LIETUVOS RESPUBLIKOS SEIMAS

LIETUVOS RESPUBLIKOS SEIMO KANCELIARIJOS
INFORMACIJOS IR KOMUNIKACIJOS DEPARTAMENTO
TYRIMŲ SKYRIUS

Gedimino pr. 53, 01109 Vilnius Tel.: (0 5) 209 6170 / (0 5) 209 6185
El. p.: tyrimai@lrs.lt; info@lrs.lt; ikd@lrs.lt www.lrs.lt/info

Analitinė apžvalga
25/27

2025-03-10

Skaitmeninis suverenitetas Europos Sąjungoje ir saugumas

Šiame darbe pateikiama skaitmeninio suvereniteto kaip siekio nustatyti ir ginti valstybių sienas pasaulinėje interneto infrastruktūroje samprata. Įvardinami skaitmeninio suvereniteto traktavimo Europos, Jungtinių Amerikos Valstijų (JAV) ir kitų šalių (Kinijos, Rusijos) tradicijose skirtumai, didžiausią dėmesį skiriant aktualiai Europos Sąjungos (ES) skaitmeninio suvereniteto politikai. Pristatoma skaitmeninio suvereniteto svarba fizinio saugumo bei kibernetinio saugumo situacijoms ES.

Svarbu atkreipti dėmesį į tai, kad praktinis skaitmeninio suvereniteto idėjos įgyvendinimas visada yra sudėtingas iššūkis ir nė viena Europos valstybė šiuo metu nėra visapusiškai suvereni skaitmeniniu požiūriu. Europos valstybių saugumo, kibernetinio saugumo politika ir IT aprūpinimo praktiniai aspektai dažnai yra silpnai susieti, todėl skaitmeninio suvereniteto de facto *praktika kartais prieštarauja paskelbtoms nacionalinėms skaitmeninio suvereniteto strategijoms.*

Dėl šios priežasties šiame darbe analizuojami aktualūs strateginiai ES lygmens skaitmeninio suvereniteto dokumentai: Skaitmeninių paslaugų aktas (įsigaliojo 2024 m.), Skaitmeninių rinkų aktas (2023 m.), Dirbtinio intelekto aktas (2024 m.), Europos lustų aktas (2023 m.), Duomenų valdymo aktas (2022 m.), Kibernetinio saugumo diplomatijos priemonių rinkinys (peržiūrėtas 2023 m.), 5G saugumo priemonių rinkinys (2021 m.).

Per praėjusias dvi Europos Parlamento kadencijas (2014–2019 m. ir ypač 2019–2024 m.) skaitmeninio suvereniteto klausimas ES tapo vienu iš strateginių prioritetų, o 2025 m. jis itin garsiai skamba JAV ir ES vertybinę priešpriešą ir interesų išsiskyrimą skaitmenizacijos klausimais išryškinančiose diskusijose. Šios diskusijos, pastaruoju metu virstančios ir atvira politine konfrontacija[1], atspindi augantį ES nerimą dėl skaitmeninių vyriausybinių paslaugų ir duomenų saugumo, ypač tais atvejais, kai skaitmeninė infrastruktūra priklauso nuo užsienio prekių ir paslaugų teikėjų. Didele dalimi šie tiekėjai – tai didžiosios IT korporacijos, tokios kaip „Google“, „Apple“, „Amazon“, „Meta“ (JAV), „Huawei“ (Kinija) ir kitos.

Skaitmeninis suverenitetas – tai valstybės gebėjimas užtikrinti skaitmeninių išteklių kontrolę fiziniu, programinio kodo ir duomenų lygmenimis. Fizinis lygmuo apima skaitmeninių technologijų infrastruktūrą; kodo lygmuo – programavimo standartus, taisykles ir dizainą; duomenų lygmuo –

[1] JAV pasipiktinimas ES skaitmeninio suvereniteto politika aktualus šiomis dienomis aiškinant aktyvią politinę ir ekonominę JAV konfrontaciją su Europa (pavyzdžiui, šiame technologijų ir verslo atstovo Mike Solana pareiškime: Solana, Mike. *Sucks to EU*: https://www.piratewires.com/p/sucks-to-eu, 2025-02-25), tačiau išsakomi argumentai ir vertybinė priešprieša buvo akivaizdi dar 2020 m.: Barker, Tyson. *Europe Can't Win the Tech War It Just Started. The European Union is running in circles in pursuit of "digital sovereignty."*: https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/, 2020-01-16.

skaitmeninę nuosavybę, informacijos srautus ir jų naudojimo taisykles[2]. Kitaip tariant, **skaitmeninio suvereniteto stiprinimas – tai siekis nustatyti ir ginti valstybių sienas pasaulinėje interneto infrastruktūroje**.

Pastebėtina, kad skaitmeninis suverenitetas, kaip gana nauja sąvoka, neturi labai griežtų apibrėžimo rėmų, tačiau turi nemažai sinonimų ir itin glaudžiai susijusių sąvokų. Skirtinguose šaltiniuose skaitmeninis suverenitetas gali būti vadinamas arba siejamas su sąvokomis kibernetinis suverenitetas, technologinis suverenitetas, duomenų suverenitetas, skaitmeninė autonomija, strateginė autonomija.

