LIETUVOS RESPUBLIKOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMO ĮSTATYMO NR. XI-1807 1, 2, 5, 6 IR 43 STRAIPSNIŲ PAKEITIMO IR ĮSTATYMO PAPILDYMO 43^2 IR 43^3 STRAIPSNIAIS ĮSTATYMO PROJEKTO AIŠKINAMASIS RAŠTAS

1. Įstatymo projekto rengimą paskatinusios priežastys, parengto projekto tikslai ir uždaviniai

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 5 6 ir 43 straipsnių pakeitimo ir Įstatymo papildymo 43^2 ir 43^3 straipsniais įstatymo projekto (toliau – Projektas) rengimą paskatino siekis pakelti kibernetinio saugumo būklės lygį Lietuvos Respublikoje. Projektu įgyvendinamos Nacionalinės kibernetinio saugumo strategijos, patvirtintos Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. posėdyje, nuostatos ir Lietuvos Respublikos Vyriausybės 2018 m. gegužės 20 d. pasitarimo protokolo Nr. 27 7 klausimo 2 punkte įtvirtinti pavedimai.

2016 m. NATO viršūnių susitikimo Varšuvoje metu kibernetinė erdvė pripažinta penktuoju kariavimo domenu. Taip dar kartą patvirtinama, kad kibernetinėmis priemonėmis gali būti pažeistas valstybės suverenitetas, panaudojama jėga ar net surengta ginkluota ataka. Kibernetinis saugumas laikytinas esminiu valstybės interesu, nacionalinio saugumo dalimi.

Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) parengtoje 2017 m. nacionalinio kibernetinio saugumo būklės ataskaitoje nurodoma, kad 2017 m. kibernetinio saugumo reikalavimų įgyvendinimo lygis tvarkant valstybės informacinius išteklius ir ypatingos svarbos informacinę infrastruktūrą kilo, tačiau reikalavimai yra įgyvendinami *ad hoc*, ne visa apimtimi ir formaliai, o didėjantis fiksuojamų incidentų kiekis ir atlikti tyrimai rodo, kad organizacijos laiku netaiko būtinų priemonių, kad užkardytų žinomus pažeidžiamumus ir grėsmes. Be to, atsižvelgiant į pasaulio ir Lietuvos kibernetinių grėsmių tendencijas, prognozuojama, kad 2018 m. ir toliau bus ieškoma saugumo spragų tvarkant Lietuvos valstybės informacinius išteklius ir ypatingos svarbos informacines infrastruktūras, toliau didės susidomėjimas technologiniuose procesuose dalyvaujančiais ir turinčiais sąsają su internetu įrenginiais.

Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos, Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Lietuvos Respublikos krašto apsaugos ministerijos surinkti duomenys rodo, kad Lietuva nuolat susiduria su įvairaus tipo kibernetiniais incidentais, skirtais valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai pažeisti, ir prognozuojama, kad ateityje jų skaičius ir mastas nemažės.

2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apdorojo 54 414 kibernetinių incidentų. 2017 m. kibernetinių incidentų užregistruota dešimtadaliu daugiau nei 2016 m. Lietuvos valstybės informaciniai ištekliai tebėra prioritetinis kibernetinio šnipinėjimo taikinys, bet taikomasi ir į privataus sektoriaus ypatingos svarbos informacinę infrastruktūrą, kitas įmones, turinčias strateginę ar svarbią reikšmę nacionaliniam saugumui. NKSC, taikydamas technines kibernetinio saugumo priemones, daugiausiai kenkimo programinės įrangos paplitimo atvejų nustatė energetikos (27 proc.), viešojo saugumo ir teisinės tvarkos (22 proc.) bei užsienio reikalų ir saugumo politikos (21 proc.) sektoriuose. Palyginti su 2016 m., kenkimo programinė įranga labiau plito viešojo saugumo ir teisinės tvarkos, užsienio reikalų ir saugumo politikos, energetikos sektoriuose. Šalies kibernetinio saugumo situacijai įtaką daro ir viešojo sektoriaus interneto svetainių būklė, kuri, 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. pablogėjo.

Atsižvelgiant į tai, kad kibernetinio saugumo plėtra valstybės informaciniuose ištekliuose yra netolygi, o tam tikrais atvejais ir nepakankama, Projektu siekiama pakelti kibernetinio saugumo būklės lygį Lietuvoje.

Siekiant įgyvendinti nurodytą tikslą, siūloma nustatyti pareigą valstybės ir savivaldybių institucijoms ir įstaigoms, dalyvaujančioms vykdant valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti, naudoti saugų valstybinį duomenų perdavimo tinklą (toliau – Saugusis tinklas) ir visų jų valdomų tarnybinių stočių ir (arba) registrų ir valstybės bei kitų informacinių sistemų įrangą ir duomenis laikyti biudžetinės įstaigos patikėjimo teise valdomose patalpose įrengtuose ir biudžetinių įstaigų eksploatuojamuose duomenų centruose (toliau – valstybinis duomenų centras) bei įstatyme įtvirtinti valstybinio duomenų centro sąvoką. Taip pat siūloma numatyti galimybę Saugiuoju tinklu bei valstybiniais duomenų centrais naudotis ir kitoms institucijoms, nedalyvaujančioms vykdant valstybines mobilizacines užduotis. Dėl tokių institucijų poreikio naudotis Saugiuoju tinklu teikiamomis elektroninių ryšių ir valstybinių duomenų centrų paslaugomis būtų sprendžiama gavus kompetentingos institucijos išvadą dėl poreikio užtikrinti nacionalinį saugumą.

