„ევროკავშირი დეტალებში“ #14

გიორგი რობაქიძე

კიბერმედეგობის აქტი

სიღრმისეული ანალიზი არაექსპერტებისთვის

გამოთქმული მოსაზრებები და დასკვნები ეკუთვნის ავტორს და შეიძლება არ ასახავდეს ევროკავშირის ცნობიერების ამაღლების ცენტრის პოზიციას.

სექტემბერი 2026

© [2026] ევროკავშირის ცნობიერების ამაღლების ცენტრი. ყველა უფლება დაცულია.

I. ხარვეზის დახურვა: რატომ დაარეგულირა ევროკავშირმა პროდუქტების კიბერუსაფრთხოება

ხარვეზი, რომლის დასახურადაც შეიქმნა რეგულაცია

ბოლო ორი ათწლეულის განმავლობაში ევროპული კიბერუსაფრთხოების კანონმდებლობა ძირითადად ორგანიზაციებს არეგულირებდა არა კონკრეტულ პროდუქციას. "NIS2 დირექტივა" უდგენს რისკების მართვის წესებს საავადმყოფოებს, ენერგეტიკულ ოპერატორებსა და ციფრული ინფრასტრუქტურის მიმწოდებლებს. 2019 წლის კიბერუსაფრთხოების აქტმა კი სერტიფიცირების სქემა შექმნა, რომლითაც კომპანიებს ნებაყოფლობით შეეძლოთ ესარგებლათ. მაგრამ არც ერთი ეს ინსტრუმენტი არ ავალდებულებდა ე.წ. ელექტრონული ჭკვიანი თერმოსტატის, საშინაო ინტერნეტ როუტერის ან სამრეწველო სენსორის მწარმოებელს, პროდუქტი დაცული გაეხადა მაღაზიის თაროზე მოხვედრამდე. ეს ხარვეზი აშკარა წინააღმდეგობაში მოდიოდა იმ ფაქტთან, რომელიც მარეგულირებლებმა კარგად იცოდნენ და რომელსაც მოქალაქეები უშუალოდ განიცდიდნენ: იაფი და ცუდად მოვლილი ქსელში ჩართული მოწყობილობები ევროპულ სახლებში, ოფისებში და ზოგჯერ კრიტიკულ ინფრასტრუქტურაშიც კიბერ შეღწევის ყველაზე მარტივ გზად იქცა.

კიბერმედეგობის აქტი (Cyber Resilience Act – CRA), ოფიციალურად — 2024 წლის 23 ოქტომბრის რეგულაცია (EU) 2024/2847, სწორედ ამ ხარვეზის აღმოსაფხვრელად შეიქმნა. ეს ჰორიზონტალური რეგულაციაა: იგი რომელიმე ერთ სექტორს არ ეხება და **ციფრული ელემენტების შემცველი პროდუქტების** მთელ ბაზარს მოიცავს. ასეთად ითვლება ნებისმიერი აპარატურა ან პროგრამული უზრუნველყოფა, რომელიც ევროკავშირში კომერციულად იყიდება და რომლის მუშაობა მოწყობილობასთან ან ქსელთან მონაცემთა კავშირზეა დამოკიდებული. რეგულაციის პრეამბულა პრობლემის მასშტაბს გულახდილად აღწერს: საუბარია „კიბერუსაფრთხოების დაბალ დონეზე", რაც „ფართოდ გავრცელებულ მოწყვლადობებსა" და „უსაფრთხოების განახლებების არასაკმარის და არათანმიმდევრულ მიწოდებაში" გამოიხატება. ამას მეორე პრობლემა ემატება — ჩვეულებრივ მყიდველს არ ჰქონდა საიმედო საშუალება, გაერკვია, რომელი პროდუქტი იყო უსაფრთხო. პრეამბულის თანახმად, კიბერშეტევები დღეს უკვე მხოლოდ კომერციული უსიამოვნება არ არის: ისინი საჯარო ინტერესის საკითხად განიხილება და დემოკრატიაზე, მომხმარებელთა უსაფრთხოებასა და ჯანმრთელობაზე აისახება.

რეგულაციის სტრუქტურულ მნიშვნელობას არა ეს დიაგნოზი განაპირობებს — კიბერუსაფრთხოების სტრატეგიების უმეტესობა მსგავსი სიტყვებით იწყება — არამედ შერჩეული გამოსავალი. ევროკავშირს შეეძლო წევრ სახელმწიფოებს მოეთხოვა, პროდუქტები თავად დაერეგულირებინათ, ან ბაზარს მიენდო, რომ ზიანის დადგომის შემდეგ სასამართლო დავები თავად გამოასწორებდა მდგომარეობას. ამის ნაცვლად კავშირმა აირჩია, უშუალოდ მწარმოებლებს დაეკისრა ერთიანი, წინასწარი (*ex ante*) ვალდებულებები, რომლებიც პროდუქტის დიზაინის ეტაპიდანვე კიბერუსაფრთხოების უზრუნველყოფას ითვალისწინებენ. ამ ვალდებულებების აღსრულება CE მარკირების იმავე სისტემის მეშვეობით ხდება, რომელიც მანქანა-დანადგარებზე, სათამაშოებსა და სამედიცინო მოწყობილობებზე ვრცელდება. სარეცხი მანქანა ევროკავშირში კანონიერად ვერ გაიყიდება, თუ ბრიუსელსა და სტრასბურგში დადგენილ უსაფრთხოების სტანდარტებს არ აკმაყოფილებს; 2027 წლიდან, პრინციპში, იგივე ითქმის დაუცველ ჭკვიან სარეცხ მანქანაზეც.

ერთიანი წესები ფრაგმენტული საფრთხის წინააღმდეგ

არგუმენტი ჰორიზონტალური კანონმდებლობის სასარგებლოდ მარტივ დაკვირვებას ეფუძნებოდა: პროდუქტების კიბერუსაფრთხოებისადმი ეროვნული მიდგომები — იქ, სადაც ისინი საერთოდ არსებობდა — ერთმანეთისგან იმდენად განსხვავდებოდა, რომ ერთიან ბაზარს ანაწევრებდა, რისკს კი არსებითად არ ამცირებდა. მწარმოებელს, რომელიც ოცდაშვიდ იურისდიქციაში ყიდდა პროდუქტს, ოცდაშვიდი შესაძლო არაფორმალური მოლოდინის გათვალისწინება უწევდა და არ ჰქონდა საიმედო ევროპული საბაზისო სტანდარტი, რომლის მიხედვითაც პროდუქტს ერთხელ დააპროექტებდა და საქმე დამთავრებული იქნებოდა. რეგულაციის განმარტებით ბარათში ეს მდგომარეობა „შიდა ბაზარზე არსებულ საკანონმდებლო სიჭრელედ“ არის მოხსენიებული, და ეს ფრაზა პოლიტიკურ ლოგიკას ზუსტად გამოხატავს. საქმე აქ არა იმდენად კიბერუსაფრთხოების იდეალიზმს ეხება, რამდენადაც ევროკავშირის უძველეს ინსტინქტს: ფრაგმენტაცია თავისთავად დანახარჯად ითვლება, იმისდა მიუხედავად, რა რისკის მართვას ემსახურება.

სწორედ ამ ინსტინქტით აიხსნება, რატომ დაეფუძნა კიბერმედეგობის აქტი ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულების 114-ე მუხლს — შიდა ბაზრის დებულებას — და არა უსაფრთხოების სფეროს რომელიმე სამართლებრივ საფუძველს. ეს არჩევანი მხოლოდ ტექნიკური არ არის. იგი იმაზე მიუთითებს, რომ ბრიუსელი პროდუქტების კიბერუსაფრთხოებას უპირველესად ბაზრის ფუნქციონირების საკითხად მიიჩნევს, სადაც კვალიფიციური უმრავლესობით კენჭისყრა და ევროპარლამენტთან სრული თანაგადაწყვეტილება მოქმედებს, და არა ისეთ სფეროდ, სადაც წევრი სახელმწიფოები ერთსულოვნებას ან უსაფრთხოების უფრო ვიწრო კომპეტენციას მოითხოვდნენ. როგორც შემდგომ ნაწილებში ვნახავთ, სამართლებრივი საფუძვლის იგივე საკითხი გაცილებით მწვავედ დგას ერთ მონათესავე, თუმცა ცალკე საკანონმდებლო აქტთან დაკავშირებით, რომელიც ამჟამად ევროკავშირის ინსტიტუტებში განიხილება.

შედეგად მივიღეთ რეგულაცია, რომელიც ზოგან სამრეწველო უსაფრთხოების კანონს ჰგავს, უბრალოდ ციფრულ სფეროშია გადმოტანილი. სწორედ ამ მიდგომის გადატანა წარმოადგენს კიბერმედეგობის აქტის განმსაზღვრელ თავისებურებას: იგი დაუცველ კოდს ხარვეზიან პროდუქტად მიიჩნევს და არა გარე ეფექტად, რომელიც ზიანის დადგომის შემდეგ უნდა მოგვარდეს.

II. მოქმედების სფერო და დეფინიციები: რა ითვლება ციფრული ელემენტების შემცველ პროდუქტად

ბაზრის საზღვრის გავლება

რეგულაციის მოქმედების სფერო შეგნებულად ფართოა. **ციფრული ელემენტების შემცველი პროდუქტი** მოიცავს დამოუკიდებელ პროგრამულ უზრუნველყოფას, მაგალითად მობილურ აპლიკაციებს; ჩაშენებული პროგრამული უზრუნველყოფის მქონე აპარატურას, მაგალითად როუტერებსა და მიერთებულ კამერებს; დამოუკიდებელ აპარატურას, მათ შორის ინტეგრირებულ მიკროსქემებს; და ამ ორის ნებისმიერ კომბინაციას, რომელიც ერთობლივი მუშაობისთვისაა განკუთვნილი. მე-2 მუხლი ზღვარს კომერციულ ხელმისაწვდომობაზე ავლებს. თუ პროდუქტი ევროკავშირის ბაზარზეა განთავსებული — ანუ კომერციული საქმიანობის ფარგლებში, ფასიანად თუ უფასოდ, დისტრიბუციისთვის ან გამოსაყენებლად არის მიწოდებული — იგი რეგულაციის მოქმედების სფეროში ექცევა, იმ პირობით, რომ მისი

განზრახული ან გონივრულად განჭვრეტადი გამოყენება მოწყობილობასთან ან ქსელთან ლოგიკურ ან ფიზიკურ კავშირს გულისხმობს.