Bet kuri valstybė, susidurianti su geopolitine įtampa ar konkurencija, gali pagrįstai nerimauti dėl savo priklausomybės nuo kitose valstybėse teikiamų skaitmeninių paslaugų skaidrumo ir saugumo. Dėl tokios priklausomybės kyla rizika, susijusi su tuo, kad kitų valstybių subjektai gali gauti prieigą prie informacijos talpyklų, kuriose laikomi jautrūs duomenys ar prie įrenginių, kuriais teikiamos skaitmeninės vyriausybinės paslaugos.

Skaitmeninis suverenitetas turi technologinį, politinį, administracinį lygmenis. Technologinis lygmuo apima prieglobą (*hosting*) ir maršrutizavimą (*routing*); jis susijęs su pagrindinių valstybės paslaugų teikimu piliečiams ir valstybės bei piliečių bendravimu skaitmeninėje erdvėje. Politinis skaitmeninio suvereniteto lygmuo susijęs su tuo, kaip aukščiau minėtos technologinės problemos interpretuojamos vertybiškai, o administracinis – su tuo, kaip praktiniai jų sprendimai įgyvendinami teisinėje valstybės sistemoje.

Skaitmeniniam suverenitetui įvertinti svarbūs šie klausimai:

- kokiu mastu vyriausybinės interneto svetainės remiasi prieglobos ir debesijos (angl. *cloud*) infrastruktūra už savo jurisdikcijos ribų;
- kokia apimtimi piliečių ir vyriausybių tarpusavio sąveikų duomenų srautas išeina už fizinių valstybės jurisdikcijos ribų;
- kaip šie technologiniai sprendimai susiję su vyriausybės politika ir skaitmeninio suvereniteto strategija;
- kokią tiesioginę riziką šie technologiniai sprendimai kelia[3].

Skaitmeninis suverenitetas ir saugumas. Nors skaitmeninio suvereniteto sąvoka išlieka gana abstrakti, vienas konkretus aspektas, plačiai suprantamas kaip pagrindinė suvereniteto dalis, yra duomenų lokalizavimas. Geografinė ir organizacinė IT paslaugų ir duomenų srauto vieta yra svarbi valstybių ar valstybės remiamų veikėjų keliamų grėsmių požiūriu.

Grėsmių valstybinėms paslaugoms ir ryšiams modelis apima dvi pagrindines rizikos klases:

- riziką, susijusią su šias paslaugas teikiančiais priimančiaisiais įrenginiais (*hosts*);
- riziką, susijusią su duomenų srautu tarp priimančiųjų įrenginių ir vartotojų, visų pirma – piliečių.

Pirmoji rizikos klasė susijusi su grėsmėmis, kurias kelia kitose valstybėse esantys priimantieji įrenginiai. Dauguma valstybių turi fizinių ir teisinių priemonių gauti prieigą prie jų jurisdikcijoje esančių priimančiųjų įrenginių. Daugelis šalių yra priėmusios teisės aktus, kuriais joms suteikiama prieiga prie kitose šalyse esančių prieglobos įrenginių, jei juos valdo juridinis asmuo, susijęs su tos valstybės jurisdikcijai priklausančiu paslaugų tiekėju. Tokio teisės akto pavyzdys yra JAV CLOUD įstatymas[4].

---

[2] Musoni, Melody ir kiti. *Global approaches to digital sovereignty: Competing definitions and contrasting policy*, 2023: https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf , p. v.

[3] Bernardus Jansen ir kiti. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 2023, p. 2: https://doi.org/10.1016/j.giq.2023.101862

[4] Clarifying Lawful Overseas Use of Data Act (CLOUD Act). H.R.4943 - To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes: https://www.congress.gov/bill/115th-congress/house-bill/4943

Kitas šios rizikos klasės aspektas susijęs su situacija, kai valstybinius domenus aptarnauja komerciniai paslaugų teikėjai, kurie taip pat aptarnauja ir kitų klientų domenus. Pavyzdžiui, suinteresuoti subjektai gali tapti tos pačios infrastruktūros nuomininkais ir pasinaudoti šoninių kanalų atakomis (*side-channel attacks*), kad išgautų slaptus duomenis.

Antroji rizikos klasė yra susijusi su duomenų srauto trikdžiais tarp piliečių ir priimančiųjų įrenginių, kai teikiamos vyriausybinės paslaugos. Tokio duomenų srauto perėmimo rizika mažinama vyriausybinėse srityse plačiai pradėjus taikyti transporto lygmens saugumo (*Transport Layer Security*, TLS) protokolus.

