

**Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra**

Gretos Činčikaitės,
Tarptautinės ir Europos Sąjungos teisės studijų šakos
V kurso, studentės

Magistro darbas

**Skaitmeninio suvereniteto iššūkiai žmogaus teisių apsaugai pagal tarptautinę ir ES
teisę**

**Digital Sovereignty Challenges for Human Rights Protection under International
and EU Law**

Vadovė: Doc. Dr. Vygantė Milašiūtė
Recenzentė: Vyr. lektorė. Dr. Gintarė Surblytė-Namavičienė

Vilnius
2026

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojami skaitmeninio suvereniteto keliamieji iššūkiai žmogaus teisių apsaugai tarptautinės teisės ir Europos Sąjungos teisės kontekste. Darbo tyrimo objektas, tai Europos Sąjungos formuojamas skaitmeninis suverenitetas. Pagrindinis šio mokslinio darbo tikslas yra įvertinti skaitmeninio suvereniteto įtaką žmogaus teisių užtikrinimui, nustatyti kylančias grėsmes ir apibrėžti sąlygas, kaip veiksmingai apsaugoti žmogaus teises skaitmeninėje aplinkoje.

Pagrindiniai žodžiai: skaitmeninis suverenitetas, žmogaus teisės, Europos Sąjunga, duomenų apsauga, skaitmeninė erdvė.

This research paper analyses the challenges posed by digital sovereignty to the protection of human rights in the context of international law and European Union law. The subject of this study is digital sovereignty as formed by the European Union. The main purpose of this research paper is to examine the impact of digital sovereignty on the protection of human rights, identify potential risks, and define the conditions for the effective protection of human rights in the digital environment.

Keywords: digital sovereignty, human rights, European Union, data protection, digital space.

TURINYS

IŽANGA	2
1. SKAITMENINIO SUVERENITETO SAMPRATA IR JOS VIETA ŠIUOLAIKINĖJE TEISINĖJE SISTEMOJE	4
1.1. Valstybės suvereniteto sampratos transformacija skaitmeninėje erdvėje.....	4
1.2. Skaitmeninio suvereniteto struktūriniai elementai kaip teisinio reguliavimo objektai	16
2. SKAITMENINIO SUVERENITETO POTENCIALAS STIPRINANT ŽMOGAUS TEISIŲ APSAUGĄ TARPTAUTINĖS IR ES TEISĖS KONTEKSTE	20
2.1. Tarptautinių žmogaus teisių normų taikymas skaitmeninėje erdvėje.....	20
2.2. Privatumo ir asmens duomenų apsaugos stiprinimas kaip skaitmeninio suvereniteto tikslas.....	26
2.3. Technologijų reguliavimas kaip žmogaus teisių apsaugos priemonė.....	36
3. SKAITMENINIO SUVERENITETO KELIAMOS GRĖSMĖS ŽMOGAUS TEISĖMS.....	43
3.1. Prioritetų disbalansas tarp technologijų plėtros ir žmogaus teisių apsaugos	43
3.2. Skaitmeninio suvereniteto piktnaudžiavimai: cenzūra ir masinė stebėsena.....	48
3.3. Teisinės gynybos trūkumas skaitmeninėje erdvėje	57
IŠVADOS IR PASIŪLYMAI.....	65
ŠALTINIŲ SĄRAŠAS	67
SANTRAUKA	80
SUMMARY	81

IŽANGA

Sparčiai besivystančios technologijos neišvengiamai veikia šiuolaikinę visuomenę. Vis daugiau visuomeninių santykių yra perkeliami į skaitmeninę erdvę, kurioje tradiciniai teisinio reguliavimo mechanizmai ne visada funkcionuoja taip pat efektyviai kaip ir realiame pasaulyje. Todėl formuojasi skaitmeninio suvereniteto koncepcija, susijusi su valstybių siekiu nustatyti kontrolę skaitmeninėje erdvėje.

Europos Sąjunga aktyviai skatina skaitmeninio suvereniteto politikos vystymą, todėl šiame moksliniame darbe skaitmeninis suverenitetas nagrinėjamas remiantis Europos Sąjungos aiškinimu bei taikymu. Europos Sąjungoje egzistuoja pakankamai išvystyta teisės aktų sistema, reguliuojanti skaitmeninę erdvę. Dėl to poreikis reguliuoti skaitmeninę aplinką nėra ginčytinas, o pagrindinis šio darbo klausimas glūdi kitur: kaip Europos Sąjunga gali praktiškai įgyvendinti skaitmeninį suverenitetą taip, kad jis iš tiesų prisidėtų prie žmogaus teisių apsaugos, o ne taptų kontrolės ir apribojimų priemone.

Nagrinėjamos temos aktualumas bei darbo originalumas. Skaitmeninio suvereniteto klausimai aktyviai diskutuoti tarptautiniu lygmeniu. Tuo tarpu Lietuvos Respublikos mokslinėje literatūroje trūksta išsamių teisinių tyrimų, išsamių teisinių tyrimų, analizuojančių skaitmeninį suverenitetą ir jo santykį su žmogaus teisių apsauga. Esami darbai yra fragmentiški. Jie analizuoja atskirus aspektus, pavyzdžiui, asmens duomenų apsaugą, tačiau pati skaitmeninio suvereniteto koncepcija išlieka mažai nagrinėta. Šią tendenciją atspindi ir darbe naudojami šaltiniai: didžiąją jų dalį sudaro anglų kalba parašyta mokslinė literatūra, Europos Sąjungos teisės aktai ir „minkštosios teisės“ (angl. soft law) teisės aktai. Pažymėtina, kad ši tema dažniausiai nagrinėjama kaip Europos Sąjungos politikos dalis ir retai analizuojama teisinio reglamentavimo aspektu. Todėl skaitmeninio suvereniteto teisinė analizė žmogaus teisių apsaugos kontekste įgyja išskirtinę reikšmę. Lietuvos Respublikoje, skaitmeninio suvereniteto tyrimas taip pat turi esminę svarbą nacionalinėje teisėje. Formuojama Europos Sąjungos politika yra perkeliama į nacionalinę teisę, t. y. yra priimami Europos Sąjungos reglamentai, kurie yra tiesiogiai taikomi Europos Sąjungos valstybėse narėse, perkeliamos Europos Sąjungos direktyvos bei nustatomos nacionalinės priežiūros institucijos Europos Sąjungos numatytam reguliavimui įgyvendinti.

Tyrimo objektas. Šio darbo tyrimo objektas yra skaitmeninis suverenitetas, kaip jis suprantamas ir įgyvendinamas Europos Sąjungos teisėje.

Darbo tikslas. Pagrindinis šio tariamo darbo tikslas – ištirti skaitmeninio suvereniteto įtaką žmogaus teisių apsaugai tarptautinės ir Europos Sąjungos teisės kontekste. Šiam tikslui pasiekti keliama keturi uždaviniai:

- 1) atkleisti skaitmeninio suvereniteto sampratą ir jos raidą;
- 2) įvertinti skaitmeninio suvereniteto galimybes stiprinti žmogaus teisių apsaugą;
- 3) nustatyti grėsmes, kurias skaitmeninis suverenitetas gali kelti žmogaus teisėms;
- 4) suformuluoti kriterijus, leidžiančius užtikrinti žmogaus teisių laikymąsi įgyvendinant skaitmeninį suverenitetą.

Darbo tyrimo metodai. Siekiant tinkamai įgyvendinti šio darbo tikslus ir uždavinius, pasitelkiami šie metodai:

- 1) lingvistinis metodas taikomas analizuojant ir aiškinant teisės aktų bei teismų praktiką;
- 2) lyginamasis metodas naudojamas lyginant, kaip skirtingose šalyse suprantamas skaitmeninis suverenitetas bei reguliuojama skiemeninė erdvė;
- 3) istorinis metodas taikomas siekiant atskleisti skaitmeninio suvereniteto sampratą ir raidą;
- 4) sisteminis metodas taikomas teisės aktų sistemei analizei;
- 5) analizės ir loginis tyrimo metodai naudojami viso darbo rašymo metu, kurių dėka buvo iškelti uždaviniai bei suformuotos išvados.

Pagrindiniai šaltiniai. Pagrindinius darbo šaltinius sudaro Europos Sąjungos teisės aktai, Europos žmogaus teisių konvencija, Europos Sąjungos Teisingumo Teismo ir Europos Žmogaus Teisių Teismo praktika. Darbe taip pat naudojami „minkštosios teisės“ šaltiniai – Europos Komisijos komunikatai ir strategijos. Be to, analizuojami tarptautinių organizacijų pranešimai ir įžvalgos. Iš mokslinės literatūros, darbe naudojami moksliniai darbai Lietuvos ir užsienio autorių - Egidijus Jarašiūnas, Theodore Christakis, Jacques Maritain, Edward Andrew, Jens Balterson, Michal Czerniawski ir kt.

