LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS KANCELIARIJA
Teisės akto projektas
2022-12-23 Nr. TAP-22-2145(2)
TAIS Nr. 22-12225(3)

Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS
DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 8 STRAIPSNIO PAKEITIMO ĮSTATYMO PROJEKTO NR. XIVP-1855

Nr.
Vilnius

Vadovaudamasi Lietuvos Respublikos Seimo statuto 138 straipsnio 3 dalimi ir atsižvelgdama į Lietuvos Respublikos Seimo valdybos 2022 m. liepos 5 d. sprendimo Nr. SV-S-599 „Dėl įstatymų projektų išvadų“ 11 punktą, Lietuvos Respublikos Vyriausybė n u t a r i a:

Iš esmės pritarti Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 8 straipsnio pakeitimo įstatymo projekto Nr. XIVP-1855 (toliau – Projektas) pagrindiniam tikslui užkirsti kelią kibernetiniams incidentams ir sumažinti jų daroma poveikį, tačiau pasiūlyti Projektą tobulinti:

1. Projektu siūlant keisti Lietuvos Respublikos kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 11 punktą, numatomi nauji Nacionalinio kibernetinio saugumo centro įgaliojimai: nustačius, kad viešųjų elektroninių ryšių tinklų, viešųjų elektroninių ryšių, elektroninės informacijos prieglobos ir (arba) skaitmeninių paslaugų gavėjas galimai dalyvauja ar jo naudojama ryšių ir informacinių technologijų įranga galimai yra naudojama kibernetiniams incidentams vykdyti ir (arba) kibernetiniam sukčiavimui, duoti nurodymą viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos ir (arba) skaitmeninių paslaugų teikėjui apriboti šių paslaugų teikimą minėtam paslaugų gavėjui ir (arba) nurodyti taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis. Atsižvelgiant į Projekto aiškinamajame rašte pateiktus argumentus, šie įgaliojimai grindžiami poreikiu stabdyti nusikalstamas sukčiavimo veikas, atliekamas kibernetinėje erdvėje.

Atkreiptinas dėmesys, kad Kibernetinio saugumo įstatyme tokio pobūdžio įgaliojimai nėra nauji – 10 straipsnio 3 punkte iš esmės tokie patys įgaliojimai yra numatyti Lietuvos policijai. Vadovaujantis Lietuvos Respublikos policijos įstatymo 5 straipsniu, policijos uždaviniai, be kita ko, yra ir nusikalstamų veikų atskleidimas, tyrimas ir prevencija, todėl tokio pobūdžio įgaliojimai Kibernetinio saugumo įstatyme atitinka policijos veiklos kryptis, nes policijai yra sudaromos sąlygos užsiimti sukčiavimo kibernetinėje erdvėje prevencija. Kartu toks teisinis reguliavimas atskleidžia ir funkcijų tarp Nacionalinio kibernetinio saugumo centro ir policijos atskirtį: galiojančio Kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 11 punkte numatomi Nacionalinio kibernetinio saugumo centro įgaliojimai duoti nurodymą viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų

teikėjui stabdyti šių paslaugų teikimą tik pačiais pavojingiausiais atvejais – kai kibernetinis incidentas daro poveikį valstybės informacinių išteklių ar ypatingos svarbos informacinių infrastruktūrų kibernetiniam saugumui, tuo tarpu policijos įgaliojimai stabdyti šias paslaugas įprastais nusikalstamų veikų atvejais nustatomi Kibernetinio saugumo įstatymo 10 straipsnio 3 punkte. Pažymėtina, kad policija siekia ne tik užkardyti nusikalstamas veikas, bet ir jas ištirti, todėl funkcijų atskyrimu užtikrinama, kad Nacionalinis kibernetinio saugumo centras veikdamas savarankiškai nepakenktų tyrimo sėkmei, pavyzdžiui, duodamas nurodymą apriboti šių paslaugų teikimą subjektui, dėl kurio veiksmų policija realiu laiku renka nusikalstamą veiką įrodančius duomenis, kartu sudaromos sąlygos taikyti vienodą praktiką. Kibernetinio saugumo įstatymo 14 straipsnio 1 dalyje numatoma, kad Nacionalinis kibernetinio saugumo centras ir policija konsultuojasi ir bendradarbiauja tirdami kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimu susijusia informacija, reikalinga pagal kompetenciją šių institucijų funkcijoms atlikti. Tai reiškia, kad jei Nacionaliniam kibernetinio saugumo centrui prireiktų apriboti šių paslaugų teikimą, to jis galėtų siekti ir pagal galiojantį teisinį reguliavimą bendradarbiaudamas su policija. Atsižvelgiant į tai, turėtų būti išlaikoma esama atskirtis tarp Nacionalinio kibernetinio saugumo centro ir policijos įgaliojimų ir šiuo aspektu nauji įgaliojimai Nacionaliniam kibernetinio saugumo centrui neturėtų būti numatomi.