Vis dėlto išlieka svarbi rizika, susijusi su šifruotais (*encrypted*) duomenimis, kurie pasiekia kitas jurisdikcijas. Net ir šifruojant išlieka du pagrindiniai pavojai: pirma, šifravimas nesutrukdo nutekinti metaduomenų; antra, perimtus užšifruotus duomenis galima saugoti ir iššifruoti ateityje, tai ypač aktualu tobulėjant kvantinės kompiuterijos galimybėms. Apskritai, kuo daugiau šalių ir organizacijų dalyvauja vyriausybinių paslaugų prieglobos ir maršrutizavimo procesuose, tuo jie gali tapti pažeidžiamesni įvairioms aukščiau minėtoms grėsmėms[5].

Skaitmeninis suverenitetas turi ir tiesioginį, ir netiesioginį poveikį fiziniam Europos saugumui. Viena vertus, ES kuria ir kontroliuoja saugumo skaitmeninėje erdvėje infrastruktūrą (netiesioginis poveikis fiziniam saugumui), kita vertus, skaitmeninės technologijos naudojamos šiuolaikinių saugumo sistemų valdymui teisingumo, vidaus reikalų, gynybos srityse (tiesioginis poveikis fiziniam saugumui). Atsižvelgiant į tai, kad kibernetinis saugumas neturi sienų, ES siekia organizuotai rinkti informaciją apie kibernetines grėsmes, teikti situacijos analizę, ir koordinuoti valstybių narių veiksmus kuriant naujas specializuotas įstaigas, pavyzdžiui, Europos Sąjungos tinklų ir informacijos apsaugos agentūrą (ENISA) ir Europos kibernetinių nusikaltimų tyrimo centrą (EC3)[6].

Skaitmeninis suverenitetas ES. Skaitmeninio suvereniteto stiprinimo politiką ES lemia tiek praktiniai interesai, tiek vertybiniai motyvai. Tai yra individualių asmens duomenų apsauga, Europos IT įmonių konkurencingumo didinimas, strateginių visuomenės interesų gynimas, didesnio atsparumo kibernetinėms rizikoms ir mažesnio pažeidžiamumo skaitmeninėms išorės intervencijoms siekis.

Skaitmeninio suvereniteto stiprinimo aktualumas ES susiformavo reaguojant į globalias skaitmenizacijos procesų tendencijas pasaulyje: JAV įsivyravimą interneto inovacijų srityje dešimto XX a. dešimtmečio pabaigoje bei Kinijos atsaką JAV skaitmeninei lyderystei. Kartais ES skaitmeninio suvereniteto politika vadinama „trečiuoju keliu tarp JAV nereguliuojamo skaitmeninio sekimo kapitalizmo ir Kinijos visuotiniu stebėjimu ir kontrole pagrįsto veikimo skaitmeninėje erdvėje“[7].

JAV būdingas itin liberalus požiūris į skaitmeninio suvereniteto klausimus, kuriame palaikoma nesuvaržyto skaitmeninio pasaulio vizija ir valstybės nesikišimo politika. Ji kritikuojama kitų pasaulio valstybių už tai, kad beveik nereguliuojamos didžiosios JAV IT korporacijos laisvai kaupia ir naudojasi vartotojų duomenimis juos monetizuodamos, analizuodamos ir įžvalgas naudodamos galimai manipuliaciniais tikslais[8].

Iš kitos pusės, du pastaruosius dešimtmečius Rusija ir Kinija siekia kontroliuoti tarptautinius ir vidaus informacijos srautus, įgalinančius jų režimų tęstinumą ir sistemiškai kuria valstybine kontrole pagrįstas nacionalines skaitmeninio suvereniteto technologines sistemas. Kinija siekia skaitmeninį suverenitetą laikyti lygiaverčiu teritoriniam suverenitetui. Tiek Didžioji Kinijos ugniasienė, tiek Rusijos parengti RuNet planai yra technologiniai skaitmeninio suvereniteto

---

[5] Bernardus Jansen ir kiti. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 2023, p. 3: https://doi.org/10.1016/j.giq.2023.101862

[6] Bellanova, Rocco. ir kiti. Digital/sovereignty and European security integration: an introduction. *European Security*, 31(3), 2022, p. 338: https://doi.org/10.1080/09662839.2022.2101887

[7] *What is digital sovereignty and how are countries aproaching it?* 2025-01-10: https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[8] Bernardus Jansen ir kiti. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 2023, p. 2–3.

įtvirtinimo projektai, kurių tikslas – blokuoti prieigą prie valstybės nepatvirtinto skaitmeninio turinio ir centralizuotai valdyti informacijos sklaidą šalių viduje[9].

Autokratiniais Kinijos ir Rusijos skaitmeninio suvereniteto modeliais didžioji dalis pasaulio valstybių neseka, tačiau ekonomiškai konkuruojančios su kaimynais ar patiriančios karinę grėsmę šalys įprastai siekia didesnio skaitmeninio suvereniteto siekdamos aktyviau apsaugoti savo skaitmeninę infrastruktūrą bei duomenis[10].