1. SKAITMENINIO SUVERENITETO SAMPRATA IR JOS VIETA ŠIUOLAIKINĖJE TEISINĖJE SISTEMOJE

1.1. Valstybės suvereniteto sampratos transformacija skaitmeninėje erdvėje

Skaitmeninė erdvė ilgą laiką buvo laikoma laisva, praktiškai neribota ir globali, tačiau visiškai leistinumai ne visuomet yra gėris visuomenėje. Asmeniniai, darbo reikalai dažniau sprendžiami internete, kas lemia riziką įvairių pažeidimų atsiradimui. Suprantama, kad tai reikalauja vis didesnės apsaugos.

Kasmet Pasaulio ekonomikos forumo skelbiamame pranešime „Pasauliniai pavojai“ analizuojamos reikšmingiausios tarptautinės grėsmės, galinčios daryti įtaką ekonomikai, politikai, visuomenei bei aplinkai trumpalaikėje ir ilgalaikėje perspektyvoje. 2026 m. pranešime daug dėmesio skiriama kritinės svarbos infrastruktūros saugumui, akcentuojant, kad dėl vis didėjančios skaitmeninimo, automatizavimo ir sistemų tarpusavio sąveikos, pramoninė valdymo įranga gali būti nepakankamai apsaugota ir kontroliuojama, o tai tiesiogiai didina jos pažeidžiamumą¹. Dėl šių priežasčių nuosekliai auga tiek kibernetinių, tiek fizinių gedimų rizika. Remiantis Europos kibernetinių incidentų archyvas (EuRepoC) (angl. European Repository of Cyber Incidents (EuRepoC)) duomenimis, iki 2020 m. kibernetinių incidentų skaičius išliko palyginti nedidelis, tačiau nuo to laikotarpio pastebimas jų staigus augimas. Jei 2020 m. buvo užregistruoti 75 incidentai, tai 2023 m. jų skaičius išaugo iki 750 atvejų. Aukštas kibernetinių incidentų lygis išliko ir vėlesniais metais². Darytina išvada, kad per pastaruosius penkerius metus kibernetinės atakos iš pavienių incidentų tapo nuolatine ir sistemine grėsme tiek valstybių nacionaliniam saugumui, tiek privačių asmenų interesams. Natūralu, kad vis daugiau valstybių suinteresuotos nustatyti aiškią šių incidentų kontrolę, taip apsaugodamos save ir gyventojus bei įgyvendindamos savo suverenitetą skaitmeninėje erdvėje. Todėl tradicinis suvereniteto supratimas, pagrįstas teritoriniu ir valstybės valdžios viršenybės principu, skaitmeninėje erdvėje reikalauja peržiūrėjimo. Tačiau siekiant suformuoti naują valstybės suvereniteto modelį svarbu išanalizuoti pačią suvereniteto sampratą, kaip ji yra suvokiama tradicinėje teisinėje doktrinoje.

¹ World Economic Forum (2026-01-14). *Global Risks Report 2026* [interaktyvus]. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf, p. 51.

² European Repository of Cyber Incidents (EuRepoC) (n.d.). *Cyber Incident Dashboard* [interaktyvus]. <https://eurepoc.eu/dashboard/>.

Nagrinėjant suvereniteto sampratą svarbu atskleisti jo atsiradimo momentą. Etimologiškai terminas „suverenitetas“ yra siejamas su lotynišku žodžiu „superanus“, reiškiančiu „aukščiausias“ arba „viršesnis“, kuris istoriškai buvo vartojamas apibūdinant asmenį, turintį aukščiausią valdžią, pavyzdžiui, aukščiausiam teisėjui³. Suvereniteto sampratą ir jos reikšmę valstybės subjektiškumo kūrimui bei palaikymui savo veikaluose analizavo įvairūs teisės mokslininkai ir filosofai. Tačiau tradiciškai pati suvereniteto sąvoka yra siejama su Žano Bodeno veikalu „Šešios knygos apie valstybę“, kuriame pirmą kartą pavartotas šis terminas šiuolaikinio valstybingumo sampratai apibrėžti. Iš pradžių ši sąvoka buvo vartojama absoliutinės monarchijos požymiams įvardyti, tačiau vėliau ji pradėta taikyti kitoms valdymo formoms ir taip tapo viena iš labiausiai vartojamų sąvokų politinėje filosofijoje⁴. Ž. Bodeno teigimu, suverenitetas yra ne asmeninis valdovo atributas, o valstybės, kaip viešosios valdžios, savybė. Jis išskyrė tris pagrindinius suvereniteto požymius: pirma, suverenitetas yra nuolatinis, t. y. jis visada egzistuoja valstybėje ir yra būdingas visoms valdymo formoms; antra, suverenitetas yra absoliutus, nes suvereni valdžia nėra saistoma įstatymų nuostatų, piliečių bei pavaldinių atžvilgiu, tačiau ją riboja dieviškieji ir prigimtiniai įstatymai; ir trečia, suverenitetas yra nedalomas, todėl negali būti skaidomas tarp įvairių valstybės dalių ar valdžios institucijų⁵. Nepaisant istorinės suvereniteto sąvokos raidos, būtent Ž. Bodeno koncepcija sukūrė teorinį pagrindą šiuolaikinio suvereniteto, kaip pagrindinio valstybingumo elemento, supratimui.

Tuo tarpu, Egidijus Jarašiūnas savo moksliniame straipsnyje suverenitetą nagrinėja dviem aspektais: vidiniu, kuris pasireiškia tuo, kad valstybei priklauso aukščiausioji valdžia, ir išoriniu, reiškiančiu tam tikros valstybės nepriklausomybę nuo kitų valstybių⁶. Taigi, suverenitetas turėtų būti vertinamas kaip kompleksinė samprata, apimanti tiek valstybės vidaus aukščiausiąją valdžią jos teritorijoje, tiek išorinę nepriklausomybę tarptautiniuose santykiuose, o šių aspektų sąveika sąlygoja valstybės teisinį subjektiškumą. Kartu E. Jarašiūnas pabrėžia, kad požiūris į valstybės suverenitetą iš esmės pakito po Antrojo pasaulinio karo, nes vis stiprėjo žmogaus teisių apsaugos judėjimas ir valstybės

³ MARITAIN, Jacques (1950). The Concept of Sovereignty. *The American Political Science Review*, 44(2), 343-357 [interaktyvus]. <https://doi.org/10.2307/1950275>, p. 348.

⁴ TOTH, Zoltan (2023). Theories on sovereignty. *Central European Journal of Comparative Law*, 4(1), 175-195 [interaktyvus]. <https://doi.org/10.47078/2023.1.175-195>, p. 175.

⁵ ANDREW, Edward (2011). Jean Bodin on Sovereignty. *Republics of Letters: A Journal for the Study of Knowledge, Politics, and the Arts*, 2(2), 75-84 [interaktyvus]. https://shc.stanford.edu/sites/default/files/2011-03/roflv02i02_Andrew_060111_0.pdf, p. 76-78.

⁶ JARAŠIŪNAS, Egidijus. Valstybės suvereniteto kategorija tarpsisteminės sąveikos srityje: konstitucinio tapatumo alternatyva ar jo esminis elementas?. Iš: TVARONAVIČIENĖ, Agnė (red.), MILIUVIENĖ, Jolita (red.) ir VEČERSKYTĖ, Juta (red.) (2021). *Konstitucija ir teisinė sistema. Liber Amicorum Vytautui Sinkevičiui*. Vilnius: Mykolo Romerio universitetas, p. 46.

ėmė siekti šių teisių užtikrinimo ir apsaugos. Taip susiformavo naujas suvereniteto bruožas, pabrėžiantis, kad „valstybė nėra vien jėga, galinti daryti, ką nori, bet valdžia, grindžiama teise“⁷.

Taigi, apibendrinant galima teigti, kad suvereniteto samprata istoriniu lygmeniu pasikeitė nuo absoliučios ir neribotos valdžios koncepcijos iki teisinėmis normomis grindžiamos valstybės, išlaikančios esminį ryšį su valstybe bei jos teritorija.

Tačiau vykstant pasaulio raidai, stiprėja ir globalizacijos procesai. Globalizacija – tai daugiapakopis procesas, kurio metu stiprėja valstybių tarpusavio ryšiai ir tarpusavio priklausomybė. Šis procesas pasižymi tarptautinių ekonominių, socialinių, kultūrinių ir politinių ryšių augimu, kuris veda prie nacionalinių sienų erozijos ir tarptautinės tarpusavio priklausomybės stiprinimo. Pažymėtina, kad globalizaciją skatina informacinių technologijų plitimas, pasauliniai finansiniai srautai, tarptautinė prekyba ir kultūriniai mainai – formuojama pasikeitusi pasaulinė aplinka, kurioje veikia valstybės, įmonės ir privatūs asmenys⁸.