2. Įstatymo projekto iniciatoriai (institucija, asmenys ar piliečių įgalioti atstovai) ir rengėjai

Projekto rengimą inicijavo Lietuvos Respublikos krašto apsaugos ministerija. Projektą parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento direktorius Jonas Skardinskas (tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt) ir Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. (8 5) 273 5545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (Įstaigų teisinės priežiūros skyriaus patarėja, atliekanti Teisėkūros skyriaus viršininko funkcijas, Svetlana Lapėnienė, tel. (8 5) 273 5563, el. p. svetlana.lapeniene@kam.lt) vyr. specialistas Mantas Keliotis (tel. (8 5) 273 5597, el. p. mantas.keliotis@kam.lt).

3. Kaip šiuo metu yra reguliuojami įstatymo projekte aptarti teisiniai santykiai

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo (toliau – VIIVĮ) 2 straipsnio 13 dalyje įtvirtinta Saugiojo tinklo sąvoka. Saugusis tinklas skirtas visoms Lietuvos Respublikos valstybės ir savivaldybių institucijoms, įstaigoms ir įmonėms bei kitiems juridiniams asmenims, tačiau nurodytiems subjektams nėra tiesiogiai nustatyta pareiga naudoti tik Saugųjį tinklą.

Lietuvos Respublikos įstatymuose neįtvirtinta nei valstybinio duomenų centro, nei duomenų centro sąvoka, bet Lietuvos Respublikos Vyriausybės 2015 m. gegužės 13 d. nutarime Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“ vartojama duomenų centro sąvoka ir nustatoma pareiga Informacinės visuomenės plėtros komitetui prie Susisiekimo ministerijos laikyti biudžetinės įstaigos patikėjimo teise valdomose patalpose įrengtuose ir biudžetinių įstaigų eksploatuojamuose duomenų centruose informacinių technologijų paslaugoms teikti reikalingą valstybės informacinių išteklių infrastruktūrą. Toks reguliavimas nepakankamas, šiuo nutarimu nenustatoma pareiga visiems valstybės informacinių išteklių valdytojams, nes nesant įstatyme įtvirtinto pagrindo Vyriausybė negali nustatyti pareigų jai nepavaldiems subjektams.

4. Kokios siūlomos naujos teisinio reguliavimo nuostatos ir kokių teigiamų rezultatų laukiama

Dėl Saugiojo tinklo

Projektu siūloma tikslinti VIIVĮ 2 straipsnyje įtvirtintą Saugiojo tinklo sąvoką ir ją supaprastinti nurodant tik esminius Saugiojo tinklo bruožus, t. y. įtvirtinti, kad saugus valstybinis duomenų perdavimo tinklas yra valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis nepriklausomas nuo viešųjų ryšių tinklų elektroninių ryšių tinklas.

Be to, Projektu siūloma papildyti VIIVĮ 43^2 straipsniu, kuriame būtų nustatoma pareiga naudoti Saugųjį tinklą ir įtvirtinamas Saugiojo tinklo naudojimo mechanizmas.

Projektu siūlomo teisinio reguliavimo bendrieji bruožai:

1. *Privalomumas.*

1.1. VIIVĮ 43^2 straipsnio 1 dalimi ribotam ratui juridinių asmenų nustatoma pareiga naudoti Saugųjį tinklą. Tai grindžiama tuo, kad Lietuvos Respublikos Konstitucijoje įtvirtinta valstybės saugumo pareiga, ir valstybė, užtikrindama nurodytą konstitucinę pareigą, turi teisę apsispręsti, kokių institucijų informacinius išteklius laiko svarbiausiais, ir tokiems juridiniams asmenims nustatyti pareigas, kuriomis remiantis būtų stiprinamas valstybės informacinių išteklių kibernetinis saugumas.

1.2. Pagrindiniai kriterijai, kuriais remiantis pasirenkama, kuriems juridiniams asmenims Saugiojo tinklo naudojimas tampa privalomas, yra: 1) valstybės informacinių išteklių, būtinų gyvybiškai svarbioms valstybės funkcijoms atlikti ir mobilizacinėms užduotims vykdyti, valdymas ir tvarkymas; 2) dalyvavimas užtikrinant gyvybiškai svarbių valstybės funkcijų vykdymą. Gyvybiškai svarbios valstybės funkcijos įtvirtintos Lietuvos Respublikos mobilizacijos ir priimančios šalies paramos įstatyme ir nustatytos Gyvybiškai svarbių valstybės funkcijų sąraše, patvirtintame Lietuvos Respublikos Vyriausybės 2012 m. gegužės 29 d. nutarimu Nr. 631 „Dėl Gyvybiškai svarbių valstybės funkcijų sąrašo patvirtinimo“. Valstybės ir savivaldybės institucijos ir įstaigos, tiesiogiai atsakingos už gyvybiškai svarbių valstybės funkcijų vykdymą, įtvirtinamos Lietuvos Respublikos Vyriausybės 2013 m. kovo 27 d. nutarime Nr. 256 „Dėl valstybinių mobilizacinių užduočių valstybės ir savivaldybių institucijoms ir įstaigoms skyrimo“.

1.3. Pastebėtina, kad šiame nutarime nurodomos tik tiesiogiai atsakingos valstybės ir savivaldybės institucijos ir įstaigos, bet jų valdymo sritis apima ir kitas institucijas ir įstaigas, valstybės įmones ir viešąsias įstaigas, kurios taip pat dalyvauja vykdant valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti. Atsižvelgiant į tai, numatoma, kad Vyriausybė arba jos įgaliota institucija tvirtintų Saugiojo tinklo naudotojų sąrašą ir tik šiame sąraše nurodytoms valstybės ir savivaldybės institucijoms ir įstaigoms, valstybės įmonėms ir viešosioms įstaigoms (toliau – Institucijos) būtų nustatoma pareiga privalomai naudoti Saugųjį tinklą. Saugiojo tinklo naudotojų sąrašas būtų tvirtinamas atsižvelgiant į tai, ar dalyvauti vykdant valstybines mobilizacines užduotis iš tiesų reikalingos informacinės sistemos ir ryšys su kitomis institucijomis. Nesant tokio poreikio, nepriklausomai nuo dalyvavimo vykdant valstybines mobilizacines užduotis, valstybės ir savivaldybės institucijos ir įstaigos nebūtų traukiamos į Saugiojo tinklo naudotojų sąrašą, todėl joms nebūtų sukuriama pareiga naudoti Saugųjį tinklą. Siūlomu teisiniu reguliavimu užtikrinama, kad pareiga naudoti Saugųjį tinklą bus nustatoma tik toms institucijoms ir įstaigoms, kurios dalyvauja vykdant gyvybiškai svarbias valstybės funkcijas.