ES ir jos valstybės narės į platesnes diskusijas apie skaitmeninį suverenitetą įsitraukė reaguodamos į tokias grėsmes kaip galimas skaitmeninis šnipinėjimas (amerikiečių, rusų ir kinų), priklausomybė nuo užsienio technologijų ir infrastruktūros, priklausomybė nuo gyvybiškai svarbių skaitmeninės tiekimo grandinės elementų ir žaliavų, pavyzdžiui, puslaidininkių. Taip pat europiečiams itin aktualus duomenų saugumo ir etiško jų naudojimo klausimas[11]. Šios diskusijos vyksta didėjančios geopolitinės įtampos, JAV ir Kinijos ekonominės ir geopolitinės konkurencijos kibernetinėje erdvėje fone[12].

Skaitmeninio suvereniteto klausimus tarp ES valstybių narių anksčiausiai ėmė kelti Prancūzija ir Vokietija.

Prancūzijoje viešos diskusijos apie asmens duomenų privatumą internete dėl rinkoje dominuojančių didžiųjų JAV IT kompanijų ir dėl to galimai menkstančių Prancūzijos pramonės ir ekonominio vystymosi galimybių prasidėjo dar prieš dvidešimt metų. Valstybės lygmeniu inicijuoti politiniai šių problemų sprendimai, tačiau ilgainiui skaitmeninio suvereniteto klausimas, didele dalimi Prancūzijos ir kartu Vokietijos iniciatyva, buvo perkeltas į ES lygmenį.

Diskusijos dėl skaitmeninio suvereniteto šiek tiek vėliau kilo ir Vokietijoje, kur be Prancūzijos išryškintų klausimų apie valstybės galią reguliuoti asmenų skaitmeninį savarankiškumą bei ekonominį ir technologinį konkurencingumą, buvo taip pat pabrėžiama nacionalinės IT infrastruktūros apsaugos nuo išorinio kišimosi svarba, kontržvalgybinių technologijų kūrimas, duomenų perdavimo už ES ribų mažinimas ir technologinės priklausomybės nuo ne ES šalių ribojimas, skatinant europietiškų IT produktų kūrimą[13].

Prancūzai ir vokiečiai aktyviai palaikė nuomonę, kad skaitmeninis suverenitetas gali būti pasiektas ne tik veikiant nacionalinėms valstybėms, bet daugiausia bendradarbiaujant ES lygmeniu. Visą Jeano-Claude'o Junckerio Europos Komisijos (EK) kadenciją (2014–2019 m.) buvo galima stebėti besiformuojantį ES diskursą, kuris ne tik atspindėjo Prancūzijos ir Vokietijos išreikštas problemas (ekonominę, duomenų apsaugą, ES vertybes ir saugumą), bet taip pat reagavo į įvairius išorinius įvykius ir procesus, pavyzdžiui, 2013 m. Edwardo Snowdeno skandalą ir svetimų valstybių kišimąsi į demokratinius rinkimus bei referendumus.

2022 m. Europos skaitmeninis suverenitetas buvo Prancūzijos pirmininkavimo ES Tarybai prioritetas. Jį sudarė:

– ES apsauginės galios vaidmens stiprinimas, reiškiantis Europos piliečių, viešųjų paslaugų ir įmonių saugumą kibernetinėje erdvėje;

---

[9] Bellanova, Rocco. ir kiti. Digital/sovereignty and European security integration: an introduction. *European Security*, 31(3), 2022, p. 346: https://doi.org/10.1080/09662839.2022.2101887

[10] Čia svarbu paminėti, kad ne visada aukštesnis skaitmeninio suvereniteto laipsnis susijęs su poreikiu riboti kitos valstybės jurisdikcijos prieglobos ir kitų paslaugų teikėjus; pavyzdžiui, Ukrainos atveju vykstant kariniam konfliktui su Rusija kaip tik didesnis suvereniteto laipsnis buvo pasiektas naudojantis užsienio tiekėjų paslaugomis prieš pat 2022 m. vasario 24 d. Radai priėmus įstatymą, leidžiantį valstybinius duomenis perkelti į viešąją debesiją (buvo naudojamasi JAV įmonių „Microsoft" ir „Amazon" paslaugomis).

[11] Duomenų suverenitetas paprastai laikomas skaitmeninio suvereniteto porūšiu ir turi valstybės suvereniteto ir asmens suvereniteto elementų. Valstybiniu lygmeniu duomenų suverenitetas susijęs su duomenų kontrole tiek dėl ekonominių priežasčių (tokių kaip žaliava duomenų ekonomikai), tiek dėl politinių priežasčių, kai siekiama išlaikyti slaptų ir konfidencialių duomenų kontrolę.

[12] Bernardus Jansen ir kiti. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 2023, p. 3: https://doi.org/10.1016/j.giq.2023.101862

[13] Bellanova, Rocco. ir kiti. Digital/sovereignty and European security integration: an introduction. *European Security*, 31(3), 2022, p. 346–347.