Siekiant efektyvesnės sukčiavimo kibernetinėje erdvėje prevencijos, turėtų būti tobulinamos kitos Kibernetinio saugumo įstatyme numatytos priemonės. Kibernetinio saugumo įstatymo 13 straipsnyje nurodytas Kibernetinio saugumo informacinis tinklas, kurio paskirtis – informacinių technologijų priemonėmis tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus, keistis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija. Pažymėtina, kad, vadovaujantis Kibernetinio saugumo įstatymo 13 straipsnio 4 dalimi, Kibernetinio saugumo informacinio tinklo duomenys, susiję su kibernetiniais incidentais, yra konfidencialūs ir teikiami tik šioje dalyje nurodytais atvejais. Siekiant teisinio aiškumo nustatant, kad Kibernetinio saugumo informaciniu tinklu būtų galima naudotis ir užtikrinant sukčiavimo kibernetinėje erdvėje prevenciją, Kibernetinio saugumo įstatymo 13 straipsnio 4 dalis turėtų būti papildoma atveju, kai Kibernetinio saugumo informacinio tinklo duomenys galėtų būti teikiami: „valdant ir tiriant kibernetinius incidentus tiek, kiek tai būtina šio įstatymo 14 straipsnio 1 ir 2 dalyse nustatytoms institucijų funkcijoms atlikti“.

2. Projektu siūlant keisti Kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 17 punktą, numatoma nauja Nacionalinio kibernetinio saugumo centro funkcija: tikrinti, kaip viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas vykdo privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę (toliau – nurodymas), jeigu to prašo nurodymą davusi institucija, ir apie patikrinimo rezultatus ją informuoti. Pažymėtina, kad domeno vardo, identifikuojančio interneto svetainę, blokavimas daugeliu atveju yra sietinas su neskelbtinos informacijos kontrole, o ne kibernetiniu saugumu, nes neskelbtinos informacijos prieinamumas pats savaime nesuponuoja kibernetinio incidento. Tai reiškia, kad Projektu Nacionaliniam kibernetinio saugumo centrui siūloma

numatyti funkciją, kurios tikslas daugeliu atveju nebūtų susijęs su Nacionalinio kibernetinio saugumo centro kompetencija.

Nurodymus duodančių institucijų (Lietuvos banko, Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos, Lošimų priežiūros tarnybos prie Lietuvos Respublikos finansų ministerijos, Žurnalistų etikos inspektoriaus tarnybos, Lietuvos radijo ir televizijos komisijos, Valstybinės vartotojų teisių apsaugos tarnybos, Narkotikų, tabako ir alkoholio kontrolės departamento) teisės ir pareigos, susijusios su nurodymų teikimu ir įgyvendinimu, įskaitant ir teisę skirti sankcijas už nurodymų nevykdymą, yra numatytos atitinkamą jų veiklą reglamentuojančiuose įstatymuose, pavyzdžiui, Lietuvos Respublikos visuomenės informavimo įstatyme, Lietuvos Respublikos vartotojų teisių apsaugos įstatyme, Lietuvos Respublikos azartinių lošimų įstatyme, Lietuvos Respublikos Lietuvos banko įstatyme ir kt.

Pritariant nurodymų davimo ir jų įgyvendinimo kontrolės efektyvumo didinimui, taip pat atsižvelgiant į tai, kad nurodymus įgyvendinantys subjektai kartu yra ir kibernetinio saugumo subjektai, veikiantys kibernetinėje erdvėje, efektyviausias būdas būtų ne numatyti dar vieną papildomą šiame procese dalyvaujančią instituciją, o didinti nurodymų davimo ir priežiūros efektyvumą, suteikiant nurodymus duodančioms institucijoms galimybę naudotis centralizuotu techniniu sprendimu, leisiančiu efektyviau vykdyti joms pavestas funkcijas, susijusias su nurodymų davimu ir jų įgyvendinimu. Toks techninis sprendimas galėtų būti Kibernetinio saugumo informacinio tinklo komponentas, kuris leistų keistis informacija tarp nurodymus duodančių institucijų ir šiuos nurodymus įgyvendinančių kibernetinio saugumo subjektų.