1.4. Atkreiptinas dėmesys, kad, priėmus Projektu siūlomą teisinį reguliavimą, būtų reguliuojamas svarbiausius valstybės informacinius išteklius valdančių institucijų duomenų perdavimas elektroninių ryšių tinklais. Institucijų, kurios nepatenka į siūlomą teisinį reguliavimą, duomenų perdavimo kibernetinio saugumo reikalavimai nustatomi vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu. Atsižvelgiant į tai, Projekte siūloma atsisakyti valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 6 dalies kaip perteklinės.

1.5. Ribotam ratui juridinių asmenų nustačius pareigą naudoti Saugųjį tinklą, sudaromos sąlygos stiprinti kibernetinio saugumo būklę, t. y. Saugųjį tinklą, tinklą naudojantiems juridiniams asmenims būtų teikiamas standartizuotas ir saugus paslaugų paketas, užtikrinamas greitesnis ir efektyvesnis reagavimas į kibernetinius incidentus, taupomi kibernetiniam saugumui skiriami ištekliai, nes būtų centralizuojamas saugos užtikrinimas, užtikrinami minimalūs pasiruošimo mobilizacijai pagrindai kibernetinio saugumo srityje. Be to, nustačius privalomumą naudoti Saugųjį tinklą, būtų sudarytos sąlygos efektyviau taikyti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos taikomas kolektyvinės gynybos priemones, ypač krizinių situacijų metu.

2. *Nepriklausomumas.*

2.1. Specialiuosiuose organizaciniuose ir techniniuose reikalavimuose, kuriuos tvirtintų saugiojo tinklo valdytojas, būtų nustatoma tik viena prieiga prie viešųjų elektroninių ryšių tinklų, kurią valdytų tik Saugųjį tinklą tvarkanti biudžetinė įstaiga (toliau – Saugiojo tinklo tvarkytojas). Tai reiškia, kad prie viešųjų elektroninių ryšių tinklų institucijos jungtųsi tik per Saugiojo tinklo tvarkytojo valdomus „vartus“, o institucijų valdomus valstybės informacinius išteklius kiti subjektai

turėtų galimybę pasiekti taip pat tik per Saugiojo tinklo tvarkytojo valdomus „vartus“. Esant poreikiui ar kritinei situacijai „vartai“ galėtų būti „uždaromi“ ir išorės subjektai svarbiausių valstybės informacinių išteklių neturėtų galimybės pasiekti. Be to, net ir uždarius „vartus“ į viešuosius elektroninius ryšius, nustatytos spartos duomenų perdavimas tarp Saugiojo tinklo naudotojų ir jų padalinių būtų išlaikomas, todėl ryšys tarp Saugiojo tinklo naudotojų išliktų.

2.2. Atsižvelgiant į tai, VIIVĮ pildant 43^2 straipsnio 1 dalimi, nustatoma esminė sąlyga, nurodanti, kad Saugiojo tinklo naudotojai gauti elektroninių ryšių paslaugas ir jungtis prie viešųjų elektroninių ryšių tinklų gali tik per Saugųjį tinklą. Neįgyvendinus šios sąlygos, saugumas Saugiuoju tinklu negalės būti užtikrinamas, nes kibernetinio saugumo grėsmės paprasčiausiai turėtų galimybę pasiekti valstybės informacinius išteklius keliu, kuris nebūtų kontroliuojamas Saugiuoju tinklu.

3. *Neatlygintinumas.*

3.1. VIIVĮ 43^2 straipsnio 3–5 dalyse nustatomas hibridinis atsiskaitymo už Saugiuoju tinklu teikiamas paslaugas modelis. Atsižvelgiant į tai, kad saugiojo tinklo ir valstybinių duomenų centrų paslaugų teikimas laikomas valstybės funkcija, atliekama biudžetinės įstaigos, standartinės Saugiojo tinklo ir valstybinių duomenų centrų paslaugos Saugiojo tinklo naudotojams bus teikiamos neatlygintinai, o atlyginimas už Saugiuoju tinklu teikiamas papildomas paslaugas neviršys sąnaudų, patiriamų teikiant šias paslaugas. Taigi nebūtų siekiama komercinio tikslo.

3.2. Standartines paslaugas apimtų: 1) duomenų perdavimas Saugiuoju tinklu institucijoms ar įstaigoms ir jų padaliniams nustatyta sparta; 2) nustatytos spartos prieiga prie viešųjų ryšių tinklų; 3) kolektyvinė apsauga kibernetinio saugumo priemonėmis; 4) sąveika su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais; 5) sujungimas tarp valstybės valdomų tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, segmentų.

3.3. Pastebėtina, kad visos standartinės paslaugos būtų teikiamos visiems Saugiojo tinklo naudotojams. Kitaip tariant, standartines paslaugas iš esmės reikėtų suprasti kaip vieną kompleksišką Saugiojo tinklo paslaugą, nes kiekvienos ar kelių standartinių paslaugų teikimas ne visa apimtimi neatitiktų Saugiojo tinklo koncepcijos ir nebūtų pasiekti kibernetinio saugumo užtikrinimo tikslai.