- ES standartų nustatymo galios stiprinimas, apimantis demokratinių institucijų ir vertybių skaitmeninėje erdvėje skatinimą, sąžiningos skaitmeninės rinkos kūrimą bei technologinių įmonių atskaitomybę;
- ES inovacinės galios stiprinimas, pasireiškiantis per užsienio investicijų pritraukimą ir technologinių įmonių kūrimui palankios aplinkos ES formavimą;
- ES atvirumo stiprinimas, įkūnijantis atviros fizinės ir programinės įrangos kūrimą[14].

Skaitmeninis suverenitetas strateginiuose ES dokumentuose. Pagrindiniai strateginiai dokumentai, kuriais formuojama ES skaitmeninio suvereniteto politika siekiant bendros skaitmeninių technologijų naudojimo ir plėtros reguliacinės aplinkos, yra Skaitmeninių rinkų aktas, Skaitmeninių paslaugų aktas, Dirbtinio intelekto aktas, Lustų aktas, Duomenų valdymo aktas. Taip pat Kibernetinio saugumo diplomatijos priemonių rinkinys ir 5G saugumo priemonių rinkinys. Šių dokumentų turinys bus trumpai pristatomas šioje darbo dalyje.

Skaitmeninių paslaugų aktas, SPA (*Digital Services Act, DSA*). SPA reguliuoja internetinių paslaugų platformų veiklą. Pavyzdžiui, elektroninių parduotuvių, socialinių tinklų, turinio dalijimosi platformų, mobiliųjų programėlių parduotuvių, internetinių kelionių ir apgyvendinimo paslaugų platformų. SPA nuostatos taip pat taikomos interneto prieigos teikėjams, prieglobos (debesų kompiuterijos, tinklalapių prieglobos) paslaugų tiekėjams, domenų vardų registratoriams.

Pagrindiniai SPA tikslai yra užkirsti kelią neteisėtai ir žalingai veiklai internete, dezinformacijos plitimui, užtikrinti internetinių paslaugų vartotojų saugumą ir teises.

Kuriant SPA taip pat mėginta suderinti inovacijų ir skaitmeninės ekonomikos skatinimo ES tikslus su sąžininga konkurencija, plėtros galimybėmis mažesnėms internetinėms platformoms ir startuoliams, veikiantiems vidinėje ES rinkoje. Vartotojų, interneto platformų ir valdžios institucijų vaidmenys šiame dokumente siekiami subalansuoti suteikiant daugiau galios vartotojams, o ne didžiosioms interneto paslaugų korporacijoms, taip pat vidinei ES skaitmeninės ekonomikos ekosistemai suteikiant pranašumo prieš JAV įmonių dominavimą pasaulinėje interneto verslų rinkoje.

Nuo 2024 m. vasario 17 d. SPA taisyklės taikomos visoms ES veikiančioms interneto paslaugų platformoms. Nuo 2023 m. rugpjūčio pabaigos šios taisyklės buvo taikomos atskiroms platformoms, turinčioms daugiau nei 45 milijonus vartotojų ES (tai atitinka 10 proc. ES gyventojų), taip pat labai didelėmis internetinėmis paieškos sistemomis. SPA taip pat apibrėžiamos šių, dėl savo dydžio išskirtinių, interneto paslaugų tiekėjų pareigos krizinių situacijų atvejais. Jei dėl ypatingų aplinkybių kyla rimta grėsmė visuomenės saugumui ar sveikatai ES ar reikšmingose jos dalyse, Komisija gali reikalauti, kad šios itin didelės interneto paslaugų platformos, įvertinusios galimą savo indėlį, nustatytų ir taikytų veiksmingas ir proporcingas rizikos mažinimo priemones, skirtas užkirsti kelią, pašalinti ar apriboti tokį indėlį, taip pat pateiktų EK ataskaitą apie savo vertinimą ir atsaką[15].

Skaitmeninių rinkų aktas, SRA (*Digital Markets Act, DMA*). SRA reglamentuojamos šios interneto platformų paslaugos: internetinės tarpininkavimo paslaugos, interneto paieškos sistemos, internetinės socialinių tinklų paslaugos, dalijimosi vaizdo medžiaga platformų paslaugos, internetinio asmenų tarpusavio ryšio paslauga, operacinės sistemos, virtualieji asistentai, saityno naršyklės, debesijos kompiuterijos paslaugos, interneto reklamos paslaugos.

SRA įsigaliojo 2022 m. lapkričio 1 d. ir pradėtas taikyti 2023 m. gegužės 2 d. Per du mėnesius nuo šios datos įmonės, teikiančios pagrindines interneto platformų paslaugas, turėjo pateikti EK visą susijusią informaciją, kuri sutikrinama su SRA numatytais kriterijais. Pagal šiuos kriterijus didelės skaitmeninės platformos, remiantis jų ekonomine galia, vartotojų baze ir rinkos pozicija, identifikuojamos kaip prieigos valdytojai (*gatekeepers*).