Teisiniu požiūriu globalizacija skatina tradicinio valstybės suvereniteto sampratos transformaciją, stiprindama tarptautinių normų ir institucijų reikšmę. Jensas Bartelsonas išskiria du požiūrius į globalizacijos proceso poveikį nusistovėjusiai suvereniteto sampratai. Pagal pirmąjį požiūrį, suvereni valstybė praranda pagrindinio valdžios nešėjo statusą, nes formuojasi naujos transnacionalinės valdžios ir bendruomenės organizavimo formos, peržengiančios įprastą vidaus bei tarptautinės sferų ribą. Šiomis sąlygomis suvereniteto samprata turi būti arba peržiūreta, arba jos visiškai atsisakyta. Pagal antrąjį požiūrį, suvereni valstybė, priešingai, ir toliau išlieka pagrindiniu valdžios nešėju, o viršvalstybinės institucijos vertinamos ne kaip silpninančios, bet kaip apsaugančios ir plėtojančios valstybės suverenitetą, kuris tebeišlaiko savo reikšmę⁹.

Pažymėtina, kad Europos Sąjungos (toliau – ES) sukūrimas yra vienas iš ryškiausių integracijos procesų pavyzdžių globalizacijos sąlygomis, kai dalis valstybės kompetencijų yra perduodama viršvalstybinio lygmens organizacijai. ES integracijos metu valstybės savanoriškai apribojo tam tikrus savo suvereniteto elementus, siekdamos gilesnio ekonominio, politinio ir teisinio bendradarbiavimo. Pabrėžtina, kad tuo pačiu valstybės

⁷ JARAŠIŪNAS, Egidijus. Valstybės suvereniteto kategorija tarpsisteminės sąveikos srityje: konstitucinio tapatumo alternatyva ar jo esminis elementas?. Iš: TVARONAVIČIENĖ, Agnė (red.), MILIUVIENĖ, Jolita (red.) ir VEČERSKYTĖ, Juta (red.) (2021). *Konstitucija ir teisinė sistema. Liber Amicorum Vytautui Šinkevičiui*. Vilnius: Mykolo Romerio universitetas, p. 50.

⁸ MAKOVETSKA, Nelia, DUBOV, Gennadii, DIDYCH, Taras ir kt. (2024). Global challenges to state sovereignty in the 21st century. *Salud, Ciencia y Tecnología - Serie de Conferencias*, 3 [interaktyvus]. <https://doi.org/10.56294/sctconf2024.661>, p. 3.

⁹ BARTELSON, Jens (2006). The Concept of Sovereignty Revisited. *The European Journal of International Law*, 17(2), 463-474 [interaktyvus], p. 464-465.

narės neatsisakė savo suvereniteto, kaip pagrindinio valstybingumo požymio, nes tam tikrų įgaliojimų perdavimas nereiškia jo praradimo. Vargu ar galima rasti bent vieną valstybę narę, kuri savo konstitucijoje nenurodytų, kad ji yra suvereni valstybė ir kad šis suverenitetas priklauso tautai. Ši koncepcija egzistuoja ir Lietuvos Respublikos Konstitucijoje (toliau – Konstitucija). Konstitucijos 1 straipsnyje nurodyta, kad Lietuvos valstybė yra nepriklausoma demokratinė respublika¹⁰.

Kaip jau minėta, nepriklausomybė yra vienas iš pagrindinių suvereniteto požymių, kuris reiškia laisvę veikti tam tikroje teritorijoje savo interesus atitinkančiu būdu. Tad galima teigti, kad nepriklausomybė yra ryškiausia suvereniteto sudedamoji dalis, o sąvokos „nepriklausoma“ ir „suvereni“, valstybės atžvilgiu, yra sinonimai – vartojant šiuos terminus teisės doktrinoje paprastai siekiama apibūdinti tą patį dalyką. Konstitucijos 2 straipsnyje nurodyta, kad suverenitetas priklauso Tautai. Konstitucijos 3 straipsnyje nurodyta, kad niekas negali varžyti ar riboti Tautos suvereniteto.

Analizuojant galimą suvereniteto sampratos pokytį po įstojimo į ES, svarbu pažymėti, kad, kaip nurodyta Konstitucijos 150 straipsnyje, viena jos sudedamųjų dalių yra 2004 m. liepos 13 d. Konstitucinis aktas „Dėl Lietuvos Respublikos narystės Europos Sąjungoje“, kurio 1 punkte nurodyta, kad „Lietuvos Respublika, būdama Europos Sąjungos valstybe nare, dalijasi ar patiki Europos Sąjungai valstybės institucijų kompetenciją sutartyse, kuriomis yra grindžiama Europos Sąjunga, numatytose srityse ir tiek, kad kartu su kitomis Europos Sąjungos valstybėmis narėmis bendrai vykdytų narystės įsipareigojimus šiose srityse, taip pat naudotųsi narystės teisėmis“¹¹. Matyti, kad dalis suverenių teisių perduodama viršnacionalinei institucijai. Be to, minėto Konstitucinio akto 2 punkte nurodoma, kad jeigu tai kyla iš sutarčių, kuriomis grindžiama Europos Sąjunga, Europos Sąjungos teisės normos taikomos tiesiogiai, o teisės normų kolizijos atveju jos turi viršenybę prieš Lietuvos Respublikos įstatymus ir kitus teisės aktus. Ši nuostata gali sudaryti klaidingą įspūdį, kad pagrindinis tautos valios išraiškos aktas – Konstitucija – yra sumenkinamas. Konstitucinis teismas sprendė, kiek šis teiginys nepažeidžia Konstitucijos viršenybės principo, nurodyto Konstitucijos 7 straipsnyje.

Dar 2006 m. Lietuvos Respublikos Konstitucinio Teismo 2006 m. kovo 14 d. nutarime Konstitucinis Teismas padarė išvadą, kad Konstitucijos viršenybės principas ir Konstitucijos 135 straipsnyje nurodytas *pacta sunt servanda* principas turi būti vertinami

¹⁰ Lietuvos Respublikos Konstitucija. Lietuvos Respublikos piliečių priimta 1992 m. spalio 25 d. referendume. *Valstybės žinios*, 1992, 33–1014.

¹¹ Lietuvos Respublikos Konstitucijos papildymo Konstituciniu aktu „Dėl Lietuvos Respublikos narystės Europos Sąjungoje“ ir Lietuvos Respublikos Konstitucijos 150 straipsnio papildymo įstatymas. *Valstybės žinios*, 2004-07-17, Nr. 111-4123.

sistemingai¹². Taip pat Lietuvos Respublikos Konstitucinio Teismo 2014 m. sausio 24 d. nutarime, Konstitucinis Teismas nurodė, kad „<...> visateisis Lietuvos Respublikos, kaip Europos Sąjungos narės, dalyvavimas joje yra Tautos suverenios valios pareiškimu grindžiamas konstitucinis imperatyvas, Lietuvos Respublikos visateisė narystė Europos Sąjungoje yra konstitucinė vertybė“¹³. O Lietuvos Respublikos Konstitucinio Teismo 2017 m. gruodžio 20 d. sprendime, Konstitucinis Teismas akcentavo, kad „<...> konstitucinis visateisio Lietuvos Respublikos dalyvavimo Europos Sąjungoje imperatyvas suponuoja ir konstitucinį Lietuvos Respublikos įsipareigojimą tinkamai įgyvendinti Europos Sąjungos teisės reikalavimus <...>“¹⁴. Vadinasi, Lietuvos įstojimas į ES yra sąmoningas ir demokratinis 2003 m. gegužės 10 ir 11 d. referendume priimtas tautos sprendimas. Šiuo atveju tam tikrų įgaliojimų perdavimas vyksta remiantis pačia Konstitucija, todėl toks žingsnis nėra suvereniteto praradimas, o yra jo realizavimas. Be to, Konstitucinis Teismas minėtame 2006 m. nutarime patikslino nustatytą kolizijos taisyklę ir išaiškino, kad ES teisė turi viršenybę prieš įstatymus, išskyrus pačią Konstituciją¹⁵.

Taigi, nėra pagrindo teigti, kad nacionalinė konstitucinė tvarka tampa besąlygiškai pavaldi ES teisei. Nors tam tikrose srityse ES teisė daro įtaką nacionalinei teisei ir gali reikalauti ją suderinti, tai nereiškia, kad Konstitucija praranda savo pamatinę reikšmę ar tampa antraeile. Todėl galima daryti išvadą, kad ES teisės ir nacionalinės teisės santykis labiau grindžiamas suderinimu ir pusiausvyra, o ne visišku pavaldumu ar konstitucinio savitumo praradimu. Lietuvos Respublikos Konstitucinio Teismo 2014 m. kovo 18 d. nutarime suformuota pozicija, kad kilus prieštaravimui tarp tarptautinių įsipareigojimų ir pagrindinio šalies įstatymo, „iš Konstitucijos 135 straipsnio 1 dalies Lietuvos Respublikai kyla pareiga tokį nesuderinamumą pašalinti *inter alia* atsisakant atitinkamų tarptautinėje sutartyje nustatytų tarptautinių įsipareigojimų vadovaujantis tarptautinės teisės normomis arba darant atitinkamas Konstitucijos pataisas“¹⁶.