3.4. Papildomos paslaugos būtų nustatomos atsižvelgiant į galimus išskirtinius Saugiojo tinklo naudotojų poreikius, kurių nebūtų galima patenkinti standartinėmis paslaugomis. Papildomos paslaugos savo esme nesiskirtų nuo standartinių paslaugų, tiesiog galimai skirtųsi tam tikro parametro kiekybinis ar kokybinis kriterijus. Pavyzdžiui, paslaugų gavėjo netenkina nustatyta duomenų perdavimo sparta, nes siekiant naujai užsibrėžtų tikslų išauga didesnės nei nustatyta duomenų perdavimo spartos poreikis, todėl paslaugų gavėjas gali visiškai pagrįstai reikalauti didinti duomenų perdavimo spartą. Siekiant užtikrinti, kad prašymas padidinti duomenų perdavimo spartą būtų racionalus ir pagrįstas, Saugiojo tinklo tvarkytojas duomenų perdavimo didesne sparta paslaugą teiktų kaip papildomą, kurią paslaugų gavėjas turėtų Saugiojo tinklo tvarkytojui kompensuoti. Tokiu teisiniu reguliavimu siekiama, kad Saugiojo tinklo tvarkytojui nebūtų nepagrįstai perkeliama didesnės spartos (ar kitos papildomos paslaugos) racionalaus poreikio įvertinimo pareiga.

3.6. Pažymėtina, kad papildomų paslaugų teikimo sąnaudas Saugiojo tinklo tvarkytojo lėšomis tikrintų auditorius ar audito įmonė.

3.7. Tiek standartinės, tiek papildomos Saugiojo tinklo paslaugos būtų nustatomos Saugiuoju tinklu teikiamų paslaugų sąraše, patvirtintame Vyriausybės ar jos įgaliotos institucijos.

4. *Valstybės funkcijos vykdymas.*

4.1. Siūlomu teisiniu reguliavimu siekiama užtikrinti esminį valstybės interesą – svarbiausių valstybės informacinių išteklių kibernetinį saugumą, todėl kibernetinio saugumo užtikrinimas laikytinas, visų pirma, valstybės funkcija. Valstybės funkcijos vykdymą siūloma pavesti biudžetinei įstaigai.

4.2. Nors tam tikrų funkcijų vykdymą valstybė gali perduoti vykdyti privatiems subjektams, kiekvienu atveju tai yra valstybės apsisprendimo reikalas. Funkcijų, susijusių su nacionalinio saugumo užtikrinimu, vykdymas paprastai neperduodamas privatiems subjektams, nes

būtina užtikrinti, kad valstybės funkcija būtų nuolatos vykdoma (net ir *force majeure* aplinkybėmis), o funkciją pavedus atlikti privačiam subjektui, valstybės gynybiniai interesai būtų priklausomi nuo rinkos sąlygų, sutartinių įsipareigojimų ir privataus subjekto interesų.

4.3. Kibernetinėje erdvėje išskirtinas ir kitas aspektas: nors sėkmingai gintis nuo kibernetinių atakų galima nepriklausomai nuo to, valstybinis ar privatus subjektas tai daro, valstybės funkcijų vykdymas sukuria tam tikras pasekmes. Saugiojo tinklo paslaugų teikimas yra susijęs su ypatinga reikšme valstybės saugumui pasižyminčios informacijos valdymu, dėl kurios ši informacija negali būti saugiai patikėta privatiems subjektams, ypač atsižvelgiant į augantį kibernetinių grėsmių mastą. Saugiajam tinklui dėl jo specifiškumo ir dėl galimos didelės žalos nacionaliniam saugumui įstatymų pagrindu yra suteiktas ypatingos reikšmės statusas.

4.4. Tinklo topologija, naudojamos techninės ir organizacinės priemonės yra įslaptintos pagal Lietuvos Respublikos valstybės tarnybos paslapčių įstatymą, todėl visos šiame tinkle naudojamos ir ketinamos naudoti žvalgybinio pobūdžio specifinės kibernetinės priemonės negali būti atskleistos jokiems privatiems ūkio subjektams ar kitoms teisės su įslaptinta informacija dirbti neturinčioms institucijoms. NATO ir ES lygmeniu valstybių narių žvalgybos institucijos, pasitelkdamos specialiąsias priemones, keičiasi įslaptinta informacija, taip pat ir apie šalių sąjungininkių valdomuose tinkluose esančias spragas bei tinklo kibernetinį pažeidžiamumą. Saugiojo tinklo perduodama ypatingos svarbos informacija yra užšifruojama ir iššifruojama, atitinkamos ir techninės saugojimo priemonės, kurių nebūtų galima atskleisti privatiems paslaugų tiekėjams. Saugiojo tinklo tvarkytojo darbuotojai privalo turėti leidimus dirbti su valstybės paslaptį sudarančia informacija, kurie, remiantis Valstybės ir tarnybos paslapčių įstatymu, suteikiami tik atitinkamoms tarnyboms atlikus patikrinimus. Privataus operatoriaus atveju kiltų rizika, jog dalis Saugųjį tinklą aptarnaujančių darbuotojų reikiamų leidimų neturės arba dėl tam tikrų priežasčių jų negaus. Dėl šių ir kitų su nacionalinio saugumo reikalavimais susijusių aplinkybių Saugiajam tinklui priskiriamų funkcijų negalėtų įgyvendinti bet koks ūkio subjektas ar kita tam įgaliojimų ar reikiamų kompetencijų neturinti įstaiga ar institucija.