Pažymėtina, kad Nacionalinis kibernetinio saugumo centras kartu su Kauno technologijos universiteto padaliniu Interneto paslaugų centru (DOMREG) kovai su kibernetiniais incidentais, ypač su žaibiškomis kibernetinėmis sukčiavimo atakomis, sukūrė domenų vardų sistemos rekursinio sprendiklio su užkarda (toliau – DNS užkarda) paslaugą Lietuvos interneto naudotojams. DNS užkarda nuo įprastos rekursinės DNS paslaugų teikėjo teikiamos paslaugos skiriasi tuo, kad joje yra įdiegta papildoma saugos funkcija, skirta interneto naudotojams ir organizacijoms apsaugoti nuo kibernetinių grėsmių, tokių kaip netikros bankų svetainės, nesąžiningos e. prekybos platformos, kenkimo kodą platinančios svetainės ir kitos Nacionalinio kibernetinio saugumo centro patvirtintos žalingos svetainės. Šia paslauga, kaip alternatyva tarptautiniams ir nacionaliniams interneto paslaugų teikėjų domenų vardų sistemos rekursiniams sprendikliams, galėtų naudotis visi Lietuvos interneto paslaugų naudotojai.

Atsižvelgiant į tai, kad nurodyto techninio sprendimo suteikimas nurodymus duodančioms institucijoms nepatektų į įprastą kibernetinio saugumo sampratą, siūlytina nustatyti specialų teisinį reguliavimą ir Kibernetinio saugumo įstatymą papildyti 13^1 straipsniu, kuriame būtų reguliuojami teisiniai santykiai, susiję su Kibernetinio saugumo informacinio tinklo ypatumais:

„**13^1 straipsnis. Duomenų apie privalomus nurodymus tvarkymas Kibernetinio saugumo informaciniame tinkle**

1. Kibernetinio saugumo informaciniame tinkle įstatymų nustatytais atvejais tvarkomi duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę.

2. Šio straipsnio 1 dalyje nurodytus nurodymus duodančios institucijos ir juos įgyvendinantys kibernetinio saugumo subjektai privalo naudotis Kibernetinio saugumo informacinio tinklo dalimi, kurioje tvarkomi duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę, nepriklausomai nuo jų atitikties Kibernetinio saugumo informacinio tinklo nuostatuose nurodytiems reikalavimams.

3. Kibernetinio saugumo informaciniame tinkle viešai skelbiami duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę.“

Atsižvelgiant į tai, kad tokio pobūdžio pakeitimams įgyvendinti reikėtų modernizuoti Kibernetinio saugumo informacinį tinklą, pritarus siūlomiems pakeitimams turėtų būti koreguojama ir keičiamo įstatymo įsigaliojimo data – numatoma, kad tokio pobūdžio pakeitimai galėtų būti atliekami ne anksčiau kaip per vienerius metus nuo įstatymo priėmimo. Taip pat pažymėtina, kad siūlymams įgyvendinti 2023 m. ir kiekvienais ateinančiais metais Lietuvos Respublikos krašto apsaugos ministerijai iš valstybės biudžeto papildomai reikėtų skirti po 100 tūkst. Eur per metus.

Papildomai atkreiptinas dėmesys, kad įgyvendinus tokį techninį sprendimą įstatymuose, numatančiuose nurodymų davimą, turėtų būti numatyta, kad institucijos nurodymus operatoriams teikia per Kibernetinio saugumo informacinį tinklą. Kartu pažymėtina, kad įstatymų, nustatančių institucijų įgaliojimus duoti nurodymus, nuostatos dėl šių įgaliojimų įgyvendinimo, teismo sankcionavimo ir blokavimo įgyvendinimo tvarkos yra skirtingos, jų visų pakeitimas tik didintų teisėkūros apimtį, bet nepadidintų teisinio reguliavimo nuoseklumo, sistemingumo ir teisinio saugumo, todėl tokių įgaliojimų įgyvendinimo, teismo sankcionavimo ir blokavimo įgyvendinimo tvarka turėtų būti nustatoma bendrajame įstatyme, specialiuose įstatymuose nustatant tik nurodymų davimo teisinius pagrindus.

Ministras Pirmininkas

Krašto apsaugos ministras