Tad galima daryti išvadą, kad net įstojimas į tarptautinę sąjungą ir pavaldumas viršnacionaliniams valdymo organams nėra suvereniteto praradimas, kadangi kol toks sprendimas yra savanoriškas, teisiškai pagrįstas ir priimtas demokratiniu būdu, jis yra suprantamas kaip viena iš suvereniteto įgyvendinimo būdu. Todėl Lietuva, įstojusi į ES, neprarado savo nepriklausomybės ir dalyvauja kaip lygiateisė narė tiek ES viduje, tiek

¹² Lietuvos Respublikos Konstitucinio Teismo 2006 m. kovo 14 d. nutarimas. *Valstybės žinios*, 2006-03-16, 30-1050.

¹³ Lietuvos Respublikos Konstitucinio Teismo 2014 m. sausio 24 d. nutarimas. TAR, 2014-01-24, 478.

¹⁴ Lietuvos Respublikos Konstitucinio Teismo 2017 m. gruodžio 20 d. sprendimas. KT21-S11/2017.

¹⁵ Lietuvos Respublikos Konstitucinio Teismo 2006 m. kovo 14 d. nutarimas. *Valstybės žinios*, 2006-03-16, 30-1050.

¹⁶ Lietuvos Respublikos Konstitucinio Teismo 2014 m. kovo 18 d. nutarimas. TAR, 2014-03-19, 3226.

tarptautinėje bendruomenėje. Šiai pozicijai pritaria ir E. Jarašiūnas, nurodydamas, kad toks įgaliojimų perdavimas savaime nepaneigia valstybės suvereniteto, nes ji lieka nepriklausoma tol, kol kartu su kitomis valstybėmis narėmis lieka „sutarčių šeimininke“, t. y. turi galimybę savo nuožiūra atšaukti perduotus įgaliojimus¹⁷. Taigi, grįžtant prie J. Bartelsono įžvalgų apie globalizacijos poveikį suvereniteto sampratai, galima pagrįstai laikytis nuomonės, kad tarptautinės organizacijos nesilpnina valstybės suvereniteto, o yra tik politiškai ir ekonomiškai patogi bei racionali egzistavimo forma, kuri remia tolesnę valstybių integraciją į tarptautinius procesus ir skatinanti globalizaciją.

Iki šiol atlikta suvereniteto analizė pirmiausia buvo sutelkta į valstybės nepriklausomybę, jos teisę veikti savo nuožiūra savo valstybės viduje, tačiau nebuvo pakankamai akcentuojama, kad ši veikimo teisė, remiantis tradicine doktrina, galioja tik tam tikroje teritorijoje. Vis dėlto, naujų technologijų ir skaitmeninės erdvės plėtra kelia iššūkius šiai nusistovėjusiai sampratai. Tokiomis sąlygomis valstybės suverenitetas skaitmeninėje erdvėje pradeda transformuotis, pereinama nuo griežto teritorinio modelio prie funkcionalaus reguliavimo. Valstybės siekia įgyvendinti savo galią per teisinės normos, taikomas duomenų apsaugos, kibernetinio saugumo, skaitmeninių paslaugų ir dirbtinio intelekto srityse, kurios paliečia jų interesus, nepriklausomai nuo paslaugų teikėjų ar techninės infrastruktūros fizinės buvimo vietos. Taigi, natūralu, kad suverenitetą reikėtų sieti ne tik su fizinės erdvės kontrole, bet ir su gebėjimu nustatyti privalomą teisinį reguliavimą skaitmeninėje erdvėje, taip užtikrinant bendrą tvarką bei žmogaus teisių apsaugą.

Analizuojant tarptautinę suvereniteto reikšmę informacinėje erdvėje, svarbu pažymėti, kad egzistuoja įvairūs požiūriai ir politinės kryptys. Mokslinėje literatūroje paprastai išskiriamos trys pagrindinės koncepcijos, kurios apibrėžia skaitmeninės erdvės reguliavimą per tarptautinės teisės prizmę. Pirmoji koncepcija pabrėžia tarptautinių institucijų ir tarpvalstybinį bendradarbiavimą, kuris grindžiamas bendrais principais, jų svarbą valdant skaitmeninę erdvę. Tačiau egzistuoja ir liberalus požiūris, grindžiamas idėja, kad virtualioji erdvė turi išlikti kuo laisvesnė ir neturi būti per daug reguliuojama, nes tai galėtų apriboti interneto laisvę. Toks požiūris buvo išreikštas dar 1996 m., kai John Perry Barlow Davose vykusiame Pasaulio ekonomikos forumame paskelbė Kibernetinės erdvės nepriklausomybės deklaraciją, kurioje teigiama, kad šiai savarankiškai erdvei neturėtų būti

¹⁷ JARAŠIŪNAS, Egidijus. Valstybės suvereniteto kategorija tarpsisteminės sąveikos srityje: konstitucinio tapatumo alternatyva ar jo esminis elementas?. Iš: TVARONAVIČIENĖ, Agnė (red.), MILIUVIENĖ, Jolita (red.) ir VEČERSKYTĖ, Juta (red.) (2021). *Konstitucija ir teisinė sistema. Liber Amicorum Vytautui Sinkevičiui*. Vilnius: Mykolo Romerio universitetas, p. 64.

taikoma tradicinė valstybių jurisdikcija¹⁸. Taip pat egzistuoja požiūris, kad būtent pačios valstybės turėtų prisiimti atsakomybę už tiek nacionalinio, tiek tarptautinio virtualios erdvės teisinio reguliavimo formavimą¹⁹. Suprantama, kad šios anksčiau minėtos koncepcijos darė tiesioginę įtaką tarptautinės skaitmeninės erdvės reguliavimo raidai. Vis dėlto, akivaizdu, kad šioje srityje dar nėra suformuota vieninga, visapusiška ir efektyvi tarptautinės teisės sistema. Pagrindinis to veiksnys – tebevykstančios intensyvios mokslinės bei politinės diskusijos. Vienas iš klausimų, kuris yra keliamas, kalbant apie veiksmingo skaitmeninės erdvės kontrolės mechanizmo sukūrimą, yra jurisdikcija. Kaip jau minėta anksčiau, tarptautinėje teisėje jurisdikcija yra tradiciškai siejama su tarptautinės teisės subjektų bei teritorinių ribų, kuriose gali būti taikomos teisinės normos, apibrėžimu. Tačiau kibernetinėje erdvėje šiuos aspektus apibrėžti tampa vis sudėtingiau.

Skaitmeninėje aplinkoje veikiantys subjektai yra labai įvairūs: tai valstybės, didelės technologijų bendrovės, taip pat pavieniai juridiniai bei fiziniai asmenys. Papildomų iššūkių kyla ir dėl to, kad internetas vartotojams suteikia galimybę veikti anonimiškai. Be to, skirtingi skaitmeninės erdvės dalyviai turi savų interesų ir nevienodai vertina teisinio reguliavimo būtinybę bei jo formas. Dėl šių priežasčių kyla klausimai – kokie subjektai turėtų priimti sprendimus skaitmeninėje erdvėje ir kuriems klausimams reguliavimas yra būtinas. Tarptautinė bendruomenė iki šiol nepasiekė sutarimo dėl pačios kibernetinės erdvės teisinio statuso. Mokslinėje literatūroje išsakomos įvairios pozicijos: ar ją reikėtų laikyti bendra pasauline erdve, ar atskirų suverenių valstybių teritorijos dalimi, ar infrastruktūra bei vartotojų nacionaline kilme grindžiama sistema²⁰. Vieningo požiūrio trūkumas iš esmės apsunkina tarptautinės teisės jurisdikcijos nustatymą skaitmeninėje erdvėje.

Aptariant tarptautinį kontekstą, viena pirmųjų valstybių, kuri aktyviai pradėjo formuoti informacinės erdvės reguliavimą, yra Kinijos Liaudies Respublika (toliau – Kinija). Ši valstybė oficialiai įvedė terminą „internetu suverenitetas“. 2010 m. birželio mėnesį šis terminas buvo nurodytas Kinijos Liaudies Respublikos Valstybės tarybos Informacinio Biuro baltojoje knygoje „Internetas Kinijoje“. Šio dokumento 5 dalyje nurodoma, kad „Kinijos teritorijoje internetas priklauso Kinijos suverenitetui“, o „Kinijos suverenitetas

¹⁸ Electronic Frontier Foundation (n.d.). *A declaration of the Independence of Cyberspace* [interaktyvus]. <https://www.eff.org/cyberspace-independence>.

¹⁹ LEWIS, James Andrew (2010). Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*, 16(2), 55-65 [interaktyvus], p. 57.