Prieigos valdytojai įpareigojami laikytis SRA numatytų taisyklių, kad būtų užkirstas kelias nesąžiningai praktikai ir užtikrinama konkurencija. Taisyklės numato trečiųjų šalių sąveikumo

---

[14] Stanelytė, Augustė. *Prancūzijos skaitmeninis suverenitetas: didžiosios strategijos pokytis globalios technologinės konkurencijos amžiuje*. Vilniaus universitetas, Tarptautinių santykių ir politikos mokslų institutas, 2023: https://epublications.vu.lt/object/elaba:192826296/index.html

[15] Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 2022 m. spalio 19 d. dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas): https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32022R2065

leidimus, verslo vartotojų prieigos prie savo duomenų suteikimą ir susilaikymą nuo savo paslaugų protegavimo. EK suteikiami įgaliojimai tirti, užtikrinti atitiktį ir skirti baudas taisyklių nesilaikantiems prieigos valdytojams, įskaitant baudas iki 10 proc. jų pasaulinės apyvartos.

SRA siekiama skatinti skaitmeninės ekonomikos inovacijas ir verslo bei privačių vartotojų galią, sprendžiant duomenų kaupimo, patekimo į rinką kliūčių ir nesąžiningos rinkos galios panaudojimo klausimus. Taip pat dokumente numatoma periodiškai peržiūrėti prieigos valdytojų paskyrimus ir nustatytų įsipareigojimų veiksmingumą.

SRA papildo esamus ES konkurencijos teisės aktus ir siekia spręsti iššūkius, kuriuos kelia didelės skaitmeninės platformos sparčiai besivystančioje skaitmeninėje ekonomikoje.

Abu aukščiau minėtieji dokumentai – SPA ir SRA – sudaro bendrą normų rinkinį ir siekia dviejų pagrindinių tikslų: 1. sukurti saugesnę skaitmeninę erdvę, kurioje būtų apsaugotos pagrindinės ES skaitmeninių paslaugų vartotojų teisės; 2. sukurti vienodas sąlygas inovacijoms, augimui ir konkurencingumui skatinti tiek ES, tiek pasauliniu mastu[16].

Dirbtinio intelekto (DI) aktas (*Artificial Intelligence Act, AIA*). 2024 m. rugpjūčio 2 d. įsigaliojo DI aktas, kuriuo siekiama užtikrinti, kad ES diegiamos DI sistemos būtų saugios, patikimos ir suderintos su galiojančiais teisės aktais bei esminėmis ES vertybėmis. DI akte nustatomas rizika pagrįstų taisyklių rinkinys DI kūrėjams ir diegėjams. Šis aktas yra platesnio politikos priemonių paketo, skirto patikimo DI kūrimui remti, dalis, į kurią taip pat įeina DI inovacijų paketas, DI gamyklų steigimo planas ir koordinuotas DI plėtros planas.

Dokumento tikslas – pagerinti ES vidaus rinkos veikimą, skatinti į žmogų orientuoto ir patikimo DI naudojimą, užtikrinant aukšto lygio sveikatos, saugumo ir pagrindinių teisių apsaugą. Akto nuostatų taikymo sritis – DI sistemų kūrimui, pateikimui rinkai, pradėjimui naudoti ir naudojimui ES, nepriklausomai nuo tiekėjų ar diegėjų kilmės. DI akte, remiantis rizika grindžiamu požiūriu, draudžiamos tam tikros nepriimtinos su DI susijusios praktikos, nustatyti reikalavimai didelės rizikos DI sistemoms, nustatyti skaidrumo reikalavimai tam tikroms DI sistemoms.

Akto nuostatos netaikomos DI sistemoms, naudojamoms kariniais, gynybos ar nacionalinio saugumo tikslais. Taip pat siekiama netrukdyti inovatyvioms mokslinių tyrimų ir plėtros veikloms. DI aktas siekia užtikrinti saugų, patikimą ir etišką DI naudojimą ES, kartu palaikant DI srities inovacijas ir sąžiningą konkurencingumą[17].

Europos lustų aktas, ELA (*European Chips Act, ECA*). ES lustų aktas siekia sustiprinti regiono puslaidininkių gamybos pajėgumus[18]. Ši iniciatyva laikoma ne tik konkurencingumo klausimu, bet ir svarbiu technologinio suverenumo aspektu[19].

ELA tikslai – užtikrinti ES konkurencingumą ir inovacinį pajėgumą puslaidininkių srityje; pagerinti vidaus rinkos veikimą ir didinti ES atsparumą bei skaitmeninės ekonomikos vystymuisi gyvybiškai svarbių puslaidininkių tiekimo saugumą. ELA skatinamas puslaidininkių srities mokslinių tyrimų, technologijų plėtros ir inovacijų rėmimas, ypač kuriant pažangias bandomąsias linijas. Taip pat akcentuojamas Europos puslaidininkių kompetencijų centrų tinklo kūrimas, inovatyvių puslaidininkių gamybos įrenginių ir gamyklų ES steigimas, procesų stebėsena ir krizių, susijusių su puslaidininkių trūkumu Europoje, valdymas.