ეს ერთადერთი კრიტერიუმი იმაზე მეტს გამორიცხავს, ვიდრე ერთი შეხედვით ჩანს. ვებგვერდი, რომელიც თავად მიერთებული პროდუქტის ფუნქციას არ ასრულებს, რეგულაციის მიღმა რჩება. დამოუკიდებელი პროგრამული უზრუნველყოფის, როგორც სერვისის (SaaS), შეთავაზებები და ღრუბლოვანი პლატფორმები, რომლებიც ნებისმიერი ფიზიკური პროდუქტისგან დამოუკიდებლად შეიქმნა და მუშაობს, როგორც წესი, ასევე კიბერმედეგობის აქტის მიღმა რჩება. გამონაკლისია შემთხვევა, როცა ისინი **დისტანციური მონაცემთა დამუშავების სერვისად** მიიჩნევა — ანუ სერვისად, რომელიც მწარმოებელმა შექმნა ან მისი პასუხისმგებლობით შეიქმნა და რომლის გარეშეც პროდუქტი რომელიმე ძირითად ფუნქციას ვერ შეასრულებდა. ჭკვიანი კარის ზარი, რომლის მოძრაობის აღმოჩენის ფუნქცია მწარმოებლის ღრუბლოვან სერვისზეა დამოკიდებული, ამ სერვისსაც რეგულაციის მოქმედების სფეროში აქცევს; ზოგადი დანიშნულების ვიდეოების შესანახი აპლიკაცია კი, რომელსაც მომხმარებელი იმავე ზარს თავად უერთებს, რეგულაციას არ ექვემდებარება.

პრაქტიკულად ეს ნიშნავს, რომ სამართლებრივი მნიშვნელობა არა მხოლოდ მწარმოებლის ფიზიკურ პროდუქტს, არამედ მისი მიწოდების ჯაჭვის არქიტექტურასაც ენიჭება. ფირმა, რომელიც პროდუქტიდან ღრუბლოვან დამოკიდებულებას საერთოდ გამორიცხავს, ვალდებულებების მთელ კატეგორიას თავიდან იცილებს; ის კი, ვინც ამ დამოკიდებულებას პროდუქტში ჩადებს, პასუხისმგებლობას იღებს სერვისზე, რომელსაც ფიზიკური მოწყობილობის გამოშვების შემდეგ კიდევ წლების განმავლობაში მოუწევს მუშაობა.

ვის ეკისრება ვალდებულებები?

რეგულაცია პასუხისმგებლობას ე. წ. **ეკონომიკურ ოპერატორებს** შორის ანაწილებს. ესენია მწარმოებლები, უფლებამოსილი წარმომადგენლები, იმპორტიორები და დისტრიბუტორები. არსებითი ვალდებულებების უდიდესი ნაწილი მწარმოებლებს ეკისრება, რადგან სწორედ მათ შეუძლიათ ყველაზე უკეთ, უსაფრთხოება პროდუქტში თავიდანვე ჩააშენონ. იმპორტიორები და დისტრიბუტორები ძირითადად მაკონტროლებელი რგოლის როლს ასრულებენ: სანამ პროდუქტს ბაზარზე განათავსებენ ან ხელმისაწვდომს გახდიან, მათ უნდა შეამოწმონ, აქვს თუ არა მას საჭირო დოკუმენტაცია და CE მარკირება. ეს საფეხურებრივი მოდელი — ყველაზე მძიმე ვალდებულებები დიზაინის გადაწყვეტილებებთან ყველაზე ახლოს მდგომ მხარეს, უფრო მსუბუქი, თუმცა რეალური ვალდებულებები ჯაჭვის შემდგომ რგოლებს — იმ სტრუქტურას იმეორებს, რომელსაც ევროკავშირი ფიზიკური პროდუქტების უსაფრთხოებისთვის უკვე იყენებს. სწორედ ეს კავშირი ნაცნობ სამართალთან ანიჭებს კიბერმედეგობის აქტს პრაქტიკულ ძალას: ეროვნულ საბაზრო ზედამხედველობის ორგანოებს აღსრულების ახალი დოქტრინის შექმნა არ სჭირდებათ — საკმარისია, არსებული პროდუქტების ახალ კატეგორიაზე გაავრცელონ.

ერთი დეფინიციური სიახლე განსაკუთრებულ ყურადღებას იმსახურებს, რადგან სწორედ მან განსაზღვრა მთელი საკანონმდებლო დებატები. ეს არის **ღია წყაროს პროგრამული უზრუნველყოფის მმართველი** — ორგანიზაცია, როგორც წესი, ფონდი ან მსგავსი იურიდიული პირი, რომელიც ღია წყაროს პროგრამული უზრუნველყოფის განვითარებას მდგრად და სისტემატურ მხარდაჭერას უწევს. ეს კატეგორია სპეციალურად იმისთვის შეიქმნა, რომ ღია წყაროს ყოველი ფონდი კომერციულ მწარმოებლად არ ჩათვლილიყო. მისი შემოტანა, რაც VI ნაწილშია დაწვრილებით განხილული, იყო ის კომპრომისი, რომელმაც ქარხნული

წარმოებისთვის შექმნილი პროდუქტზე პასუხისმგებლობის ლოგიკის შეთავსება შესაძლებელი გახადა მოხალისეებზე დაფუძნებულ განვითარების მოდელთან.

მოქმედების სფეროს დებულებები, ერთად აღებული, გამორიცხვების ჩამონათვალზე მეტ ფუნქციას ასრულებს. ისინი ადგენენ, რომ ევროპული სამართალი „მიერთებული პროდუქტის ბაზარზე განთავსებას“ ამიერიდან ისეთ ქმედებად განიხილავს, რომელსაც თავისთავად სამართლებრივი შედეგები მოჰყვება. ამით უქმდება დიდი ხნის დამკვიდრებული დაშვება, რომ ციფრული პროდუქტი თავისუფლად შედიოდა ბრუნვაში, თუ კონკრეტული ნორმა სხვას არ ითვალისწინებდა.

III. მწარმოებლის ძირითადი ვალდებულებები: უსაფრთხოება დიზაინის დონეზე და ნაგულისხმევი პარამეტრებით

რისკის შეფასება როგორც ცენტრალური პრინციპი

რეგულაციის ოპერაციული გული მე-13 მუხლია. იგი მწარმოებლებს ავალდებულებს, პროდუქტის ბაზარზე განთავსებამდე უზრუნველყონ, რომ იგი I დანართით დადგენილი კიბერუსაფრთხოების არსებითი მოთხოვნების შესაბამისად იყოს დაპროექტებული, შემუშავებული და დამზადებული. შესაბამისობა მხოლოდ ფიქსირებული საკონტროლო ნუსხით არ ფასდება. იგი სავალდებულო **კიბერუსაფრთხოების რისკის შეფასებით** იწყება, რომელშიც პროდუქტის დანიშნულება, მისი გონივრულად განჭვრეტადი გამოყენება, საოპერაციო გარემო და სავარაუდო ექსპლუატაციის ვადა უნდა გაანალიზდეს. ეს შეფასება უნდა დოკუმენტირდეს, პროდუქტის ტექნიკურ ფაილში შეინახოს და მხარდაჭერის მთელი პერიოდის განმავლობაში გადაიხედოს — და არა ერთხელ, გაშვების მომენტში, შედგეს და შემდეგ თაროზე შემოიდოს.

ეს რეგულირების არსებითად განსხვავებული ფილოსოფიაა, ვიდრე ერთჯერადი შესაბამისობის ტესტი. მწარმოებლებს მოეთხოვებათ, საფრთხეებზე მუდმივად ფიქრობდნენ და არა ერთხელ დაადასტურონ შესაბამისობა და საქმე დამთავრებულად ჩათვალონ. ამასთან, საბაზრო ზედამხედველობის ორგანოს შეუძლია შეამოწმოს არა მხოლოდ ის, ჩატარდა თუ არა შეფასება, არამედ მისი ხარისხიც. ზედაპირული და საფუძვლიანი რისკის შეფასება ერთსა და იმავე პროცედურულ მოთხოვნას აკმაყოფილებს, მაგრამ, როცა ინციდენტის შემდეგ მარეგულირებელი ფაილს გამოითხოვს, შემოწმებას მხოლოდ ერთი მათგანი გაუძლებს.

წარმოვიდგინოთ საშუალო ზომის ევროპული კომპანია, რომელიც შენობებში დაშვების კონტროლის ჭკვიან მოწყობილობებს აწარმოებს. კიბერმედეგობის აქტის პირობებში მას აღარ შეუძლია მოწყობილობა ნაგულისხმევი პაროლითა და „საჭიროებისამებრ განახლების“ დაპირებით გამოუშვას. მან უნდა შეაფასოს, როგორ გამოიყენებენ მოწყობილობას რეალურად — სავარაუდოდ, უსაფრთხოების არაერთგვაროვანი დონის მქონე შენობის ქსელში ჩართავენ და იქ ათი წელი დატოვებენ — და პროდუქტი შესაბამისად დააპროექტოს, შემდეგ კი ეს მსჯელობა ისეთ დოკუმენტში ასახოს, რომელსაც მარეგულირებელი მოგვიანებით შეამოწმებს.