²⁰ LIAROPOULOS, Andrew. Cyberspace Governance and State Sovereignty. Iš: BITROS, George C. (red.) and KYRIAZIS, Nicholas C. (red.) *Democracy and an Open-Economy World Order* (2017). Cham: Springer International Publishing AG. DOI10.1007/978-3-319-52168-8, p. 27.

internete turi būti gerbiamas ir saugomas“²¹. Ši sąvoka atspindi Kinijos valdančiosios partijos teiginį, kad tradicinis nacionalinio suvereniteto principas taikomas ir kibernetinei erdvei. Tokiu būdu valstybė deklaravo teisę kontroliuoti informacijos srautus internete tiek savo šalies viduje, tiek už jos ribų, net jei tai gali pažeisti asmenų, esančių už Kinijos fizinių sienų, teises²². Anupamo Chanderio ir Haocheno Sun atlikta analizė patvirtina, kad Kinijos paskelbtas skaitmeninis suverenumas sustiprino jos politinę kontrolę. Kinijoje skaitmeninės erdvės kontrolė įgyvendinama pasitelkiant tokias priemones kaip interneto filtravimas, skaitmeninis stebėjimas ir neteisėtas duomenų naudojimas. Visa tai lėmė žmogaus teisių pažeidimus²³.

Analogiški terminai, tokie, kaip „informacinis suverenitetas“, o vėliau „skaitmeninis suverenitetas“ yra vartojami ir Rusijos Federacijoje. Aktyvus dėmesys informacinės erdvės kontrolei ypač išaugo po 2014 m. įvykių. Ši tendencija atsispindi 2016 m. išleistoje Rusijos Federacijos „Informacinio saugumo doktrinoje“, kurioje įtvirtinta nacionalinių interesų apsaugos informacinėje srityje idėja. Dar didesnis poslinkis įvyko 2019 m. priėmus federalinių įstatymų pataisas, kurios visuomenėje tapo žinomos kaip įstatymas dėl „suverenaus interneto“²⁴. Šių pataisų tikslas yra sukurti nepriklausomą infrastruktūrą ir centralizuotai kontroliuoti duomenų srautą.

Abu paminėti atvejai yra orientuoti į duomenų kontrolę bei cenzūrą, todėl vėlesnėje mokslinėje literatūroje ši koncepcija tapo įvardijama kaip „skaitmeninis autoritarizmas“, kuris iki šiol tęsiasi, pasireikšdamas masiniais interneto blokavimais ir cenzūra skaitmeninėje erdvėje.

2024 m. gegužės 6 d. Jungtinės Amerikos Valstijos (toliau – JAV) paskelbė „Tarptautinę kibernetinės erdvės ir skaitmeninės politikos strategiją“, kurioje pagrindinis dėmesys skiriamas į JAV vadinamojo „skaitmeninio solidarumo“ kūrimą²⁵. Priešingai nei minėtuose pavyzdžiuose, ši politikos kryptis grindžiama atviro interneto bei globalios

²¹ China.org.cn (2010-06-08). *The Internet in China* [interaktyvus]. http://www.china.org.cn/government/whitepaper/node_7093508.htm.

²² China Media Project (2015-09-30). *Internet Sovereignty* [interaktyvus]. <https://chinamediaproject.org/2015/09/30/internet-sovereignty/>.

²³ CHANDER, Anupam ir SUN, Haochen. Digital Sovereignty as Double-Edged Sword. Iš: CHANDER, Anupam (red.) ir SUN, Haochen (red.) (2023). *Data Sovereignty. From the Digital Silk Road to the Return of the State*. New York: Oxford University Press, p.72-88. DOI: 10.1093/oso/9780197582794.001.0001, p. 88.

²⁴ LITVINENKO, Anna (2021). Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. *Media and Communication*, 9(4), 5-15 [interaktyvus]. <https://doi.org/10.17645/mac.v9i4.4292>. p. 75.

²⁵ U.S. Department of State. (2024-05-06). *Building Digital Solidarity: The United States International Cyberspace & Digital Policy Strategy* [interaktyvus]. <https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/>.

valstybių sąveikos koncepcijomis. Ja pirmiausia siekiama stiprinti tarptautinį pasipriešinimą skaitmeniniam autoritarizmui.

Tačiau „skaitmeninis suverenitetas“ – tai terminas, kuris labiausiai įsitvirtino ES. Svarbu pabrėžti, kad nors šis terminas vis dažniau vartojamas ES institucijų atstovų, tačiau neegzistuoja jo aiškos ir vieningos sąvokos. Taip pat išlieka diskusinis klausimas, ar ES jau turi skaitmeninį suverenitetą, ar tai tik ateities tikslas. Toks neapibrėžtumas apsunkina ES tikslų supratimą, be to, trukdo užtikrinti platų palaikymą ir veiksmingai įgyvendinti bendrą sukoordinuotą reguliavimo strategiją skaitmeninėje erdvėje.

Šio termino atsiradimą galima sieti su „technologinio suvereniteto“ idėjų sklaida, kurią inicijavo Emmanuelis Macronas. Jis pabrėžė, kad bendros skaitmeninės rinkos sukūrimas yra unikali galimybė parengti priemones, kurios leis užtikrinti tiek fizinių asmenų teisių bei privatumo apsaugą, tiek Europos įmonių duomenų saugumą. Pasak jo, pastarųjų rėmimas ir plėtra yra būtina sąlyga siekiant ES ekonominės gerovės²⁶. Vadinasi, jo požiūriu pagrindinis tikslas yra sukurti bendrą skaitmeninę rinką. 2019 m. Ursula von der Leyen savo politinėse gairėse taip pat pabrėžė apie „technologinio suvereniteto“ būtinybę²⁷.

Pats terminas „skaitmeninis suverenitetas“ pradėtas sistemingai naudoti oficialioje ES retorikoje, kai Europos Komisija 2020 m. paskelbė strateginį dokumentą Europos skaitmeninės ateities formavimas (angl. *Shaping Europe's Digital Future*)²⁸. Šis aktas yra Europos Komisijos komunikatas, t. y. dokumentas, priskiriamas minkštosios teisės kategorijai, kuris nors ir neturi privalomos teisinės galios pagal Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 288 straipsnį, tačiau jis nustato politikos ir reguliavimo gaires tolesnei ES teisės plėtrai skaitmeninėje erdvėje²⁹. Šiame komunikate detalizuojama skaitmeninio suvereniteto politika. Jame pagrindinis dėmesys skiriamas galimybei savarankiškai priimti sprendimus skaitmeninės aplinkos reguliavimo srityje. Taip siekiama mažinti priklausomybę nuo trečiųjų šalių ar didžiųjų technologijų įmonių. Pažymėtina, kad greta jau aptartų tikslų, tokių kaip technologinės infrastruktūros plėtra ir vartotojų duomenų apsauga, šiame dokumente „pasitikėjimas“ įvardijamas kaip esminis skaitmeninės

²⁶ Elysee (2017-09-26). *President Macron gives speech on new initiative for Europe* [interaktyvus]. <https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe>.

²⁷ European Commission (n.d.). *Political Guidelines. Ursula von der Leyen. Candidate for the European Commission President* [interaktyvus]. https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf.

²⁸ European Commission (2020-02-19). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future. COM(2020) 67 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067>.

²⁹ Sutarties dėl Europos Sąjungos veikimo suvestinė redakcija. OL C 202, 2016, p. 47–360.

transformacijos pagrindas. Komunikate pabrėžiama, kad be vartotojų pasitikėjimo technologijomis, šių technologijų naudojimo saugumu ir skaidria duomenų valdymo politika neįmanoma sukurti visiškai funkcionuojančios skaitmeninės ekonomikos³⁰. Ši išvalga yra pagrįsta, nes būtent privačių asmenų ir verslo subjektų palaikymas turi lemiamą reikšmę sėkmingos šios politikos įgyvendinimui. Panašu, kad klausimas, kaip įveikti žmonių baimę dėl visuotinio skaitmenizavimo ir kontrolės, yra tolesnio švietimo ir komunikacijos su visuomene uždavinys. Siekiant, kad visuomenė ir įmonės pritartų griežtesniam teisiniam reguliavimui, būtina aiškiai pagrįsti jo teikiamą naudą, kuri turėtų atsvirti galimus suvaržymus. Priešingu atveju, skaitmeninio suvereniteto politika galiausiai pavirs skaitmeninio autoritarizmo politika, ką jau galime stebėti kitose šalyse. Komunikate taip pat yra pabrėžiama, kad „<...> žalioji ir skaitmeninė transformacija – turi vykti kartu“³¹. Tačiau manytina, kad skaitmenizavimą šiame kontekste tikslinga nagrinėti keliais aspektais. Viena vertus, kaip pagrįstai pažymėta komunikate, technologijos yra efektyvus įrankis ES žaliojo kurso tikslams pasiekti, įskaitant energijos vartojimo efektyvumo didinimą bei neigiamo poveikio aplinkai mažinimą. Kartu pripažįstama, kad pats skaitmeninis sektorius daro reikšmingą poveikį aplinkai, todėl būtina ir toliau jį transformuoti ekologiškumo linkme³².

