცევტული საქმიანობის რეგულირების სააგენტო		
სსიპ სოციალური მომსახურების სააგენტო		
სსიპ ჯანმრთელობის ეროვნული სააგენტო		
სსიპ ინფორმაციული ტექნოლოგიების სააგენტო		
სსიპ სახელმწიფო შესყიდვების სააგენტო		
სსიპ საპენსიო სააგენტო		
სსიპ საჯარო სამსახურის ბიურო		
ქალაქ თბილისის მუნიციპალიტეტის საკრებულო		
ქალაქ თბილისის მუნიციპალიტეტის მერია		
ა(ა)იპ მუნიციპალური სერვისების განვითარების სააგენტო		
შპს „საქაერონავიგაცია“		
შპს „საქართველოს ფოსტა“		
სს „საქართველოს რკინიგზა“		