ჯეროვანი გულისხმიერება მიწოდების ჯაჭვში

თანამედროვე პროგრამული უზრუნველყოფა ნულიდან არ იწერება — იგი მზა კომპონენტებისგან იწყობა, და რეგულაცია ამ რეალობას სერიოზულად ითვალისწინებს. მე-13 მუხლის მე-5 პუნქტის თანახმად, მესამე მხარის კომპონენტების — მათ შორის იმ თავისუფალი და ღია წყაროს კომპონენტების, რომლებიც თავად ბაზარზე არ არის განთავსებული — ინტეგრირებისას მწარმოებელმა ჯეროვანი გულისხმიერება უნდა გამოიჩინოს, რათა ეს

კომპონენტები საბოლოო პროდუქტის უსაფრთხოებას არ დააზიანოს. თუ მწარმოებელი ინტეგრირებულ კომპონენტში მოწყვლადობას აღმოაჩენს, მან ამის შესახებ უნდა აცნობოს იმას, ვინც ამ კომპონენტს ავითარებს ან მხარს უჭერს, და, თუ გამოსწორება უკვე მოამზადა, შესაბამისი კოდი ან დოკუმენტაცია გაუზიაროს.

სწორედ ეს ვალდებულება ცვლის, თუმცა შეუმჩნევლად, სტიმულებს პროგრამული უზრუნველყოფის მთელ მიწოდების ჯაჭვში. მწარმოებელს, რომელსაც აქამდე არასდროს შეუმოწმებია პროდუქტში გამოყენებული კომპონენტები, ახლა ამის სამართლებრივი მოტივი აქვს — და ისიც, რომ გამოსწორებები კომპონენტის შემქმნელებს დაუბრუნოს და მხოლოდ საკუთარი ასლი არ შეაკეთოს. მექანიზმი ამბიციურია, რადგან კოლექტიური ქმედების იმ ჩავარდნის გამოსწორებას ცდილობს, რომელიც ღია წყაროს უსაფრთხოებას უკვე ათი წელია აწუხებს: საზიარო კომპონენტებს ყველა ეყრდნობა, მათ მოვლას კი თითქმის არავინ აფინანსებს. ამავე დროს იგი მყიფეა, რადგან ჯეროვანი გულისხმიერების ვალდებულება არაფერს ამბობს იმაზე, ვინ გადაიხდის მის შედეგად საჭირო აუდიტების, გამჟღავნებებისა და გამოსწორებების ხარჯებს.

მწარმოებლის ვალდებულებები, ერთად წაკითხული, ერთ გადასვლას აღწერს: კიბერუსაფრთხოება, რომელიც აქამდე დამატებითი საფასურით გასაყიდი ფუნქცია იყო, ბაზარზე დაშვების წინაპირობად იქცევა. რეგულაციის განმარტებითი ბარათი ამ გადასვლას, გადაჭარბების გარეშე, ფუძემდებლურს უწოდებს.

IV. მოწყვლადობების მართვა, მხარდაჭერის პერიოდი და ანგარიშგების ვადები

რამდენ ხანს უნდა დარჩეს პროდუქტი უსაფრთხოდ გამოსაყენებელი

კიბერმედეგობის აქტის ერთ-ერთი ყველაზე მნიშვნელოვანი — და ყველაზე სადავო — დებულება მწარმოებელს ავალდებულებს, განსაზღვროს **მხარდაჭერის პერიოდი**: ვადა, რომლის განმავლობაშიც იგი პროდუქტში მოწყვლადობების აღმოფხვრას კისრულობს. მე-13 მუხლის მე-8 პუნქტის თანახმად, ეს ვადა მომხმარებელთა რეალისტურ მოლოდინებსა და პროდუქტის სავარაუდო სასიცოცხლო ციკლს უნდა შეესაბამებოდეს. ევროკომისიის სახელმძღვანელომ, რომელიც რეგულაციას ახლავს, შემდგომში განმარტა, რომ ხშირად ნახსენები ხუთწლიანი ვადა მინიმუმია და არა ნაგულისხმევი სტანდარტი. პროდუქტს, რომელიც გონივრულად უფრო ხანგრძლივ გამოყენებას ითვალისწინებს — მაგალითად, სამრეწველო სენსორს ან შენობის ინფრასტრუქტურის ელემენტს — შესაბამისად უფრო გრძელი მხარდაჭერა უნდა ჰქონდეს. ამ პერიოდის დასრულების თარიღი მყიდველს შეძენისას უნდა ეცნობოს, ხოლო ტექნიკური დოკუმენტაცია სულ მცირე ათი წლის განმავლობაში — ან მხარდაჭერის მთელი პერიოდის განმავლობაში, თუ ის უფრო გრძელია — ხელმისაწვდომი უნდა დარჩეს; მოქმედებს ის ვადა, რომელიც მომხმარებელს მეტ დაცვას აძლევს.

ამით ის, რაც აქამდე მარკეტინგული არჩევანი იყო — რამდენ ხანს გაუგრძელებდა მიმწოდებელი მოწყობილობას მხარდაჭერას — საჯარო და სამართლებრივად სავალდებულო ვალდებულებად იქცევა. რთულია გადაჭარბებით შეფასდეს, რამხელა ცვლილებაა ეს ინდუსტრიისთვის, რომელიც ახალი მოდელის გამოშვებისთანავე ძველის მიტოვებას არის შეჩვეული.

ანგარიშგების ვადები: 24 საათი, 72 საათი და შემდგომი ეტაპები

2026 წლის 11 სექტემბრიდან მწარმოებლები ვალდებული არიან, ნებისმიერი აქტიურად ექსპლუატირებული მოწყვლადობისა და პროდუქტის უსაფრთხოებაზე მოქმედი ნებისმიერი

მძიმე ინციდენტის შესახებ ერთდროულად და ერთიანი ანგარიშგების პლატფორმის მეშვეობით აცნობონ კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ეროვნულ ჯგუფს (CSIRT) და ევროკავშირის კიბერუსაფრთხოების სააგენტოს (ENISA). ვადები შეგნებულად მკაცრია: პრობლემის შესახებ ინფორმაციის მიღებიდან ოცდაოთხ საათში — ადრეული გაფრთხილება, სამოცდათორმეტ საათში — უფრო სრული შეტყობინება, ხოლო საბოლოო ანგარიში ექსპლუატირებული მოწყვლადობის შემთხვევაში გამოსწორების გამოქვეყნებიდან თოთხმეტ დღეში, მძიმე ინციდენტის შემთხვევაში კი სამოცდათორმეტსაათიანი შეტყობინებიდან ერთ თვეში უნდა წარედგინოს.

ეს ვადები შეგნებულად შეესაბამება NIS2-ით დადგენილ ვადებს — გადაწყვეტილება, რომელსაც ინდუსტრიის არაერთი გაერთიანება მიესალმა. სხვაგვარად ერთი და იგივე ინციდენტი, რომელიც პროდუქტის მწარმოებელსაც ეხება და მის გამომყენებელ ოპერატორსაც, ორ სხვადასხვა ანგარიშგების ვადას სხვადასხვა გრაფიკით ამოქმედებდა. ვადების ასეთი შეთანხმება ფორმალური ჟესტი არ არის: სწორედ ის აძლევს ორივე რეჟიმში მოხვედრილ ფირმებს საშუალებას, ორივე მოთხოვნა ერთდროულად და ადმინისტრაციულად ასატანი ხარჯით დააკმაყოფილონ.

ყველაზე მცირე ფირმებისთვის მოკლე გარდამავალი გამონაკლისია გათვალისწინებული: მიკრო და მცირე საწარმოებს მხოლოდ ოცდაოთხსაათიანი ვადის დარღვევისთვის ჯარიმა არ დაეკისრებათ, თუმცა ანგარიშგების ვალდებულება მათზეც ვრცელდება. ეს დათმობა, რაოდენ უმნიშვნელოც არ უნდა ჩანდეს ქაღალდზე, საკანონმდებლო პროცესის ერთ-ერთი ყველაზე სადავო დეტალი იყო და ამ რეგულაციისთვის დამახასიათებელ სქემას კარგად ასახავს: ნორმა მთელი ბაზრისთვის იწერება და შემდეგ იმ მონაწილეებისთვის რბილდება, რომლებსაც მისი შესრულება ყველაზე უჭირთ.

მთლიანობაში, ეს არქიტექტურა რამდენიმე დღეში გამჟღავნებულ და გამოსწორებულ მოწყვლადობას საქმიანობის ჩვეულებრივ, მართვად ხარჯად მიიჩნევს, დაფარულ ან აღმოუფხვრელ მოწყვლადობას კი — თავისთავად მარეგულირებელი ნორმის დარღვევად. ეს განსხვავება რეალურ შედეგებს მაშინ იძენს, როცა VII ნაწილში განხილული აღსრულების დებულებები ამოქმედდება.

V. შესაბამისობის შეფასება და ბაზარზე დაშვება: თვითსერტიფიცირება, შეტყობინებული ორგანოები და CE მარკირება

ზედამხედველობის საფეხურებრივი სისტემა

ყველა მიერთებული პროდუქტი ერთნაირ რისკს არ შეიცავს და კიბერმედეგობის აქტიც მათ ერთნაირად არ ეპყრობა. რეგულაცია პროდუქტებს ძირითად კატეგორიად და მომატებული რისკის ორ კატეგორიად ყოფს — ზოგადად, ციფრული ელემენტების შემცველ „მნიშვნელოვან“ პროდუქტებად (I და II კლასი) და „კრიტიკული“ პროდუქტების უფრო ვიწრო ჯგუფად — იმის მიხედვით, რა ფუნქციას ასრულებს პროდუქტი და რა შედეგები მოჰყვება მის მწყობრიდან გამოსვლას. პაროლების მმართველები, ქსელური ეკრანები (firewall) და კრიტიკული ინფრასტრუქტურის საოპერაციო სისტემები უფრო მკაცრი კონტროლის საფეხურებზეა; ჭკვიანი ჩაიდანი, ჩვეულებრივ, არა.