Išaugusį susidomėjimą skaitmeninio suvereniteto tema patvirtina 2025 m. lapkričio 18 d. Berlyne įvykęs aukščiausiojo lygio susitikimas „Summit on European Digital Sovereignty“. Šiame susitikime ES valstybės narės priėmė politinę deklaraciją dėl Europos skaitmeninio suvereniteto³³. Nors deklaracijos tekste akcentuojama, kad tai nėra teisiškai įpareigojantis dokumentas, vis dėlto ši deklaracija nustato bendrą ES politikos bei teisinio reguliavimo kryptį skaitmeninėje srityje. Tai patvirtina ir tai, kad šią deklaraciją vieningai parėmė visos ES valstybės narės. Dokumente skaitmeninis suverenitetas, vėlgi, suprantamas, ne kaip klasikinė teritorinė kontrolė, o kaip ES bei valstybių narių gebėjimas veikti skaitmeninėje erdvėje autonomiškai. Tai apima savarankišką infrastruktūros, duomenų bei technologijų naudojimo taisyklių nustatymą ir sprendimų priėmimą šiose srityse. Kartu pabrėžiama, kad siekiama ne izoliacijos, o bendradarbiavimo, nes tekste aiškiai nurodoma, kad „<...> skaitmeninis suverenitetas nereiškia izoliacijos ar

³⁰ European Commission (2020-02-19). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future. COM(2020) 67 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067>.

³¹ *Ibid.*

³² *Ibid.*

³³ Bundesministerium für Digitales und Staatsmodernisierung (2025-11-17). *Summit for More Digital Sovereignty Starts in Berlin* [interaktyvus]. <https://bmfs.bund.de/aktuelles/pressemitteilungen/detail/summit-for-more-digital-sovereignty-starts-in-berlin>.

protekcionalizmo <...>³⁴. Tai patvirtina, kad šiuolaikinė skaitmeninio suvereniteto samprata grindžiama ne uždaru, o autonomijos, savarankiško teisinio reguliavimo bei tarptautinio bendradarbiavimo deriniu.

Autonomija taip pat pasireiškia per duomenų srautų kontrolę. Europos Komisijos 2020 m. priimtoje „Europos duomenų strategijoje“ pabrėžiama būtinybė sukurti bendras ES duomenų erdves. Taip siekiama sustiprinti duomenų valdymą ES viduje bei sumažinti priklausomybę nuo išorės subjektų, ypač nuo stambių tarptautinių technologinių bendrovių³⁵. Vėlesniuose politiniuose dokumentuose, įskaitant 2021 m. Europos Komisijos komunikatą „2030 m. skaitmeninės politikos kelrodis: Europos skaitmeninio dešimtmečio kelias“, toliau sistemingai plėtojamas požiūris, kad skaitmeninis suverenumas yra neatskiriama ES strateginės autonomijos dalis³⁶.

Teisės aktuose, priimtuose plėtojant skaitmeninio suvereniteto strategiją, pavyzdžiui, Europos Parlamento ir Tarybos 2022 m. spalio 19 d. reglamente (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas)³⁷ (toliau – Skaitmeninių paslaugų aktas) ir Europos Parlamento ir Tarybos 2022 m. rugsėjo 14 d. reglamente (ES) 2022/1925 dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828 (Skaitmeninių rinkų aktas)³⁸, (toliau – Skaitmeninių rinkų aktas) terminas „skaitmeninis suverenitetas“ nėra tiesiogiai įtvirtintas kaip teisinis apibrėžimas. Tačiau jų reguliavimo logika yra akivaizdžiai nukreipta į ES kontrolės stiprinimą skaitmeninių platformų, infrastruktūros ir duomenų srautų atžvilgiu, kas praktiškai iliustruoja skaitmeninio suvereniteto strategijos įgyvendinimą. Svarbu pažymėti, kad Europos skaitmeninio suvereniteto kontekste dėmesys sutelkiamas ne į cenzūrą ir (ar) apribojimus, o į saugios ir vientisos skaitmeninės erdvės kūrimą. Šiuo tikslu 2022 m. Europos Parlamentas ir ES Taryba priėmė sprendimą, kurio nustatė 2030 m.

³⁴ Council of the European Union (2025-11-27). *Declaration for European Digital Sovereignty*, ST 15781/25 [interaktyvus]. <https://data.consilium.europa.eu/doc/document/ST-15781-2025-INIT/en/pdf>.

³⁵ Europos Komisija (2020-02-19). *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Europos duomenų strategija*, COM(2020) 66 final [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52020DC0066>.

³⁶ Europos Komisija (2021-03-09). *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: 2030 m. skaitmeninės politikos kelrodis: Europos skaitmeninio dešimtmečio kelias*, COM(2021) 118 final [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52021DC0118>.

³⁷ Europos Parlamento ir Tarybos 2022 m. spalio 19 d. reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas). OL L 277/1, 2022, p. 1–102.

³⁸ Europos Parlamento ir Tarybos 2022 m. rugsėjo 14 d. reglamentas (ES) 2022/1925 dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828 (Skaitmeninių rinkų aktas). OL L 265/1, 2022, p. 1–66.

Skaitmeninio dešimtmečio politikos programą. Pirmas tikslas, nurodytas šio sprendimo 3 straipsnio 1 dalies a punkte, yra „skatinti į žmogų orientuotą, pagrindinėmis teisėmis grindžiamą, įtraukią, skaidrią ir atvirą skaitmeninę aplinką, kurioje saugios ir sąveikios skaitmeninės technologijos ir paslaugos būtų prieinamos visiems visoje Sąjungoje ir jas naudojant būtų laikomasi Sąjungos principų, teisių bei vertybių ir jie būtų stiprinami“³⁹. Tai patvirtina, kad pagrindinis akcentas teikiamas žmogaus teisių užtikrinimui skaitmeninėje aplinkoje. Be to, to paties straipsnio 1 dalies c punkte nurodoma, kad siekiama „užtikrinti Sąjungos skaitmeninį suverenumą atviruoju būdu <...>“⁴⁰. Tai atskleidžia specifinį suverenumo pobūdį informacinėje erdvėje – ES nesiekia izoliuotis nuo globalaus interneto tinklo. Priešingai, pagrindinis tikslas yra įgyti gebėjimą savarankiškai kontroliuoti skaitmenines technologijas, infrastruktūrą bei duomenis. Taip siekiama sumažinti kritinę priklausomybę nuo trečiųjų šalių bei jų kontroliuojamų technologinių platformų.

Taigi, atsižvelgiant į atliktą skaitmeninio suvereniteto sąvokos analizę, galima išvesti jos bendrą apibrėžimą, o būtent, kad skaitmeninis suverenitetas yra:

(1) ES politinis kursas, todėl kita analizė moksliniame darbe bus atliekama atsižvelgiant būtent į ES teisinę sistemą, atliekant pavienius palyginimus su kitomis skaitmeninio reguliavimo sistemomis;

(2) nors tai politinis terminas, šiame darbe skaitmeninis suverenitetas bus nagrinėjamas teisėkūros sritis, tačiau visiškai atsiriboti nuo politinio diskurso nepavyks, nes būtent politinės gairės bei pareiškimai leidžia tiksliau interpretuoti teisinio reguliavimo tikslus bei jų esmę;

(3) nors skaitmeninis suverenitetas susideda iš įvairių struktūrinių elementų (plačiau apie juos – 1.2 poskyryje), esminį jo tikslą galima apibrėžti kaip siekį skaitmeninėje erdvėje nustatyti tokias pačias reguliavimo priemones, kokios galioja fizinėje erdvėje. Šios priemonės turi būti aiškos, veiksmingos, saugančios tiek visos ES interesus, tiek atskirų rinkos dalyvių teises. Taip pat jos privalo numatyti mechanizmus, leidžiančius efektyviai ginti savo pažeistas teises. Be to, nustatytos priemonės turi būti tinkamai integruotos į ES teisinę sistemą, o tai, be kita ko, reiškia ir pagrindinių ES vertybių apsaugą.

³⁹ Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. sprendimas (ES) 2022/2481 kuriuo nustatoma 2030 m. Skaitmeninio dešimtmečio politikos programa. OL L 323, 2022, p. 4-26.

⁴⁰ *Ibid.*

1.2. Skaitmeninio suvereniteto struktūriniai elementai kaip teisinio reguliavimo objektai

Terminas „skaitmeninis suverenitetas“ ES teisėje nėra įtvirtintas vienu bendru teisės aktu, kuris apimtų visas reguliavimo sritis. Priešingai, oficialiose strategijose jis vartojamas kaip politinis ir teisinis tikslas, įgyvendinamas per teisinio reguliavimo objektų rinkinį, t. y. atskiras sritis, reglamentuojamas konkrečiais teisės aktais.