4.5. Reaguojant į tarptautinio pobūdžio kibernetines atakas, nepaisant subjekto priklausomumo, veiksmai, atliekami vykdant valstybės funkcijas, laikomi valstybės veiksmais. Taip privatus subjektas gali sukurti situaciją, kai besigindamas nuo kibernetinių atakų atlieka veiksmus, kurie tarptautinės teisės požiūriu būtų laikomi net ginkluota ataka prieš kitą valstybę[1].

4.6. Planuojama, kad valstybės funkcijos vykdymas biudžetinei įstaigai būtų perduodamas reorganizuojant krašto apsaugos ministro valdymo sričiai priskirtą valstybės įmonę „Infostruktūra“, kuri šiuo metu yra įgaliota Saugiojo tinklo tvarkytoja ir atitinka kitus reikalavimus Saugiajam tinklui tvarkyti, į biudžetinę įstaigą.

Dėl valstybinių duomenų centrų

Projektu siūloma VIIVĮ 2 straipsnyje įtvirtinti dvi naujas sąvokas: duomenų centro ir valstybinio duomenų centro. Duomenų centras būtų suprantamas kaip patalpos, skirtos serverių ir (arba) registrų ir valstybės bei kitų informacinių sistemų įrangai ar duomenims laikyti, o valstybinis duomenų centras, kaip biudžetinės įstaigos patikėjimo teise valdomose patalpose įrengtas ir jos eksploatuojamas duomenų centras, įrašytas į Vyriausybės ar jos įgaliotos institucijos tvirtinamą valstybinių duomenų centrų sąrašą.

Be to, VIIVĮ 43^3 1 straipsnyje siūloma numatyti pareigą Institucijoms, kurios valdo ir tvarko valstybės informacinius išteklius, būtinus gyvybiškai svarbioms valstybės funkcijoms atlikti ir mobilizacinėms užduotims vykdyti, atlikdamos gyvybiškai svarbias valstybės funkcijas,

---

[1] Pvz., valstybės A institucijai Saugiojo tinklo paslaugas teikia privatus subjektas B. Valstybės C subjektas atlieka provokacinę kibernetinę ataką prieš valstybės A institucijos informacinę sistemą. Subjektas B nustato kibernetinės atakos šaltinį (pvz., IP adresą), tačiau neidentifikuoja nei šaltinio valstybės, nei konkretaus šaltinio subjekto. Gindamasis nuo kibernetinės atakos, subjektas B atlieka puolamuosius veiksmus kibernetinės atakos šaltinio atžvilgiu (savigynos situacija), kartu sukeldamas padarinius valstybės C subjektui. Padarinių sukėlimas būtų priskiriamas ir valstybei A (nes subjektas B vykdė valstybės A funkciją), priklausomai nuo subjekto B sukeltų padarinių, tokie veiksmai potencialiai galėtų apimti ir ginkluotą ataką, kurios autoriumi būtų pripažįstama valstybė A.

dalyvauja vykdant valstybines mobilizacines užduotis, įrašytoms į valstybinių duomenų centrų naudotojų sąrašą, visų jų valdomų serverių ir (arba) registrų ir valstybės bei kitų informacinių sistemų įrangą ir duomenis laikyti valstybiniuose duomenų centruose. Taip būtų sukurtos sąlygos taikyti kolektyvines kibernetinio saugumo priemones, užtikrinant aukštesnį kibernetinio saugumo lygį, mažinti valstybei svarbių valstybės informacinių sistemų ir registrų valdytojų pažeidžiamumą, koordinuotai valdyti nacionaliniam saugumui užtikrinti svarbią infrastruktūrą.

Projektu siūlomo teisinio reguliavimo bendrieji bruožai daugeliu atveju atitinka Saugiojo tinklo atžvilgiu nustatomus privalomumo, neatlygintinumo ir valstybės funkcijos vykdymo bruožus. Pagrindiniai skirtumai:

1. *Privalomumas.*

1.1. Privalomumas nustatomas vadovaujantis iš esmės tais pačiais kriterijais kaip ir Saugiojo tinklo atžvilgiu, todėl atskiro valstybinių duomenų centrų naudotojų sąrašo nereikėtų tvirtinti, būtų taikomas tas pats Saugiojo tinklo sąrašas.

1.2. Atkreiptinas dėmesys, kad Projektu siūlomu reguliavimu nėra nustatomas konkretus valstybinių duomenų centrų skaičius. Projektu nustatomas lankstus valstybės informacinių išteklių valdymo konsolidavimo koncepcijos įgyvendinimo modelis. Siūlomu teisiniu reguliavimu būtų galima steigti neribotą kiekį valstybės duomenų centrų, tačiau, atsižvelgiant į poreikius ir galimybes, valstybinių duomenų centrų kiekį būtų galima keisti. Tokiu būdu būtų sudaromos sąlygos valstybės informacinių išteklių valdymo konsolidavimo koncepciją dėl vieno valstybinio duomenų centro steigimo įgyvendinti palaipsniui mažinant valstybinių duomenų centrų kiekį.

2. *Neatlygintinumas.*

Nenustatomas hibridinis atsiskaitymo modelis, nesukuriama pareiga tvirtinti paslaugų sąrašo, nes iš esmės įtvirtinama pareiga teikti tik vieną paslaugą – duomenų centro paslaugą (angl. *Data centre as a service*). Valstybinių duomenų centrų naudotojams valstybinių duomenų centrų paslaugos būtų teikiamos neatlygintinai, o biudžetinės įstaigos, eksploatuojančios valstybinius duomenų centrus, išlaidos, patirtos dėl neatlygintinai teikiamų valstybinių duomenų centrų paslaugų ir valstybiniuose duomenų centruose laikomos įrangos eksploatavimo, finansuojamos iš biudžetinei įstaigai, eksploatuojančiai valstybinius duomenų centrus, skiriamų valstybės biudžeto lėšų ir (arba) kitų teisės aktuose nustatytų finansavimo šaltinių. Pastebėtina, kad, atsižvelgiant į siūlomą teisinį reguliavimą, biudžeto lėšos, Institucijoms skiriamos eksploatuoti jų valdomai serverių ir (arba) registrų ir valstybės bei kitų informacinių sistemų įrangai, turėtų būti paskirtos atitinkamą valstybinį duomenų centrą eksploatuojančiai institucijai.