ძირითადი კატეგორიის პროდუქტებისთვის მწარმოებელს შეუძლია I დანართის მოთხოვნებთან შესაბამისობა თავად შეაფასოს. მომატებული რისკის საფეხურებისთვის რეგულაცია გარე

შემოწმებას მოითხოვს — ან ჰარმონიზებული სტანდარტების სრული გამოყენებით, ან, სათანადო სტანდარტების არარსებობისას, **შეტყობინებული ორგანოს** მიერ ჩატარებული შეფასებით. შეტყობინებული ორგანო შესაბამისობის შეფასების ორგანიზაციაა, რომელსაც წევრი სახელმწიფო ნიშნავს და რომელიც მთელ კავშირში აღიარებულია. შეფასების წარმატებით გავლის შემდეგ მწარმოებელი ევროკავშირის შესაბამისობის დეკლარაციას ადგენს და პროდუქტს CE მარკირებას უკეთებს — იმავე ვიზუალურ ნიშანს, რომელსაც ევროპელი მომხმარებელი ფიზიკური პროდუქტების უსაფრთხოებას უკავშირებს და რომელიც ახლა პროდუქტის კიბერუსაფრთხოების შესახებაც მიუთითებს.

CE მარკირების მიღმა არსებული სტანდარტების პრობლემა

CE მარკირების სანდოობა მთლიანად იმაზეა დამოკიდებული, არსებობს თუ არა ჰარმონიზებული ტექნიკური სტანდარტები, რომლებიც I დანართის ფართო პრინციპებს კონკრეტულ, შემოწმებად შინაარსს აძლევს — და ეს სტანდარტები საკანონმდებლო გრაფიკს ჩამორჩა. ეს შემთხვევითი შეფერხება არ არის. სწორედ ამიტომ ხელოვნური ინტელექტის შესახებ ციფრული ომნიბუსის წინადადება, რომელიც კიბერმედეგობის აქტის პარალელურად განიხილება ინსტიტუტებში, ხელოვნური ინტელექტის აქტით გათვალისწინებული მაღალი რისკის მსგავსი ვალდებულებების ამოქმედებას ფიქსირებულ თარიღს კი არ უკავშირებს, არამედ დამხმარე სტანდარტების რეალურ არსებობას. ევროკომისიის სახელმძღვანელო იმავე დაძაბულობას კიბერმედეგობის აქტთან დაკავშირებითაც აღიარებს: მწარმოებლებმა შესაბამისობა უნდა დაადასტურონ იმ მოთხოვნებთან, რომელთა დეტალური ტექნიკური საზომი ზოგან ჯერ კიდევ არ არსებობს.

შედეგად დგება პერიოდი — სავარაუდოდ 2026 წელი და 2027 წლის ნაწილი — როდესაც შესაბამისობის შეფასება უფრო მეტად მწარმოებლების საკუთარ ტექნიკურ მსჯელობას დაეყრდნობა, რომელიც სტანდარტების პროექტებსა და ევროკომისიის განმარტებებს ეფუძნება, ვიდრე რეგულაციის ავტორებს თავდაპირველად ჰქონდათ განზრახული. ეს გადამწყვეტი ხარვეზი არ არის. ეს შეხსენებაა, რომ CE მარკირება მხოლოდ იმდენად საიმედოა, რამდენადაც მის უკან მდგარი სტანდარტების ინფრასტრუქტურა, ამ ინფრასტრუქტურის აშენებას კი საკანონმდებლო ტექსტის მიღებაზე მეტი დრო სჭირდება.

საფეხურებრივი შეფასების მოდელი ყველაზე მკაფიოდ გამოხატავს პრინციპს, რომელიც მთელ რეგულაციას გასდევს: პროპორციულობა განისაზღვრება შესაძლო შედეგით და არა მწარმოებლის მიმართ დამოკიდებულებით. ზედამხედველობის მოცულობას პროდუქტის რისკის საფეხური განსაზღვრავს.

VI. ღია წყაროს კომპრომისი: მმართველები და არა მწარმოებლები

პროტესტი, რომელმაც ტექსტი შეცვალა

მიღებამდე კიბერმედეგობის აქტის არც ერთ ნაწილს არ გამოუწვევია ისეთი ხანგრძლივი კამათი, როგორიც თავისუფალი და ღია წყაროს პროგრამული უზრუნველყოფისადმი მის მიდგომას მოჰყვა. 2022 წლის დასაწყისის პროექტი გამონაკლისს აწესებდა ღია წყაროს იმ პროგრამული უზრუნველყოფისთვის, რომელიც „კომერციული საქმიანობის ფარგლებს გარეთ“ იყო შემუშავებული. ამ ფორმულირებამ ღია წყაროს საზოგადოება შეაშფოთა, და ეს შეშფოთება მხოლოდ სემანტიკას არ ეხებოდა. **OpenForum Europe**-მა, **Open Source Initiative**-მა და ღია წყაროს სფეროში მოქმედი ფონდების კოალიციამ გააფრთხილეს, რომ გამონაკლისის ფორმულირება არ

შეესაბამებოდა იმას, როგორ ფუნქციონირებენ ღია წყაროს პროექტები სინამდვილეში: სპონსორობით, შეცდომების აღმოჩენის ჯილდოებით, კორპორაციული წვლილითა და არაფორმალური მხარდაჭერით, რაც „კომერციულ“ და „არაკომერციულ“ საქმიანობას შორის ნებისმიერ მკაფიო ზღვარს შლის. Open Source Initiative-ის საიმონ ფიფსი (Simon Phipps) უფრო შორს წავიდა: მისი თქმით, განუსაზღვრელი პასუხისმგებლობის წინაშე მდგომმა დეველოპერებმა შესაძლოა ევროპელი მომხმარებლების წვდომა უბრალოდ გეოგრაფიულად დაბლოკონ, იმის ნაცვლად, რომ რისკი იკისრონ. ასეთ შემთხვევაში რეგულაცია, რომელიც ევროპელთა უსაფრთხოებისთვის შეიქმნა, მათ, პირიქით, გლობალურ დონეზე შენარჩუნებულ უსაფრთხოების განახლებებს მოწყვეტდა.

საბოლოო ტექსტი ამ პროტესტს სპეციალურად შექმნილი კატეგორიით პასუხობს — ეს **ღია წყაროს პროგრამული უზრუნველყოფის მმართველია**: როგორც წესი, ფონდი ან მსგავსი იურიდიული პირი, რომელიც კომერციული გამოყენებისთვის განკუთვნილი ღია წყაროს პროდუქტების განვითარებას მდგრად და სისტემატურ მხარდაჭერას უწევს, თავად კი მათ არ აწარმოებს და არ ყიდის. საკანონმდებლო დებატებში ტიპურ მაგალითებად სწორედ Linux Foundation და Apache Software Foundation იგულისხმებოდა. მმართველებზე უფრო მსუბუქი, მათთვის მორგებული რეჟიმი ვრცელდება: დოკუმენტირებული კიბერუსაფრთხოების პოლიტიკა, საბაზრო ზედამხედველობის ორგანოებთან თანამშრომლობა და მოწყვლადობებზე ანგარიშგება მხოლოდ იმდენად, რამდენადაც ისინი პროდუქტის შემუშავებაში რეალურად მონაწილეობენ. რაც მთავარია, 64-ე მუხლის მე-10 პუნქტი მათ იმ ადმინისტრაციული ჯარიმებისგან ათავისუფლებს, რომლებიც მწარმოებლებზე ვრცელდება. ეს პირდაპირი აღიარებაა იმისა, რომ არაკომერციული ფონდის კომერციულ მიმწოდებელთან გათანაბრება არაპროპორციული და, სავარაუდოდ, თვითდამაზიანებელიც იქნებოდა.

გადაუჭრელი დაძაბულობა და არა დახურული საკითხი

ეს კომპრომისი თავდაპირველ პროექტზე უფრო განხორციელებადია, თუმცა ძირითადი კამათი მან არ ჩააქრო. მიღების შემდეგ გამოქვეყნებული აკადემიური შეფასებები — მათ შორის *Journal of Intellectual Property, Information Technology and E-Commerce Law*-ში გამოქვეყნებული ანალიზი — ასკვნის, რომ კიბერმედეგობის აქტი „ნამდვილად აღწევს ბალანსს ღია წყაროს პროგრამული უზრუნველყოფის რეგულირებასა და კიბერუსაფრთხოების გაძლიერებას შორის, თუმცა მხოლოდ ვიწროდ გამოსაყენებელი და ზოგჯერ რთული საკანონმდებლო მიდგომით“. სიტყვა „რთული“ ამ წინადადებაში შემთხვევითი არ არის. მმართველის ვალდებულებები იმაზეა დამოკიდებული, კონკრეტულად როგორ მონაწილეობს იგი მოცემული პროდუქტის შემუშავებაში. ეს ფაქტობრივ გარემოებებზე დამოკიდებული ტესტია, და მცირე ფონდებს, რომლებსაც საკუთარი იურისტი არ ჰყავთ, მისი თავდაჯერებულად გამოყენება შესაძლოა გაუჭირდეთ.