---

[16] Europos Parlamento ir Tarybos reglamentas (ES) 2022/1925 2022 m. rugsėjo 14 d. dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828 (Skaitmeninių rinkų aktas): https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32022R1925

[17] Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689 2024 m. birželio 13 d., kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas): https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=OJ:L_202401689

[18] *How can the European Union achieve digital strategic autonomy? Views from future leaders*, 2022-12: https://www.cidob.org/en/publications/how-can-european-union-achieve-digital-strategic-autonomy-views-future-leaders

[19] Musoni, Melody ir kiti. *Global approaches to digital sovereignty: Competing definitions and contrasting policy*, 2023: https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf

ELA vykdymą prižiūri ir krizių stebėseną atlieka Europos puslaidininkių taryba[20], kurią sudaro ES valstybių narių atstovai. ELA taip pat reglamentuojamas tarptautinis bendradarbiavimas puslaidininkių klausimais su trečiųjų šalių atstovais. Šiuo aktu siekiama stiprinti ES pozicijas pasaulinėje puslaidininkių rinkoje ir sumažinti ES priklausomybę nuo trečiųjų šalių puslaidininkių gamintojų, didinti technologinį suverenumą ir užtikrinti stabilų puslaidininkių tiekimą Europos pramonei[21].

Duomenų valdymo aktas, DVA (*Data Governance Act, DGA*). DVA įsigaliojo 2022 m. birželio 23 d. ir, pasibaigus 15 mėnesių lengvatiniam laikotarpiui, visa apimtimi taikomas nuo 2023 m. rugsėjo mėn. Jo tikslai – sukurti bendrą Europos duomenų erdvę, reglamentuoti viešojo sektoriaus subjektų saugomų duomenų pakartotinį naudojimą ir įgalinti saugų dalijimąsi duomenimis ES[22]. Šiame dokumente reglamentuojamas duomenų naudojimas ir dalijimasis duomenimis tarp viešojo ir privataus sektorių, taip pat nustatomos taisyklės duomenų tarpininkavimo paslaugoms ir „duomenų altruizmui“[23]. DVA nuostatos yra taikomos tiek asmens, tiek ne asmens duomenims. Jame nustatomos apsaugos priemonės ne asmens duomenų perdavimui į trečiąsias šalis. DVA įgyvendinimą prižiūri Europos duomenų inovacijų valdyba[24], kuri veikia kaip ekspertų iš visų ES valstybių narių grupė[25].

Kibernetinio saugumo diplomatijos priemonių rinkinys (*Cyber Diplomacy Toolbox*). Kenkėjiška kibernetinė veikla prieš ypatingos svarbos valstybinę infrastruktūrą ir kibernetinis šnipinėjimas tampa vis labiau sofistikuoti, o jų ardomasis poveikis kelia sisteminę grėsmę ES saugumui, ekonomikai, demokratijai ir visuomenei. Kaip atsaką į išaugusią valstybinių ir nevalstybinių subjektų kenkėjišką kibernetinę veiklą 2017 m. ES priėmė Kibernetinio saugumo diplomatijos priemonių rinkinį. Pagrindiniai jo tikslai – konfliktų prevencija, kibernetinio saugumo grėsmių mažinimas ir didesnis tarptautinių santykių stabilumas[26].

2023 m. Kibernetinio saugumo diplomatijos priemonių rinkinio gairės buvo peržiūrėtos ir patikslintos reaguojant į karinę Rusijos agresiją Ukrainoje, kai pastebėtas stipriai išaugęs kibernetinės erdvės nesaugumas[27]. Šiose gairėse pateikiama ES diplomatinio atsako į kenkėjišką kibernetinę veiklą sistema. ES pozicijos pagrindą sudaro penki pagrindiniai komponentai:

- kibernetinis atsparumas, gebėjimas užkirsti kelią kenkėjiškai kibernetinei veiklai ir nuo jos apsisaugoti;
- ES valstybių narių solidarumas ir krizių valdymo pajėgumų suderinimas;
- ES vizija dėl pasaulinės, atviros, laisvos, stabilios ir saugios kibernetinės erdvės reguliuojamos tarptautinės teisės ir taisyklėmis grindžiamos tvarkos;
- tvirti pasauliniai partnerystės ryšiai, ES pajėgumų stiprinimas trečiosiose šalyse;
- ES gebėjimas užkirsti kelią, atgrasyti ir reaguoti į grėsmių kėlėjus, siekiančius paveikti ES strateginius interesus, įskaitant jos partnerių saugumą, taip pat reagavimas į siekiančius sutrikdyti saugią ir atvirą prieigą prie kibernetinės erdvės bei ypatingos svarbos funkcijų.

2025 m. vasario 24 d. EK pristatytas naujas kibernetinio saugumo planas, skirtas ES kibernetinių krizių koordinavimui. Jis remiasi ES Kibernetinio saugumo diplomatijos priemonių

---

[20] European Semiconductor Board: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3932

[21] Europos Parlamento ir Tarybos reglamentas (ES) 2023/1781 2023 m. rugsėjo 13 d., kuriuo nustatoma Europos puslaidininkių ekosistemos stiprinimo priemonių sistema ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Lustų aktas): https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32023R1781

[22] Musoni, Melody ir kiti. *Global approaches to digital sovereignty: Competing definitions and contrasting policy*, 2023: https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf

[23] Duomenų altruizmas – tai savanoriškas dalijimasis duomenimis bendrojo intereso tikslais.