3. *Valstybės funkcijos vykdymas.*

Priežastys, dėl kurių valstybės duomenų centrų paslaugos turėtų būti teikiamos biudžetinės įstaigos, yra iš esmės tos pačios kaip ir priežastys, dėl kurių Saugiojo tinklo paslaugas turėtų teikti biudžetinė įstaiga.

5. Numatomo teisinio reguliavimo poveikio vertinimo rezultatai (jeigu rengiant įstatymo projektą toks vertinimas turi būti atliktas ir jo rezultatai nepateikiami atskiru dokumentu), galimos neigiamos priimto įstatymo pasekmės ir kokių priemonių reikėtų imtis, kad tokių pasekmių būtų išvengta

Be jau minėtų priežasčių, pagrindžiančių poreikį naudoti Saugųjį tinklą, Saugųjį tinklą naudojantiems juridiniams asmenims būtų teikiamas saugus paslaugų paketas, užtikrinamas greitesnis ir efektyvesnis reagavimas į kibernetinius incidentus, taupomi kibernetiniam saugumui skiriami ištekliai, nes būtų centralizuojamas kibernetinės saugos užtikrinimas, būtų sudarytos sąlygos efektyviau taikyti kolektyvinės gynybos priemones.

Nustačius pareigą naudoti valstybinius duomenų centrus sukuriamos sąlygos taikyti kolektyvines kibernetinio saugumo priemones, taip užtikrinant aukštesnį kibernetinio saugumo lygį, mažinti valstybei svarbių valstybės informacinių sistemų ir registrų valdytojų pažeidžiamumą, koordinuotai valdyti nacionaliniam saugumui užtikrinti svarbią infrastruktūrą.

Vertinant siūlomą teisinį reguliavimą, akivaizdu, kad jis neatitinka ūkinės veiklos sąvokos, kaip ji suprantama Europos Sąjungos ir nacionalinėje teisėje, todėl siūlomas teisinis reguliavimas

nevertintinas kaip galintis riboti privačių ūkio subjektų ūkinę veiklą. Naudojant Saugųjį tinklą ir valstybinius duomenų centrus neperkamos prekės ir paslaugos rinkoje, teikiant Saugųjį tinklą ir valstybinių duomenų centrų paslaugas neatlygintinai nesiekiama komercinių tikslų, naudojimas yra privalomas valstybės ir savivaldybės institucijoms ir įstaigoms, vykdančioms apibrėžtas funkcijas. Svarbiausia siūlomu teisiniu reguliavimu įgyvendinama valstybės funkcija – užtikrinamas svarbiausių valstybės informacinių išteklių kibernetinis saugumas. Savo praktikoje Europos Sąjungos Teisingumo Teismas nuosekliai laikosi pozicijos, jog valstybės institucijos, atlikdamos viešosios valdžios funkcijas, neužsiima ūkine veikla.[2] Pažymėtina, kad Europos Komisija jau yra pasisakiusi dėl panašių santykių, teigdama, kad ryšio paslaugų teikimas tik valdžios institucijoms yra neūkinė veikla ir viešasis vadinamųjų uždarųjų tinklų finansavimas nėra valstybės pagalba.[3] Atsižvelgiant į tai, konkurencijos teisės normos negali būti taikomos.

Atkreiptinas dėmesys į tai, kad, vadovaujantis Europos Sąjungos Teisingumo Teismo praktika, ūkine veikla gali būti laikoma tik tokia veikla, kurią sudaro prekių arba paslaugų siūlymas rinkoje. Veikla nelaikoma ūkine, jeigu ji nevykdoma rinkoje. Veikla vykdoma rinkoje tuo atveju, jeigu subjektas susiduria su kitų subjektų konkurencija ir gauna atlygį už parduotas prekes ar suteiktas paslaugas. Projektu siūlomas teisinis reguliavimas yra apribotas vien valstybės kontroliuojamų paslaugų gavėjų vidinių poreikių – prieigos prie neviešo elektroninių ryšių tinklo – tenkinimu. Projektu siūlomu teisiniu reguliavimu paslaugos nebūtų teikiamos „į išorę“, arba, kitaip tariant, paslaugos nebūtų teikiamos rinkoje.

Šis aspektas iliustruotinas pavyzdžiu: šiais metais Vyriausybės nutarimu buvo įsteigtas ir veiklą pradėjo Nacionalinis bendrųjų funkcijų centras. Centre buvo sutelktos Vyriausybės, ministerijų ir kitų valstybės įstaigų buhalterinės apskaitos bei centralizuoto personalo administravimo funkcijos. Tiek buhalterinės apskaitos, tiek personalo administravimo paslaugų teikimas įprastai galėtų būti apibūdinamas kaip ūkinė veikla. Tačiau būtų nepagrįsta teigti, jog Nacionalinio bendrųjų funkcijų centro sukūrimas ir pavedimas be konkurso jam teikti minėtas paslaugas būtų galėjęs pažeisti Lietuvos Respublikos konkurencijos įstatymo 4 str., kadangi, kaip minėta, centro tikslas yra tenkinti būtent vidinius valstybės poreikius. Vien tai, kad kai kurios funkcijos efektyvumo sumetimais yra iškeliamos į atskirai veikiančias struktūras (neefektyvu kiekvienai atskirai valstybės institucijai atskirai kurti savo nuosavą saugų tinklą), neturi sudaryti prielaidų to traktuoti pagal Konkurencijos įstatymo 4 str., nes valstybės atliekamų funkcijų turinys dėl to nesikeičia.