სამეცნიერო ლიტერატურის ცალკე მიმართულება ღია წყაროს დებულებებს **ციფრული სუვერენიტეტის** ჭრილში განიხილავს. მისი მტკიცებით, ევროკავშირის სწრაფვა პროგრამული უზრუნველყოფის მიწოდების ჯაჭვებზე მეტი კონტროლისკენ ძნელად ეთავსება განვითარების იმ მოდელს, რომელიც ღიაობასა და ნებაყოფლობით გლობალურ თანამშრომლობაზეა აგებული. ეს კრიტიკა იმას არ ამბობს, რომ კიბერმედეგობის აქტი ღია წყაროს მიმართ მტრულადაა განწყობილი — რეგულაციის პრეამბულა მის წვლილს ინოვაციაში საგანგებოდ აღნიშნავს. მაგრამ იგი მიანიშნებს, რომ კავშირის მარეგულირებელი რეფლექსები და ღია წყაროს მუშაობის ლოგიკა

განხორციელების პროცესში კვლავ შეეჯახება ერთმანეთს, განსაკუთრებით იქ, სადაც ჯეროვანი გულისხმიერების ვალდებულებები აუნაზღაურებელ, არაფორმალურ წვლილს შეეხება.

ამ ისტორიის ღია წყაროსთან დაკავშირებული ნაწილი გვიჩვენებს იმას, რისი გადაჭრაც კიბერმედეგობის აქტს მხოლოდ ტექსტის ფორმულირებით არ შეუძლია: მწარმოებლებისა და პროდუქტების ლოგიკაზე აგებული კანონი ყოველთვის გარკვეულ შეუთავსებლობაში იქნება იმ განვითარების კულტურასთან, რომელიც წვლილის შემტანებსა და საერთო რესურსზეა აგებული — რაოდენ ფრთხილადაც არ უნდა იყოს დეფინიციები ჩამოყალიბებული.

VII. აღსრულება და მოთხოვნების დაუცველობის ფასი

ჯარიმები, გათვლილი შეკავებაზე და არა მხოლოდ დასჯაზე

კიბერმედეგობის აქტი სანქციების დეტალურ დიზაინს წევრ სახელმწიფოებს უტოვებს, თუმცა ადგენს ზედა ზღვარს, რომელიც დირექტორთა საბჭოებს დააფიქრებს: ადმინისტრაციული ჯარიმა 15 მილიონ ევრომდე ან კომპანიის წინა საფინანსო წლის მთლიანი მსოფლიო წლიური ბრუნვის 2,5%-მდე — ამ ორიდან უფრო მაღალი. GDPR-იდან ნაცნობი ეს ფორმულა შეგნებული სიგნალია: ბრიუსელი პროდუქტების კიბერუსაფრთხოებას მონაცემთა დაცვის ტოლი სერიოზულობით ეკიდება და მას მონაცემთა დაცვის მეორეხარისხოვან ტექნიკურ დანართად არ მიიჩნევს.

ფინანსურ სანქციებს უფრო მყისიერი ეფექტის მქონე ინსტრუმენტებიც ახლავს: ეროვნულ საბაზრო ზედამხედველობის ორგანოებს შეუძლიათ პროდუქტის გაყიდვიდან ამოღება მოითხოვონ, იგი ბაზრიდან გამოითხოვონ ან მისი ხელმისაწვდომობა მაკორექტირებელი ზომების მიღებამდე შეზღუდონ. მწარმოებლისთვის პროდუქტის გამოთხოვის ბრძანება ხშირად თანმხლებ ჯარიმაზე მძიმეა: რეპუტაციული ზიანი და გაყიდვების არხების დაკარგვა ერთჯერად ჯარიმაზე უფრო სწრაფად იზრდება. სწორედ ეს ასიმეტრია ანიჭებს საბაზრო ზედამხედველობის უფლებამოსილებებს რეალურ ძალას.

ვინ ახორციელებს რეალურ კონტროლს

აღსრულების უფლებამოსილება ძირითადად ეროვნულ საბაზრო ზედამხედველობის ორგანოებს ეკუთვნის. მათ შეუძლიათ ტექნიკური დოკუმენტაცია გამოითხოვონ, ტესტირება დანიშნონ და როგორც საჩივრის საფუძველზე, ისე საკუთარი ინიციატივით იმოქმედონ. ENISA და CSIRT-ების ქსელი საკოორდინაციო როლს ასრულებენ, უპირველესად მე-14 მუხლით შექმნილი მოწყვლადობებისა და ინციდენტების ანგარიშგების არხის მეშვეობით. ეს ნამდვილად ფედერალური ტიპის აღსრულების მოდელია: წესები ბრიუსელში დგინდება, ინსპექტორები კი, უმეტესწილად, ეროვნული მთავრობების დაქვემდებარებაში არიან. ფუნქციების ასეთმა განაწილებამ ევროკავშირის პროდუქტების უსაფრთხოების სამართალს ფიზიკური საქონლის შემთხვევაში საკმაოდ კარგად მოემსახურა. შეძლებს თუ არა ოცდაშვიდი — ზომითა და ტექნიკური შესაძლებლობებით განსხვავებული — ეროვნული უწყება იმავე სიმკაცრით მიუდგეს სწრაფად ცვალებად პროგრამულ პროდუქტებს, რეგულაციის ერთ-ერთი ნამდვილად ღია საკითხია, და პასუხი მასზე მხოლოდ პირველი სერიოზული აღსრულების საქმეების შემდეგ გაირკვევა.

მთლიანობაში, აღსრულების არქიტექტურა მწარმოებლებს მარტივ, მაგრამ მნიშვნელოვან რამეს ეუბნება: კიბერუსაფრთხოების ჩავარდნა აღარ არის მხოლოდ რეპუტაციული ან კომერციული რისკი, რომელიც კომპანიამ შიდა რესურსებით უნდა მართოს. ეს ახლა მარეგულირებელი

რისკია, რომელიც იმავე ინსტიტუციური მექანიზმებით — და სულ უფრო ხშირად იმავე ფინანსური მასშტაბით — ისჯება, როგორც კავშირის მონაცემთა დაცვის სამართლის დარღვევა.

VIII. გრძელი და ეტაპობრივი გზა: კიბერმედეგობის აქტის ფაზებად დაყოფილი ვადები

ოთხი მნიშვნელოვანი თარიღი

რეგულაცია ძალაში 2024 წლის 10 დეკემბერს შევიდა, თუმცა ევროკავშირის სამართალში „ძალაში შესვლა“ და „გამოყენების დაწყება“ სხვადასხვა რამაა, და აქ მათ შორის სხვაობა უჩვეულოდ დიდი და შეგნებულად ეტაპობრივია. გარდამავალ პერიოდს ოთხი თარიღი განსაზღვრავს. შესაბამისობის შეფასების ორგანოების შეტყობინებასთან დაკავშირებული მმართველობითი დებულებები 2026 წლის 11 ივნისიდან მოქმედებს, რათა მაღალი რისკის პროდუქტების სერტიფიცირებისთვის საჭირო ინფრასტრუქტურა უკვე არსებობდეს, სანამ მწარმოებლებს მისი გამოყენება მოეთხოვებათ. მე-14 მუხლით გათვალისწინებული ანგარიშგების ვალდებულებები — IV ნაწილში აღწერილი ოცდაოთხ და სამოცდათორმეტსაათიანი შეტყობინების მოვალეობები — 2026 წლის 11 სექტემბრიდან მოქმედებს; ამ ანალიზის წერის მომენტისთვის ეს თარიღი ახლახან დადგა. არსებითი ვალდებულებების უდიდესი ნაწილი, მათ შორის III და V ნაწილებში აღწერილი კიბერუსაფრთხოების არსებითი მოთხოვნები და შესაბამისობის შეფასების პროცედურები, 2027 წლის 11 დეკემბრიდან ამოქმედდება. პროდუქტების უფრო ვიწრო კატეგორია, რომელიც ამ თარიღამდე უკვე ბაზარზეა, რეგულაციის მიღმა რჩება, თუ მასში არსებითი ცვლილება არ შევიდა; ანგარიშგების მოვალეობები კი მათზეც ვრცელდება.

ვადების ასეთი ეტაპობრივი დაყოფა გააზრებული არჩევანი იყო და არა შემთხვევითობა. იგი სტანდარტების დამდგენ ორგანოებს, შეტყობინებულ ორგანოებსა და ეროვნულ უწყებებს დროს აძლევს, ის ინფრასტრუქტურა ააგონ, რომლის არსებობასაც რეგულაცია გულისხმობს, და ამავე დროს ყველაზე გადაუდებელ ვალდებულებას — შეტყობინებას იმის თაობაზე, რომ პროდუქტის მოწყვლადობა აქტიურად გამოიყენება შეტევებისთვის — დანარჩენებზე წლებით ადრე ამოქმედებს.

ფარული დაძაბულობა ვადის ირგვლივ

მიუხედავად ამისა, რომ 2026 წლის სექტემბრის ვადის ირგვლივ გამოქვეყნებული ინდუსტრიული ანალიზი შესაბამისობის ისეთ გარემოს აღწერს, რომელიც ჯერ კიდევ შექმნის პროცესშია. I დანართის არაერთი მოთხოვნისთვის ჰარმონიზებული სტანდარტები დაუსრულებელია; ევროკომისიამ დასრულებული ტექნიკური ნორმების ნაცვლად შუალედური პრაქტიკული სახელმძღვანელოებით უპასუხა — უკანასკნელი მათგანი 2026 წლის 27 ივლისს, ანგარიშგების ვალდებულების ამოქმედებამდე რამდენიმე კვირით ადრე გამოქვეყნდა. ასეთი თანმიმდევრობა — სახელმძღვანელო სამართლებრივი ვადის უშუალოდ წინ ჩნდება და არა ბევრად ადრე — ევროკავშირის ციფრული რეგულირების მსხვილი პროექტების ამოსაცნობ ნიშნად იქცა, და კიბერმედეგობის აქტი, ზოგიერთის იმედის მიუხედავად, გამონაკლისი არ აღმოჩნდა.