[24] Europos duomenų apsaugos valdyba: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_lt

[25] Europos Parlamento ir Tarybos reglamentas (ES) 2022/868 2022 m. gegužės 30 d. dėl Europos duomenų valdymo, kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1724 (Duomenų valdymo aktas): https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32022R0868

[26] Council of the European Union. *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox*, 2023-06-08: https://www.cyber-diplomacy-toolbox.com/Revised_Implementing_Guidelines_Cyber_Diplomacy_Toolbox.html

[27] Ten pat.

rinkiniu ir yra suderintas su Ypatingos svarbos infrastruktūros plano ir ES elektros energetikos sektoriaus kibernetinio saugumo tinklo kodekso nuostatomis[28]. Naujajame kibernetinio saugumo plane siūlomos priemonės stiprinti civilinių ir karinių subjektų bendradarbiavimą.

5G saugumo priemonių rinkinys (*Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*). Siekdama padidinti 5G interneto ryšio saugumą, 2021 m. EK pristatė 5G saugumo priemonių rinkinį, kuriuo nustatomi apribojimai nacionalinėms rinkoms, kad 5G infrastruktūra būtų apsaugota nuo kenėjiškų kibernetinių atakų[29].

Atlikus koordinuotą 5G tinklų saugumo rizikos vertinimą ES, nustatyta devynių rūšių rizika, suskirstyta į penkis rizikos scenarijus. 5G saugumo priemonių rinkinyje pateikiami išsamūs kiekvienos nustatytos rūšies rizikos mažinimo planai ir rekomenduojamos pagrindinės strateginės ir techninės priemonės, kurių turėtų imtis visos valstybės narės ir (arba) EK:

- griežtinti judriojo ryšio tinklų operatoriams taikomus saugumo reikalavimus;
- vertinti tiekėjų rizikos profilį;
- taikyti atitinkamus apribojimus tiekėjams, kurie laikomi keliančiais didelę riziką, be kita ko, taikyti būtinus su pagrindiniais objektais susijusius draudimus;
- užtikrinti, kad kiekvienas operatorius turėtų tinkamą kelių pardavėjų strategiją, kad būtų išvengta bet kokios didelės priklausomybės nuo vienintelio tiekėjo arba ji būtų apribota vengiant priklausomybės nuo tiekėjų, kurie laikomi keliančiais didelę riziką.

EK kartu su valstybėmis narėmis turėtų imtis priemonių, kuriomis, siekiant išvengti ilgalaikės priklausomybės, būtų išlaikoma 5G tiekimo grandinės diversifikacija ir tvarumas. Šiuo tikslu, be kita ko, turėtų būti:

- visapusiškai naudojamasi esamomis ES priemonėmis (tokiomis kaip tiesioginių užsienio investicijų tikrinimas, prekybos apsaugos priemonės, konkurencija);
- toliau stiprinami ES pajėgumai 5G ir vėlesnės kartos technologijų srityje naudojant atitinkamas ES programas ir finansavimą;
- sudaromos palankesnės sąlygos koordinuoti valstybių narių veiksmus standartizacijos srityje, kad būtų pasiekti konkretūs saugumo tikslai ir parengtos atitinkamos ES masto sertifikavimo schemos[30].

Pastaruoju metu pastebima, kad ES skaitmeninio suvereniteto politika tampa kur kas nuoseklesnė nei anksčiau, kai atskirų ES valstybių narių skaitmenizacijos strategijos, tyrėjų teigimu, ne visada sutapdavo su realia skaitmeninio suvereniteto praktika valstybėms teikiant skaitmenines paslaugas. Šis prasilenkimas pamažu išsprendžiamas tokiuose ES lygmens dokumentuose kaip aukščiau minėtieji Skaitmeninių paslaugų aktas, Skaitmeninių rinkų aktas ar DI aktas. Juose Europos ekonominiai interesai derinami su geopolitiniais argumentais ir realiomis IT infrastruktūros galimybėmis[31].

Parengė

Informacijos ir komunikacijos departamento
Tyrimų skyriaus
Patarėja dr. Veronika Urbonaitė-Barkauskienė,
tel. (0 5) 209 6180, el. p. veronika.urbonaite@lrs.lt

[28] European Commission. *Commission launches new cybersecurity blueprint to enhance EU cyber crisis coordination*, 2025-02-24: https://digital-strategy.ec.europa.eu/en/news/commission-launches-new-cybersecurity-blueprint-enhance-eu-cyber-crisis-coordination
[29] Europos Komisija. *5G saugumo priemonių rinkinys*: https://ec.europa.eu/newsroom/dae/redirection/document/64591
[30] Ten pat.
[31] Bernardus Jansen ir kiti. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 2023, p. 11: https://doi.org/10.1016/j.giq.2023.101862