Net jeigu būtų pripažįstama, kad Projektu sukuriamu teisiniu reguliavimu yra ribojama ūkinė veikla, atkreiptinas dėmesys, kad toks ribojimas pats savaime nėra draudžiamas. Lietuvos Respublikos Konstitucinis Teismas išaiškino, kad, imantis ūkinės veiklos ribojimų ir draudimų nustatymo, turi būti laikomasi tam tikrų sąlygų: 1) ūkinės veiklos laisvė ribojama įstatymu; 2) ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises ir laisves bei Lietuvos Respublikos Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; 3) ribojimais nėra paneigiama teisių ir laisvių prigimtis bei esmė; 4) yra laikomasi konstitucinio proporcingumo principo[4]. Projektu siūlomu teisiniu reguliavimu: 1) ūkinės veiklos ribojimas būtų atliekamas įstatymo lygmens teisės aktu nustatant pareigą įstatyme numatytus kriterijus atitinkantiems subjektams; 2) ribojimu būtų užtikrinamas nacionaliniam saugumui svarbios infrastruktūros saugumas, sukuriamos sąlygos taikyti kolektyvines kibernetinio saugumo priemones, užtikrinamas aukštesnis kibernetinio saugumo lygis, mažinamas valstybei svarbių valstybės informacinių sistemų ir registrų valdytojų pažeidžiamumas; 3) ribojimais nebūtų

---

[2] Žr. 1987 m. birželio 16 d. Europos Sąjungos Teisingumo Teismo sprendimo *Komisija prieš Italiją*, 118/85, ECLI:EU:C:1987:283, 7 ir 8 punktus.

[3] Komisijos pranešimo dėl Sutarties dėl Europos Sąjungos veikimo 107 straipsnio 1 dalyje vartojamos sąvokos (2016/C262/01) 216 punktas; Europos Komisijos gairės dėl valstybės pagalbos sampratos: analitinis tinklelis dėl plačiajuosčio tinklo infrastruktūros, 5 pastraipa.
Prieiga per internetą – http://ec.europa.eu/competition/state_aid/modernisation/grid_broadband_en.pdf.
Taip pat žr. Europos Komisijos 2007 m. gegužės 30 d. sprendimą byloje Nr. 46/2007 (OL C 157 [2007], 2 p.).

[4] Lietuvos Respublikos Konstitucinio Teismo 2006 m. gegužės 31 d. nutarimo byloje Nr. 42/03 „Dėl kvotinio baltojo cukraus eksporto“ II konstatuojamosios dalies 2.2 punktas. http://www.lrkt.lt/dokumentai/2006/n060531.html

paneigiama teisių ir laisvių prigimtis bei esmė; 4) ūkinės veiklos ribojimas būtų nustatomas uždraudžiant dalyvavimą rinkoje tik tų subjektų, kurie dalyvauja užtikrinant gyvybiškai svarbių valstybės funkcijų vykdymą.

6. Kokią įtaką priimtas įstatymas turės kriminogeninei situacijai, korupcijai

Pagal Projektą priimtas įstatymas įtakos kriminogeninei situacijai ir korupcijai neturės.

7. Kaip įstatymo įgyvendinimas atsilieps verslo sąlygoms ir jo plėtrai

Siūlomu teisiniu reguliavimu dėl Saugiojo tinklo neribojama ar nenaikinama galimybė juridiniams asmenims teikti viešųjų elektroninių ryšių tinklų paslaugas, taip pat teikti susijusias paslaugas, prekes ar darbus Saugiojo tinklo tvarkytojui. Ūkio subjektai turės teisę teikti viešųjų elektroninių ryšių tinklų paslaugą Saugiojo tinklo tvarkytojui, dalyvauti viešųjų pirkimų konkursuose ir konkuruoti tarpusavyje teisėtomis priemonėmis.

Dėl siūlomo teisinio reguliavimo, susijusio su valstybinių duomenų centrų paslaugų teikimu, kiti ūkio subjektai neteks galimybės teikti duomenų centrų paslaugų valstybinių duomenų centrų naudotojams. Kaip pagrįsta aukščiau, toks ribojimas nustatytinas siekiant užtikrinti nacionalinio saugumo reikalavimus, todėl toks ribojimas yra proporcingas, be to, neribojantis privačių ūkio subjektų galimybių teikti valstybinio duomenų centro valdytojui su valstybinių duomenų centrų įrengimu, aptarnavimu susijusias paslaugas, prekes ir darbus teisės aktų nustatyta apimtimi. Atsižvelgiant į tai ir į tai, kad valstybinių duomenų centrų naudotojai sudaro nedidelę visų duomenų centrų rinkos dalį, numatoma, kad toks teisinis reguliavimas rinkos sąlygoms didelės įtakos neturės.

8. Įstatymo inkorporavimas į teisinę sistemą, kokius teisės aktus būtina priimti, kokius galiojančius teisės aktus reikia pakeisti ar pripažinti netekusiais galios

Nėra.

9. Ar įstatymo projektas parengtas laikantis Lietuvos Respublikos valstybinės kalbos, Lietuvos Respublikos teisėkūros pagrindų įstatymų reikalavimų, o įstatymo projekto sąvokos ir jas įvardijantys terminai įvertinti Lietuvos Respublikos terminų banko įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka

Projektas parengtas laikantis Lietuvos Respublikos valstybinės kalbos, Lietuvos Respublikos teisėkūros pagrindų įstatymų, kitų Lietuvos Respublikos įstatymų ir teisės norminių aktų rengimo tvarkos reikalavimų ir atitinka bendrinės lietuvių kalbos normas. Projekto terminai vertinami Lietuvos Respublikos terminų banko įstatymo nustatyta tvarka.