ეს არ ნიშნავს, რომ ვადები ფორმალურად გადაიწევს: რეგულაციაში ჩაწერილი თარიღები სავალდებულო სამართალია და არა მისწრაფება. ეს ნიშნავს, რომ 2026 წლის მეორე ნახევარში შესაბამისობის უზრუნველყოფა პრაქტიკაში დასრულებული წესების დაცვას ნაკლებად დაემსგავსება და უფრო ზოგადი პრინციპების გამოყენებას, მაშინ როცა მათი ზუსტი ტექნიკური შინაარსი კვლავ გაურკვეველია. ფიზიკური საქონლის მწარმოებლებს ასეთი მდგომარეობის

ატანა იშვიათად უწევთ, და სწორედ ეს ხსნის ნაწილობრივ შესაბამისობის ტვირთის შესახებ დებატებს, რომლებსაც შემდეგ ნაწილში განვიხილავთ.

IX. გამარტივების დაღლილობა: მცირე და საშუალო საწარმოები, კონკურენტუნარიანობა და შესაბამისობის ტვირთის პოლიტიკა

რას აჩვენებს მონაცემები მცირე მწარმოებლების შესახებ

ENISA-ს 2026 წლის კვლევა, რომელიც მცირე და საშუალო ზომის მწარმოებლებს შორის ევროკომისიის მცირე და საშუალო საწარმოების კიბერუსაფრთხოების სტრატეგიის ფარგლებში ჩატარდა, უჩვეულოდ პირდაპირ გვიჩვენებს, როგორ აისახება კიბერმედეგობის აქტი იმ ბიზნესებზე, რომლებსაც მისი შესრულება ყველაზე უჭირთ. რესპონდენტთა ორმა მესამედმა განაცხადა, რომ რეგულაციას უკვე იცნობდა, თუმცა ცოდნა თავდაჯერებულობად არ ქცეულა: ყველაზე სუსტ მხარეებად ტექნიკური დოკუმენტაცია და შესაბამისობის შეფასება დასახელდა, ყველაზე ხშირად მოთხოვნილ დახმარებად კი — ფინანსური მხარდაჭერა. მიკროკომპანიების ერთ მესამედზე მეტს ინციდენტზე რეაგირების გეგმა საერთოდ არ აქვს — ანუ სწორედ ის, რასაც კიბერმედეგობის აქტით განსაზღვრული ანგარიშგების ვადები თავისთავად გულისხმობს.

ეს სხვაობა სამართლებრივ ვალდებულებასა და ორგანიზაციულ შესაძლებლობას შორის მეორეხარისხოვანი დეტალი არ არის — ეს რეგულაციის სანდოობის მთავარი პრაქტიკული რისკია. წესი, რომელიც უსაფრთხოების ისეთ სიმწიფეს გულისხმობს, როგორიც მიკროსაწარმოების უმეტესობას ჯერ არ აქვს, ორიდან ერთ შედეგს გამოიწვევს: ან აიძულებს მათ, ამ სიმწიფეში რეალურად ჩადონ ინვესტიცია — რასაც რეგულაციის ავტორები ისახავენ მიზნად — ან ყველაზე პატარა და ყველაზე მწირი რესურსების მქონე მწარმოებლებს არასრული ანგარიშგებისკენ, ფარული შეუსაბამობისკენ ან ევროკავშირის ბაზრიდან საერთოდ წასვლისკენ უბიძგებს. რომელი შედეგი გადაწონის, რამდენიმე წლის განმავლობაში არ გაირკვევა.

რეგულაცია უფრო დიდი პოლიტიკური დინების ტყვეობაში

კიბერმედეგობის აქტის შესაბამისობის ტვირთი ამავე დროს ერთგვარ სიმბოლოდ იქცა გაცილებით ფართო დავაში ევროკავშირის მარეგულირებელი პოლიტიკის მიმართულების შესახებ. ბიზნესგაერთიანებები, მათ შორის კავშირის სავაჭრო პალატების წარმომადგენელი **Eurochambres**, რეგულაციის მიზნებს მიესალმნენ, თუმცა უფრო ძლიერი გარანტიები მოითხოვეს წევრი სახელმწიფოების მიერ ზედმეტი ეროვნული დამატებების („gold-plating“) წინააღმდეგ და კიბერმედეგობის აქტის, NIS2-ისა და კიბერუსაფრთხოების აქტის უფრო მკაფიო ურთიერთშესაბამისობა, რათა ერთ კომპანიას ერთი ინციდენტისთვის სამი გადამფარავი ანგარიშგების მოვალეობა არ დაეკისროს. ფართო ბიზნესაუდიტორიისთვის განკუთვნილი კომენტარები გაცილებით ნაკლებად თავშეკავებული იყო: მათში კიბერმედეგობის აქტი წარმოდგენილია როგორც კიდევ ერთი ჩანაწერი წესების იმ გრძელ ნუსხაში, რომელიც, ერთობლიობაში, ევროპულ მცირე ტექნოლოგიურ ფირმებს საკუთარი ბაზრიდან განდევნის საფრთხეს უქმნის — არსებითად იგივე არგუმენტი, რომელიც ევროკომისიის საკუთარ ციფრული ომნიბუსის გამარტივების პაკეტს ასაზრდოებს.

ის, რომ ევროკომისია ერთდროულად კიბერმედეგობის აქტის არსს იცავს და ციფრული კანონმდებლობის სხვა ნაწილებში ჰორიზონტალურ გამარტივებას ატარებს, წინააღმდეგობა არ არის. ეს იმის ანარეკლია, საით წავიდა ევროპული პოლიტიკა 2022 წლის შემდეგ, როცა რეგულაცია პირველად შემოთავაზდა. ეს რეგულაცია მაშინ ჩაფიქრდა, როცა ევროკავშირი

ყველაზე მეტად იყო დარწმუნებული რეგულირების გზით გლობალური სტანდარტების დაწესების საკუთარ უნარში; ახლა კი კონკურენტუნარიანობაზე გაცილებით მეტად შეშფოთებულ პოლიტიკურ გარემოში ხორციელდება. ამ ცვლილებას წინამდებარე გამოცემა ამ სერიაში განხილული არაერთი აქტის მაგალითზე ადევნებდა თვალს — ციფრული სერვისების აქტიდან კრიტიკული ნედლეულის აქტამდე.

შესაბამისობის ტვირთის შესახებ დავას წინამდებარე ანალიზი ვერ გადაწყვეტს და არც უნდა გადაწყვიტოს. დარწმუნებით მხოლოდ ის შეიძლება ითქვას, რომ კიბერმედეგობის აქტის საბოლოო რეპუტაცია — ამბიციური დამცავი მექანიზმი თუ ზედმეტი ტვირთი — არა იმდენად მისი ტექსტით, რამდენადაც იმით განისაზღვრება, განხორციელდება თუ არა რეალურად მცირე მწარმოებლებისთვის დაპირებული ფინანსური და ტექნიკური მხარდაჭერა 2027 წლის დეკემბრის ვადის დადგომამდე.

X. სად დგას კიბერმედეგობის აქტი ევროკავშირის კიბერუსაფრთხოების არქიტექტურაში

პროდუქტის წესები ორგანიზაციული წესების გვერდით

კიბერმედეგობის აქტი იზოლირებულად არ მოქმედებს. იგი პროდუქტის დონეზე ავსებს NIS2-ის ორგანიზაციულ მოთხოვნებსა და კიბერუსაფრთხოების აქტის ნებაყოფლობითი სერტიფიცირების ჩარჩოს. სამი ინსტრუმენტი ერთად სამ საკითხს ფარავს: როგორი უნდა იყოს პროდუქტი, როგორ უნდა მოიქცეს მისი გამომყენებელი ორგანიზაცია და როგორ შეუძლია ორივეს, უსაფრთხოების შესახებ საკუთარი განაცხადები დამოუკიდებლად დაადასტუროს. IV ნაწილში განხილული ანგარიშგების ვადების შეთანხმება ყველაზე მკაფიო მტკიცებულებაა იმისა, რომ ევროკომისიამ ეს ინსტრუმენტები ერთმანეთის შემავსებლად და არა კონკურენტებად შექმნა, თუმცა ისინი სხვადასხვა დროს და სხვადასხვა საკანონმდებლო პროცედურით მიიღეს.

ეს არქიტექტურა ამჟამად კვლავ ფართოვდება. კიბერუსაფრთხოების აქტის შემოთავაზებული გადასინჯვა — არაფორმალურად **CSA2** — ევროკომისიას ახალ უფლებამოსილებას მისცემდა: განესაზღვრა „მაღალი რისკის მესამე ქვეყნები“ და კონკრეტული მიმწოდებლები საინფორმაციო-საკომუნიკაციო ტექნოლოგიების სენსიტიური მიწოდების ჯაჭვებიდან გამოერიცხა. ამით 2019 წლის 5G ინსტრუმენტთა ნაკრების ლოგიკა ნებაყოფლობითი რეკომენდაციიდან სავალდებულო მექანიზმად გადაიქცეოდა. *Euractiv*-ში გამოქვეყნებულმა სამართლებრივმა კომენტარმა ამ წინადადებასთან დაკავშირებით სერიოზული ინსტიტუციური საკითხი დააყენა: წინადადება იმავე შიდა ბაზრის სამართლებრივ საფუძველზეა აგებული, რომელზეც თავად კიბერმედეგობის აქტი, თუმცა არსებითად, შესაძლოა, ეროვნულ უსაფრთხოებას ემსახურებოდეს — სფეროს, რომელიც ევროკავშირის შესახებ ხელშეკრულების მე-4 მუხლის მე-2 პუნქტით მხოლოდ წევრი სახელმწიფოების კომპეტენციაა. თუ ეს არგუმენტი მართლმსაჯულების სასამართლოში გაიმარჯვებს, კიბერმედეგობის აქტს ეს პირდაპირ არ შეეხება, მაგრამ კარგად გვიჩვენებს, რამდენად სადავო გახდა კიბერუსაფრთხოების სფეროში „შიდა ბაზრის“ კომპეტენციის საზღვარი. ამის აღნიშვნა იმიტომაც არის საჭირო, რომ ზოგად კომენტარებში CSA2-ს ხშირად — და არასწორად — კიბერმედეგობის აქტთან აიგივებენ. ეს მონათესავე ინსტრუმენტებია, რომლებიც სხვადასხვა მიზანს სხვადასხვა მექანიზმით ემსახურება, და მკითხველმა თავი უნდა შეიკავოს მათი ერთ „ევროკავშირის კიბერუსაფრთხოების პაკეტად“ გაერთიანებისგან.