2030 m. Skaitmeninio dešimtmečio strategijoje (3-4 straipsniuose) galima rasti tokių reguliavimo sričių paminėjimus, kaip: (1) skaitmeninės infrastruktūros ir duomenų plėtra; (2) kibernetinis saugumas; (3) skaitmeninė ekonomika ir konkurencija; (4) technologijų plėtra; (5) skaitmeninių įgūdžių ugdymas visuomenėje; (6) prieigos prie technologijų užtikrinimas ir skaitmeninės nelygybės mažinimas; (7) verslo ir viešųjų paslaugų skaitmenizavimas; (8) skaitmeninės aplinkos reguliavimas; (9) skaitmeninių technologijų tvarumas aplinkai. Šių sričių reguliavimas vykdomas lygiagrečiai, todėl sudėtinga išskirti prioritetines sritis, nes visos jos yra glaudžiai susijusios tarpusavyje ir viena kitą papildo įgyvendinant bendrą ES skaitmeninio suvereniteto politiką. Visgi mokslinėje literatūroje autoriai, priklausomai nuo tyrimo krypties, akcentuoja skirtingus ir, jų nuomone, svarbiausius šios strategijos elementus.

Pavyzdžiui, Theodoras Christakis savo tyrime, kuriame analizavo ES skaitmeninį suverenitetą, išskyrė du, jo nuomone, esminius skaitmeninio suverenumo elementus. Pirma, „skaitmeninis suverenitetas“ traktuojamas kaip teise reguliuoti tai, kas vyksta skaitmeninėje srityje, įskaitant didžiųjų informacinių technologijų bendrovių veiklą. Būtent tai Europos Vadovų Taryba įvardija kaip Europos gebėjimą stiprinti savo galias nustatyti taisykles bei naudoti priemones, leidžiančias formuoti pasaulinius standartus. Antra, skaitmeninis suverenitetas traktuojamas kaip priemonė strateginei autonomijai pasiekti ir Europos technologiniam konkurencingumui didinti, t. y. tai, ką Europos Vadovų Taryba vadina savarankišku technologijų pasirinkimu, taip pat strateginių skaitmeninių galimybių ir infrastruktūros kūrimu ir įdiegimu⁴¹.

Tuo tarpu, P. Coletti, S. Ducci ir F. N. Moro atliktame tyrime nurodo, kad mokslinėje literatūroje išskiriami trys skaitmeninio suvereniteto komponentai: (1) infrastruktūros

⁴¹ CHRISTAKIS, Theodore (2020). *“European Digital Sovereignty”: Successfully Navigating Between the Brussels Effect and Europe’s Quest for Strategic Autonomy* [interaktyvus]. Multidisciplinary Institute on Artificial Intelligence / Grenoble Alpes Data Institute. <http://dx.doi.org/10.2139/ssrn.3748098>, p. 11.

kontrolė, (2) konkurencingų europietišκών skaitmeninių technologijų plėtra ir (3) piliečių bei jų teisių apsauga⁴².

Tikslinga apžvelgti ir 2025 m. Berlyne įvykusį aukščiausiojo lygio susitikimą, kuris atspindi pagrindines šiuolaikinės ES politikos kryptis skaitmeninėje erdvėje. Šiame susitikime buvo organizuota paroda, sudaryta iš šešių teminių paviljonų, kurie vaizdingai iliustravo pagrindines ES skaitmeninio suvereniteto vystymo kryptis. Paviljonai apėmė tokias sritis kaip skaitmeninės infrastruktūros ir „žaliųjų“ informacinių technologijų plėtra, startuolių ir inovacijų rėmimas, dirbtinio intelekto pritaikymas, bei atviros programinės įrangos naudojimas. Taip pat akcentuotas Europos elektroninių mokėjimo sprendimų kūrimas (pavyzdžiui, projektas „WERO“) bei debesijos technologijų ir duomenų erdvių plėtra (ypač „Gaia-X“ iniciatyva). Parodoje buvo demonstruojami tiek technologiniai sprendimai (įskaitant superkompiuterius, kvantines technologijas ir dirbtinį intelektą), tiek instituciniai metodai, skirti užtikrinti skaidrumą, kontrolę ir saugumą skaitmeninėje aplinkoje⁴³. Taigi, šis susitikimas atskleidė kompleksinį ES skaitmeninio suvereniteto įgyvendinimo pobūdį, kuris vykdomas plėtojant skaitmeninę infrastruktūrą, skatinant inovacijas, tobulinant teisinį reguliavimą ir kuriant savas technologines ekosistemas.

Kiti autoriai, atlikę „Google“ puslapių, kuriuose minimas skaitmeninis suverenitetas, analizę, pagal vartojimo dažnumą išskiria šias pagrindines jo sudedamąsias dalis: (1) duomenų kontrolę; (2) ES įtakos didžiųjų neeuropietišκών įmonių (ypač tarptautiniu mastu veikiančių internetinių platformų) kontrolei stiprinimą, (3) pagrindinės skaitmeninės infrastruktūros tobulinimą; (4) naujų technologijų, tokių, kaip puslaidininkių gamyba, superkompiuterių kūrimas ir dirbtinio intelekto valdymas, reguliavimą; (5) kibernetinio saugumo stiprinimą⁴⁴.

Nagrinėjant kiekvieną iš šių sričių, tikslinga sistemingai išanalizuoti, kokie konkretūs teisės aktai buvo priimti siekiant jas reguliuoti. Analizuojant mokslinę literatūrą bei ES politines gaires, matytina, kad ypatingas dėmesys skiriamas duomenų kontrolei (pažymėtina, kad aptariamuoju atveju šią sąvoką reikėtų suprasti plačiąja prasme, o ne tik kaip asmens duomenų apsaugą), kuri įgyvendinama priimant tokius teisės aktus kaip:

⁴² COLETTI, Paola, DUCCI, Cecilia ir MORO, Francesco Niccolo (2025). Digital Sovereignty and the EU's Identity between Technological Innovation and European Values. *JCMS: Journal of Common Market Studies*, p. 1-19 [interaktyvus]. <https://doi.org/10.1111/jcms.70074>. p. 3.

⁴³ Bundesministerium für Digitales und Staatsmodernisierung (2025-11-17). *Summit for More Digital Sovereignty Starts in Berlin*. [interaktyvus]. <https://bmds.bund.de/aktuelles/pressemitteilungen/detail/summit-for-more-digital-sovereignty-starts-in-berlin>.

⁴⁴ ROBERTS, Huw, COWLS, Josh, CASOLARI, Federico ir kt. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet policy review*, 10(3) [interaktyvus]. DOI10.14763/2021.3.1575.

Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR), Europos Parlamento ir Tarybos 2022 m. gegužės 30 d. reglamentas (ES) 2022/868 dėl Europos duomenų valdymo, kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1724 (Duomenų valdymo aktas)⁴⁵ (toliau – Duomenų valdymo aktas); Europos Parlamento ir Tarybos 2023 m. gruodžio 13 d. reglamentas (ES) 2023/2854 dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/2394 ir Direktyva (ES) 2020/1828 (Duomenų aktas)⁴⁶ (toliau – Duomenų aktas); Europos Parlamento ir Tarybos 2018 m. lapkričio 14 d. reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų⁴⁷ ir kt. Pastebėtina, kad duomenų valdymas darys reikšmingą įtaką ir medicinos sektoriui. 2025 m. buvo priimtas 2025 m. vasario 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/327, dėl Europos bendros sveikatos duomenų erdvės, kuriuo iš dalies keičiama Direktyva 2011/24/ES ir Reglamentas (ES) 2024/2847 (toliau - ESDE), kurio tikslas yra sukurti bendrą sveikatos duomenų naudojimo ir keitimosi sistemą visoje ES, kartu užtikrinant jų saugumą ir kontrolę⁴⁸. Šis reglamentas suteiks daugiau galimybių naudotis duomenimis tiek pacientams, tiek medikams, be to, jis sudarys sąlygas juos pakartotinai naudoti mokslinių tyrimų ir viešojo intereso tikslais. Šiuo metu prasidėjo pereinamasis laikotarpis, todėl ESDE dar nėra taikomas ir bus įgyvendinamas palaipsniui⁴⁹. Visi šie minėti teisės aktai bei kitos susijusios iniciatyvos, buvo priimti kaip ES duomenų strategijos dalis, siekiant įgyvendinti ES skaitmeninį suverenitetą.

Reguliuojant infrastruktūrą ir strateginės reikšmės technologijas, pavyzdžiui, puslaidininkių gamybą, ryšių, komunikacijų, debesijos sistemų plėtrą ir kt., buvo priimti tokie teisės aktai, kaip, pavyzdžiui, Europos Parlamento ir Tarybos 2023 m. rugsėjo 13 d. reglamentas (ES) 2023/1781, kuriuo nustatoma Europos puslaidininkių ekosistemos

⁴⁵ Europos Parlamento ir Tarybos 2022 m. gegužės 30 d. reglamentas (ES) 2022/868 dėl Europos duomenų valdymo, kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1724 (Duomenų valdymo aktas). OL L 152/1, 2022, p. 1-44.

⁴⁶ Europos Parlamento ir Tarybos 2023 m. gruodžio 13 d. reglamentas (ES) 2023/2854 dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/2394 ir Direktyva (ES) 2020/1828 (Duomenų aktas). OL L 2023/2854, 2023.

⁴⁷ Europos Parlamento ir Tarybos 2018 m. lapkričio 14 d. reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų. OL L 303/59, 2018, p. 59–68.