10. Ar įstatymo projektas atitinka Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos dokumentus

Projektas atitinka Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos teisės aktus.

11. Jeigu įstatymui įgyvendinti reikia įgyvendinamųjų teisės aktų, – kas ir kada juos turėtų priimti

Krašto apsaugos ministerija parengs ir teiks Lietuvos Respublikos Vyriausybei tvirtinti Lietuvos Respublikos Vyriausybės nutarimo dėl atlyginimo už naudojimąsi Saugiuoju tinklu teikiamomis papildomomis paslaugomis dydžių kriterijų ir atlyginimo nustatymo tvarkos tvirtinimo projektą.

Vyriausybės įgaliota institucija parengs ir patvirtins (arba teiks Lietuvos Respublikos Vyriausybei tvirtinti):

1) Saugiojo tinklo naudotojų sąrašo tvirtinimo projektą;
2) Saugiuoju tinklu teikiamų paslaugų sąrašo tvirtinimo projektą;
3) Paslaugų teikimo Saugiuoju tinklu taisyklių tvirtinimo projektą;

4) valstybės ir savivaldybių institucijų ir įstaigų prisijungimo prie Saugiojo tinklo ir atsijungimo nuo jo sąlygų, planų ir terminų tvirtinimo projektą;

5) valstybinių duomenų centrų naudotojų sąrašo tvirtinimo projektą;

6) valstybinių duomenų centrų sąrašo tvirtinimo projektą;

7) techninių reikalavimų, taikomų valstybiniams duomenų centrams, tvirtinimo projektą;

8) naudojimosi valstybinių duomenų centrų paslaugomis tvarkos tvirtinimo projektą;

9) valstybės ir savivaldybių institucijų ir įstaigų valdomų serverių ir (arba) registrų ir valstybės bei kitų informacinių sistemų įrangos ir duomenų perkėlimo į valstybinius duomenų centrus sąlygų, planų ir terminų tvirtinimo projektą.

Krašto apsaugos ministerija parengs ir patvirtins:

1) krašto apsaugos ministro įsakymą dėl specialiųjų organizacinių ir techninių reikalavimų, taikomų Saugiajam tinklui, tvirtinimo;

2) krašto apsaugos ministro įsakymą dėl Saugiojo tinklo nuostatų tvirtinimo;

3) krašto apsaugos ministro įsakymą dėl atlyginimo už naudojimąsi Saugiuoju tinklu dydžių tvirtinimo;

4) teisės aktų, susijusių su Saugiuoju tinklu ir Saugiojo tinklo tvarkytoju, krašto apsaugos ministro įsakymus.

12. Kiek valstybės, savivaldybių biudžetų ir kitų valstybės įsteigtų fondų lėšų prireiks įstatymui įgyvendinti, ar bus galima sutaupyti (pateikiami prognozuojami rodikliai einamaisiais ir artimiausiais 3 biudžetiniais metais)

Saugusis tinklas bus kuriamas remiantis Saugiu valstybiniu duomenų perdavimo tinklu (toliau – SVDPT), kuris jau dabar jungia 1 300 valstybės institucijų ir įstaigų, mokančių už SVDPT paslaugas. SVDPT tvarkytoją valstybės įmonę „Infostruktūra“ įsigaliojus įstatymo pakeitimams planuojama pertvarkyti į biudžetinę įstaigą. Šios įstaigos teikiamos paslaugos būtų finansuojamos iš Saugiajame tinkle esančių institucijų šiuo metu SVDPT ryšiams skirtų lėšų, perkėlus jas į būsimą biudžetinės įstaigos, administruojančios Saugųjį tinklą, biudžetą.

Pažymėtina, kad steigiant ir eksploatuojant Saugųjį tinklą būtų tikslinga pasinaudoti ir kitų institucijų, pavyzdžiui VĮ „Registrų centro“, turima infrastruktūra. Tokiu būdu būtų racionaliai panaudojama jau esama infrastruktūra, užtikrinant tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą, ir esami ištekliai.

Valstybės duomenų centro Vilniuje, Gedimino pr. 11, investicijų projekto, skirto valstybės duomenų centro patalpoms įrengti, vykdymui lėšos jau skirtos ir šis centras planuojamas įrengti 2019 m. pradžioje. Taip pat numatyta skirti patalpas valstybės duomenų centrui Kaune, jam įrengti iki 2020 m. vidurio planuojama panaudoti Europos Sąjungos lėšas.

13. Įstatymo projekto rengimo metu gauti specialistų vertinimai ir išvados

Projektų rengimo metu specialistų vertinimų ir išvadų negauta.

14. Reikšminiai žodžiai, kurių reikia šiam projektui įtraukti į kompiuterinę paieškos sistemą, įskaitant Europos žodyno „Eurovoc“ terminus, temas bei sritis

Reikšminiai žodžiai, kurių reikia Projektui įtraukti į kompiuterinę paieškos sistemą, – „valstybės informacinių išteklių politika“.

15. Kiti, iniciatorių nuomone, reikalingi pagrindimai ir paaiškinimai

Galimos situacijos, kai, įgyvendinus pareigą naudoti valstybinius duomenų centrus, pareigą įgyvendinusių subjektų šiuo metu eksploatuojami duomenų centrai liktų nenaudojami. Pastebėtina, kad Projektu nesiekiama reguliuoti santykių, išeinančių už Saugiojo tinklo ir valstybinių duomenų centrų reguliavimo ribų, todėl nenaudojamus duomenų centus, kaip ir bet kurį kitą nenaudojamą turtą, nurodyti subjektai turėtų valdyti galiojančių teisės aktų nustatyta tvarka.

Raimundas Karoblis
Krašto apsaugos ministras