ხელოვნური ინტელექტის აქტის ჩრდილი

შეხების კიდევ ერთი წერტილი **ხელოვნური ინტელექტის აქტია**, რომელიც ამ სერიაში უკვე განვიხილეთ. თუ ციფრული ელემენტების შემცველი პროდუქტი ამავე დროს მაღალი რისკის ხელოვნური ინტელექტის სისტემადაც ითვლება, კიბერმედეგობის აქტით მოთხოვნილი კიბერუსაფრთხოების რისკის შეფასება ხელოვნური ინტელექტის აქტით უკვე გათვალისწინებულ რისკის შეფასებაში შეიძლება ჩაერთოს და ცალკე არ გამეორდეს. ეს კავშირი პრაქტიკულად მნიშვნელოვანია ყველა იმ ფირმისთვის, რომელიც ჩაშენებული ხელოვნური ინტელექტის ფუნქციების მქონე მიერთებულ პროდუქტებს ქმნის — რაც ინდუსტრიაში სულ უფრო ნორმაა და არა გამონაკლისი. ეს იმ მარეგულირებელი გარემოს ერთ-ერთი ნამდვილად გამამარტივებელი ელემენტია, რომელსაც უფრო ხშირად ახალი ფენების დამატებას უსაყვედურებენ, ვიდრე მათ მოხსნას.

ერთად აღებული, ეს ურთიერთგადამფარავი ინსტრუმენტები ევროკავშირის კიბერუსაფრთხოების ისეთ არქიტექტურას ქმნის, რომელიც ჯერ კიდევ შენების პროცესშია: მისი ნაწილები სხვადასხვა დროს, სხვადასხვა შეშფოთების საპასუხოდ დაემატა და ახლა — არა ყოველთვის გლუვად — ერთ მთლიანობად იკერება, რომელიც, ავტორების იმედით, საბოლოოდ თანმიმდევრულ სისტემად და არა მომიჯნავე ნორმების კრებულად იმუშავებს.

XI. მნიშვნელობა ევროკავშირში გაწევრიანების მსურველი ქვეყნებისთვის

წესების კრებული, რომლის გადმოტანაც კანდიდატ ქვეყნებს საბოლოოდ მოუწევთ

იმ ცხრა ქვეყნისთვის, რომლებიც ამჟამად ევროკავშირში გაწევრიანებაზე მოლაპარაკებებს აწარმოებენ ან მათ დაწყებას ელოდებიან — უკრაინა, მოლდოვა, საქართველო და დასავლეთ ბალკანეთის ექვსი სახელმწიფო: ალბანეთი, ბოსნია და ჰერცეგოვინა, კოსოვო, მონტენეგრო, ჩრდილოეთ მაკედონია და სერბეთი — კიბერმედეგობის აქტი ჯერ პირდაპირი სამართლებრივი ვალდებულება არ არის, თუმცა იგი წინასწარ წარმოდგენას გვაძლევს იმ *acquis*-ის შესახებ, რომლის გადმოტანაც თითოეულ ქვეყანას საბოლოოდ მოუწევს. ევროკავშირის უსაფრთხოების კვლევების ინსტიტუტმა (EUISS) 2026 წლის ანალიტიკურ მიმოხილვაში აღნიშნა, რომ გაფართოების პროცესში ციფრული და კიბერუსაფრთხოების საკითხებზე დაახლოება „დიდწილად თანდათანობით, შესაბამისობაზე ორიენტირებულ გაწევრიანების პროცესშია ჩაშენებული“, და რომ რეგულაციების გადმოტანა ხშირად წინ უსწრებს იმ ოპერაციულ შესაძლებლობებს, რომელთა გარეშე ეს ნორმები პრაქტიკაში ვერ მუშაობს. ეს გაფრთხილება კიბერმედეგობის აქტს განსაკუთრებით ეხება: რეგულაცია შეტყობინებული ორგანოების, ეროვნული საბაზრო ზედამხედველობის უწყებებისა და CSIRT-ების მთელ ეკოსისტემას გულისხმობს, რომლის აშენებას თავად ევროკავშირის ოცდაშვიდეულს წლები დასჭირდა და რომელიც შესადარისი სახით ჯერ არც ერთ კანდიდატ ქვეყანას არ აქვს.

ამ ქვეყნებს შორის სამართლებრივი საწყისი პირობები საგრძნობლად განსხვავდება, და ეს განსხვავება იმაზეც აისახება, როგორ მიუდგება თითოეული მათგანი გადმოტანას. EU4Digital-ის შეფასებებით, აღმოსავლეთ პარტნიორობის ქვეყნებს შორის საქართველო ერთადერთია, რომელმაც კიბერუსაფრთხოების ეროვნული სტრატეგიის უკვე მესამე თაობა შეიმუშავა; მოლდოვა და უკრაინა თავიანთ სტრატეგიებს ჯერ კიდევ აახლებდნენ, სომხეთს, აზერბაიჯანსა და ბელარუსს კი ასეთი სტრატეგია საერთოდ არ მიუღიათ. დასავლეთ ბალკანეთის კანდიდატები სხვა სურათს გვიჩვენებენ: რამდენიმე მათგანმა ბოლო ათწლეულის განმავლობაში, ენერგეტიკული გაერთიანებისა და სტაბილიზაციის პროცესების ფარგლებში,

თავდაპირველი NIS დირექტივის ელემენტები გადმოიტანა, რის გამოც ევროკავშირის კიბერუსაფრთხოების სამართალთან მათი შეხება უფრო ხანგრძლივი, თუმცა არაერთგვაროვანია, ვიდრე აღმოსავლეთ პარტნიორობის ქვეყნების უმეტესობისა. მაგრამ ეს განსხვავებები ამ ქვეყნებიდან არც ერთში კიბერმედეგობის აქტისთვის მზაობას არ ნიშნავს. თითოეული კანდიდატის არსებული ჩარჩო, რაოდენ განვითარებულიც არ უნდა იყოს, ორგანიზაციულ ან კრიტიკული ინფრასტრუქტურის ვალდებულებებზეა აგებული და არა ევროკავშირის უფრო ახალ, დეტალურ მიდგომაზე — პროდუქტის დონეზე შესაბამისობის შეფასებაზე, მხარდაჭერის პერიოდებზე და პროგრამული უზრუნველყოფის CE მარკირებაზე. ეს ცნებები ევროპულ სამართალში მაშინ არ არსებობდა, როცა ეს ეროვნული ჩარჩოები იწერებოდა.

ჯერ შესაძლებლობები, შემდეგ შესაბამისობა

ევროკავშირის ტექნიკური დახმარების ინსტრუმენტები ამ ხარვეზს ირიბად აღიარებენ, და ისინი რეგიონული პრინციპითაა ორგანიზებული და არა ცალკეულ კანდიდატზე მორგებული. **დასავლეთ ბალკანეთის კიბერშესაძლებლობების ცენტრი** ბალკანეთის ექვს კანდიდატს ოპერაციულ თანამშრომლობასა და ერთობლივ წვრთნებში ეხმარება. **აღმოსავლეთ პარტნიორობის კიბერუსაფრთხოების ინიციატივა**, რომელსაც საქართველოში, აზერბაიჯანსა და მოლდოვაში e-Governance Academy ახორციელებს, უკრაინასა და სომხეთში კი GIZ პარალელურად მუშაობს, სამართლებრივი დაახლოების ტრადიციულ საქმიანობასთან ერთად ციფრულ წიგნიერებასა და სამოქალაქო საზოგადოების ჩართულობას — განსაკუთრებით დედაქალაქების გარეთ — შეგნებულად უსვამს ხაზს. ორივე ინსტრუმენტს ერთი და იგივე შეფასება უდევს საფუძვლად: საკანონმდებლო გადმოტანა ინსტიტუციური შესაძლებლობების შესაბამისი ზრდის გარეშე შესაბამისობას ქაღალდზე ქმნის, მაგრამ არა მედეგობას პრაქტიკაში. EUISS-ის მიმოხილვა რეგიონულ დონეზე იმავე დასკვნამდე მიდის: გაფართოების პარტნიორები — როგორც დასავლეთ ბალკანეთში, ისე აღმოსავლეთ სამეზობლოში — „წინა ხაზის აქტორებად“ უნდა განიხილებოდნენ, რომელთა ოპერაციული შესაძლებლობების ევროკავშირის სტრუქტურებში ჩართვა გაწევრიანებამდეც მიზანშეწონილია, და არა *acquis*-ის პასიურ მიმღებებად, რომლებიც მას მოლაპარაკებების დასრულების შემდეგ უბრალოდ გადმოიღებენ.

ასეთ მდგომარეობაში მყოფი ქვეყნისთვის კიბერმედეგობის აქტის მთავარი გაკვეთილი, სავარაუდოდ, მისი კონკრეტული ტექნიკური მოთხოვნები არ არის — ისინი მხოლოდ მაშინ გახდება აქტუალური, როცა გაწევრიანების მოლაპარაკებები შესაბამის თავს მიაღწევს. მთავარი გაკვეთილი მათ უკან მდგარი ინსტიტუციური მოდელია: შესაბამისობის შეფასების მოქმედი სისტემა, სანდო ეროვნული უწყებები, რომლებსაც შემოწმებისა და სანქცირების უფლებამოსილება აქვთ, და მწარმოებლებსა და სახელმწიფოს შორის ანგარიშგების ნამდვილი კულტურა. ამ ინსტიტუციური შესაძლებლობების გაძლიერება ახლა, ნებისმიერ ფორმალურ ვადამდე, გაწევრიანებისთვის მზაობას უფრო მეტს შემატებს, ვიდრე კიბერმედეგობის აქტის ტექსტის ნაადრევად ეროვნულ კანონმდებლობაში გადმოტანის მცდელობა. **საქართველო** ამას მკაფიოდ აჩვენებს: სახელმწიფოს, რომელიც საკუთარი ინსტიტუტების წინააღმდეგ მიმართულ რუსეთთან დაკავშირებულ კიბერაქტივობას მუდმივად აწყდება, ამ შესაძლებლობების განვითარების საფუძველი გაწევრიანების გრაფიკისგან დამოუკიდებლადაც აქვს და არა მხოლოდ იმიტომ, რომ ბრიუსელი ამას ოდესმე მოსთხოვს. იგივე ლოგიკა, სხვა გეოპოლიტიკურ რეგისტრში, ვრცელდება უკრაინის საომარი პირობების ციფრულ ინფრასტრუქტურაზე და დასავლეთ ბალკანეთის სახელმწიფოებზეც, რომლებიც რეგიონის გარედან მომდინარე ჰიბრიდული ზეწოლის მიმართ მოწყვლადები არიან.

დასკვნა. სტრუქტურული ცვლილება, რომელიც დაძაბულ პირობებში დგება

რას ცვლის რეალურად კიბერმედეგობის აქტი

კიბერმედეგობის აქტი იმას აკეთებს, რაც ევროპულ სამართალს ასეთი მასშტაბით აქამდე არ უცდია: ევროკავშირის ბაზარზე გაყიდულ კომერციულ პროდუქტში ძირითადი კიბერუსაფრთხოების არარსებობას სამართლებრივ ხარვეზად აქცევს და არა ბიზნესრისკად, რომლის ფასსაც ბაზარი თავად უნდა დაედგინა. ეს ნამდვილი სტრუქტურული ცვლილებაა, რომელიც ხასიათით — თუმცა კულტურული წონით ჯერ არა — იმ მომენტს შეედრება, როცა პროდუქტების უსაფრთხოების სამართალმა დაუცველი სათამაშოს ან გაუმართავი საყოფაცხოვრებო ტექნიკის გაყიდვა პირველად უკანონო გახადა და არა უბრალოდ არაგონივრული შენაძენი. მწარმოებლები, იმპორტიორები და დისტრიბუტორები ახლა იმ დაშვებით მოქმედებენ, რომელიც ათი წლის წინ უცხო იქნებოდა: კიბერუსაფრთხოება არ არის დამატებითი საფასურით გასაყიდი ფუნქცია, არამედ ბაზარზე კანონიერი დაშვების პირობაა.

რეგულაციის არქიტექტურა თანმიმდევრულია და, ზოგადად, დასაცავიც. რისკზე დაფუძნებული ვალდებულებები იმ ზიანის პროპორციულად იზრდება, რომელიც პროდუქტის მწყობრიდან გამოსვლას შეიძლება მოჰყვეს. ანგარიშგების ვადები მომიჯნავე კანონმდებლობასთანაა შეთანხმებული და არა იზოლირებულად გამოგონილი. ნამდვილად რთულ პოლიტიკურ პრობლემას — როგორ დარეგულირდეს კომერციული პროდუქტები ისე, რომ სრულიად სხვა წანამძღვრებზე აგებული ღია წყაროს ეკოსისტემა არ დაინგრეს — სპეციალურად შემუშავებული კომპრომისით უპასუხეს და არა მეორეხარისხოვანი, დამატებით მიღებული გადაწყვეტით.

თუმცა ეს ყველაფერი გარანტიას არ იძლევა, რომ კიბერმედეგობის აქტი ჩანაფიქრისამებრ იმუშავებს. სავალდებულო ვადები ახლოვდება, სტანდარტები კი დაუსრულებელი რჩება. მცირე მწარმოებლები თავდაჯერებულობის ნაკლებობას სწორედ იმ სფეროებში აღნიშნავენ, რომლებსაც რეგულაცია ფუძემდებლურად მიიჩნევს. ამასთან, რეგულაცია ისეთ პოლიტიკურ გარემოში ამოქმედდა, რომელიც იმ მარეგულირებელ ინსტინქტს, რომელმაც იგი წარმოშვა, გაცილებით სკეპტიკურად უყურებს, ევროკომისიის საკუთარი გამარტივების დღის წესრიგი კი ციფრული კანონმდებლობის მომიჯნავე ნაწილებს უკვე ეხება — სწორედ მაშინ, როცა კიბერმედეგობის აქტის პირველი მკაცრი ვადები დგება. დარჩება თუ არა კიბერმედეგობის აქტი ისტორიაში იმ მომენტად, როცა ევროპულმა კიბერუსაფრთხოების სამართალმა მოწიფულობას მიაღწია, თუ კარგად დაპროექტებულ ნორმად, რომელიც ერთი პოლიტიკური ციკლით დააგვიანდა და რომლის სრულად აღსრულების ნება უკვე აღარ არსებობდა — ეს არა იმდენად ამ ანალიზში განხილულ ტექსტზეა დამოკიდებული, რამდენადაც იმ არჩევანზე, რომელიც ევროპულ ინსტიტუტებს ჯერ არ გაუკეთებიათ: დაფინანსებაზე, სტანდარტებზე და იმაზე, რამდენ მარეგულირებელ ამბიციას გაუძლებს კავშირის დღევანდელი განწყობა.

[1] **Regulation (EU) 2024/2847 (Cyber Resilience Act)** - ევროპარლამენტისა და საბჭოს 2024 წლის 23 ოქტომბრის რეგულაცია (EU) 2024/2847 ციფრული ელემენტების შემცველი პროდუქტებისთვის კიბერუსაფრთხოების ჰორიზონტალური მოთხოვნების შესახებ, OJ L, 2024/2847, 20.11.2024. ხელმისაწვდომია EUR-Lex-ზე.

[2] **European Commission, 'The Cyber Resilience Act — Summary of the legislative text'** -Shaping Europe's Digital Future, digital-strategy.ec.europa.eu, განახლებულია 2025 წლის 3 დეკემბერს.

[3] **Pinsent Masons, 'Cyber Resilience Act marks major shift in EU cybersecurity compliance'** - Out-Law-ის ანალიზი, 2026 წლის 25 აგვისტო — მიმოხილულია ევროკომისიის 2026 წლის 27 ივლისს გამოქვეყნებული სახელმძღვანელო მწარმოებელთა ვალდებულებების, მხარდაჭერის პერიოდებისა და ანგარიშგების ვადების შესახებ.

[4] **ENISA, 'SME CRA Survey Report'** -ევროკავშირის კიბერუსაფრთხოების სააგენტო, 2026 წლის ივნისი — მცირე და საშუალო საწარმოების ინფორმირებულობა და მზაობა კიბერმედეგობის აქტის ვალდებულებების მიმართ.

[5] **Eurochambres, 'Position on the Cybersecurity Package'** - ევროპის სავაჭრო და სამრეწველო პალატების ასოციაცია, 2026 წლის ივნისი.

[6] **OpenForum Europe et al., submission on the 2022 Cyber Resilience Act draft** - OpenForum Europe-ის, Eclipse Foundation-ის, Open Source Initiative-ისა და სხვათა ერთობლივი მიმართვა ევროკომისიისადმი, 2023 წლის იანვარი.

[7] **JIPITEC, 'The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act'** - Journal of Intellectual Property, Information Technology and E-Commerce Law, ტ. 16, №1 (2025).

[8] **Euractiv, 'Brussels' proposed cybersecurity overhaul risks constitutional red flags'** - Euractiv, 2026 წლის 4 მარტი — კიბერუსაფრთხოების აქტის შემოთავაზებული გადასინჯვის („CSA2“) შესახებ.

[9] **European Union Institute for Security Studies, 'Shared threats, shared resilience'** - EUISS-ის ანალიტიკური მიმოხილვა, 2026 წლის 26 მაისი — გაფართოების პარტნიორების ევროკავშირის ციფრულ და კიბერუსაფრთხოების ჩარჩოებში ინტეგრირების შესახებ.

[10] **EU4Digital / e-Governance Academy, Eastern Partnership Cybersecurity Initiative** - e-Governance Academy-ის პროექტის დოკუმენტაცია და EU4Digital, 'Cybersecurity guidelines for the Eastern Partner countries' — საქართველოსა და აღმოსავლეთ პარტნიორობის სხვა ქვეყნებში კიბერუსაფრთხოების კანონმდებლობის მდგომარეობის შესახებ.

გიორგი როზაქიძე

გიორგი როზაქიძე დიპლომატი და საერთაშორისო პოლიტიკის, უსაფრთხოებისა და ევროპული ინტეგრაციის ექსპერტია. საქართველოს სახელმწიფო სამსახურში მრავალწლიანი კარიერის მანძილზე (2004–2023) ის იკავებდა სხვადასხვა მნიშვნელოვან პოზიციას ევროპული და ევროატლანტიკური ინტეგრაციისა და, აგრეთვე, რეგიონული უსაფრთხოების მიმართულებით. დიპლომატიური სამსახურის გარდა, გიორგი როზაქიძე არის არაერთი სამეცნიერო პუბლიკაციის ავტორი, მათ შორის აღმოსავლეთ ევროპაში პოპულისტური და რადიკალური პარტიების კვლევის თემატიკაზე.