⁴⁸ Europos Parlamento ir Tarybos 2025 m. vasario 11 d. reglamentas (ES) 2025/327, dėl Europos bendros sveikatos duomenų erdvės, kuriuo iš dalies keičiama Direktyva 2011/24/ES ir Reglamentas (ES) 2024/2847. OL L 2025/327, 2025.

⁴⁹ Europos Komisija (n.d.). *Europos sveikatos duomenų erdvės (ESDE) reglamentas* [interaktyvus]. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_lt.

stiprinimo priemonių sistema ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Lustų aktas)⁵⁰ ir Europos Parlamento ir Tarybos 2023 m. kovo 15 d. reglamentas (ES) 2023/588, kuriuo nustatoma 2023–2027 m. Sąjungos saugaus junglumo programa⁵¹.

Kibernetinio saugumo srityje kaip svarbiausią galima išskirti Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. direktyvą (ES) 2022/2555, dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva), kuri yra jau perkelta į Lietuvos nacionalinę teisę ir ja siekiama užtikrinti kibernetinį saugumą 18-oje ypatingos svarbos sektorių visoje ES⁵².

Reguliuojant platformas ir skaitmeninę rinką, esminę reikšmę turi šiame darbe jau minėti Skaitmeninių paslaugų aktas bei Skaitmeninių rinkų aktas. Naujų technologijų reguliavimo srityje, iš esmės kalbant apie sparčiai besivystančias dirbtinio intelekto technologijas, galima išskirti 2024 m. priimtą Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas, (EU) (2024/1689, 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)⁵³ (toliau - DI aktas), kuris yra pirmasis tokio pobūdžio teisės aktas, reglamentuojantis dirbtinio intelekto technologijų naudojimą.

Taigi, galima daryti išvadą, kad pastaraisiais metais ES atliko plataus masto, sistemiską darbą, kurdama skaitmeninį suverenitetą, kuris ir toliau aktyviai plėtojamas. Atsižvelgiant į tai, toliau darbe bus nagrinėjami ne visi priimti teisės aktai, o tik tie, kurie tiesiogiai ar netiesiogiai daro esminį poveikį žmogaus teisėms.

⁵⁰ Europos Parlamento ir Tarybos 2023 m. rugsėjo 13 d. reglamentas (ES) 2023/1781, kuriuo nustatoma Europos puslaidininkių ekosistemos stiprinimo priemonių sistema ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Lustų aktas). OJ L 229/1, 2023, p. 1-53.

⁵¹ Europos Parlamento ir Tarybos 2023 m. kovo 15 d. reglamentas (ES) 2023/588, kuriuo nustatoma 2023–2027 m. Sąjungos saugaus junglumo programa. OL L 79/1, 2023, p. 1-39.

⁵² Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. direktyva (ES) 2022/2555, dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva). OL L 333/80, 2022, p. 80-152.

⁵³ Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas, (EU) (2024/1689, 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). OL L, 2024/1689, 2024.

2. SKAITMENINIO SUVERENITETO POTENCIALAS STIPRINANT ŽMOGAUS TEISIŲ APSAUGĄ TARPTAUTINĖS IR ES TEISĖS KONTEKSTE

2.1. Tarptautinių žmogaus teisių normų taikymas skaitmeninėje erdvėje

Analizuojant žmogaus teisių užtikrinimą skaitmeninėje erdvėje tikslinga apžvelgti tarptautinį kontekstą. Esminis dokumentas, kuris tarptautiniu lygiu įtvirtina, kad būtina ginti žmogaus teises, yra 1948 m. Jungtinių Tautų Visuotinė žmogaus teisių deklaracija (toliau – Deklaracija). Šiame dokumente įtvirtinta daugybė fundamentalių žmogaus teisių ir laisvių, tačiau nagrinėjamos temos kontekste pagrindinis dėmesys turėtų būti skirtas Deklaracijos 12 straipsnyje nurodytai teisei į privatumą ir 19 straipsnyje įtvirtintai teisei į žodžio laisvę⁵⁴. Nors Deklaracija yra rekomendacinio pobūdžio, ji tapo moraliniu pagrindu ir nustatė bendrus standartus, kurie vėliau buvo įtvirtinti kituose teisiniuose aktuose. Pavyzdžiui, jau 1966 m. Tarptautinio pilietinių ir politinių teisių pakto (toliau – Paktas) 17 straipsnyje galime įtvirtinta teisę į privatumą, kuri apima ir susirašinėjimo slaptumą bei draudžia savavališkai ir neteisėtai kištis į asmeninį gyvenimą. Tuo tarpu Pakto 19 straipsnyje nurodyta saviraiškos laisvė, kuri apima galimybę nekliudomai ieškoti, gauti ir perteikti bet kokią informaciją bei idėjas, nepaisant valstybių sienų, tiek žodžiu, tiek raštu ar bet kokiomis kitomis priemonėmis⁵⁵.

Pažymėtina, kad šiuolaikinė tarptautinė teisė nurodo, jog žmogaus teisių galiojimas nepriklauso nuo susisiekimo kanalų. Šios teisės garantuojamos ir saugomos ir skaitmeninėje erdvėje, remiantis aplinkos tęstinumo principu. 2014 m. JT Žmogaus teisių taryba pabrėžė kad, tos pačios teisės, kurias asmuo turi neprisijungęs prie interneto, privalo būti užtikrinamos ir internetinėje erdvėje, kartu ragindama valstybes garantuoti konfidencialumą bei saviraiškos laisvę skaitmeninėje aplinkoje⁵⁶. JT taip pat išreiškia susirūpinimą dėl naujų skaitmeninių technologijų plėtros, galinčios neigiamai paveikti žmogaus teises, ir nurodo, kad jų naudojimui gali trūkti tinkamų reguliavimo bei valdymo mechanizmų, todėl valstybės skatinamos kurti naujas veiksmingas priemones, siekiant užkirsti kelią galimam neigiamam tokių technologijų poveikiui arba jį sušvelninti⁵⁷.

⁵⁴ Visuotinė žmogaus teisių deklaracija (1948). *Valstybės žinios*, 2006-06-17, 68-2497.

⁵⁵ Tarptautinis pilietinių ir politinių teisių paktas (1966). *Valstybės žinios*, 2002-08-02, Nr. 77-3288.

⁵⁶ United Nations (2015-02-16). *Resolution adopted by the General Assembly on 18 December 2014. 69/166. The right to privacy in the digital age* [interaktyvus]. <https://docs.un.org/en/A/RES/80/215>.

⁵⁷ United Nations (2025-12-22). *Resolution adopted by the General Assembly on 18 December 2025. 80/215. Promotion and protection of human rights in the context of digital technologies* [interaktyvus]. <https://docs.un.org/en/A/RES/80/215>.

Tad galima teigti, kad šiuolaikinė tarptautinė teisė jau suformavo tvirtą pagrindą žmogaus teisių apsaugai skaitmeninėje erdvėje, tačiau esamos normos yra bendro pobūdžio, todėl jas būtina adaptuoti. Atsižvelgiant į kylančius technologinius iššūkius, jas reikia toliau plėtoti ir konkretizuoti, taip siekiant užtikrinti ne tik formalų teisių deklaravimą skaitmeninėje erdvėje, bet ir realią, efektyvią žmogaus teisių bei laisvių apsaugą.

Europos lygiu vienas iš pagrindinių šaltinių žmogaus teisių apsaugos klausimais yra 1950 m. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (toliau - EŽTK). Šio dokumento 8 straipsnis nurodo, kad kiekvienas turi teisę į tai, kad būtų gerbiama jo privatus ir šeimos gyvenimas ir susirašinėjimo slaptumas⁵⁸. EŽTK 10 straipsnis užtikrina saviraiškos laisvę. Plėtojantis technologijoms, abi šios teisės taikomos ir interneto komunikacijoms. Svarbu pažymėti, kad, nors abi šios teisės yra besąlygiškai garantuojamos, jos visgi gali būti ribojamos, tačiau tokie apribojimai turi būti numatyti teisės aktuose ir atitikti EŽTK nurodytus pagrindus. EŽTK 8 straipsnio 2 dalyje nurodyti šeši pagrindai, kai galima riboti asmens privatumo teisę: „<...> kai tai būtina demokratinėje visuomenėje (1) valstybės saugumo, (2) visuomenės apsaugos ar (3) šalies ekonominės gerovės interesams, (4) siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, (5) taip pat būtina žmonių sveikatai ar moralei arba (6) kitų asmenų teisėms ir laisvėms apsaugoti“. EŽTK 10 straipsnio 2 dalyje nurodyti saviraiškos laisvės ribojimo pagrindai iš dalies sutampa su minėtaisiais: pirmi trys pagrindai skiriasi tuo, kad vietoje ekonomines geroves interesu yra numatytas teritorinio vientisumo pagrindas, ketvirtasis ir penktas pagrindas išlieka nepakeistas, o šeštajame pagrinde žodis „laisvė“ keičiamas į „asmens garbę“. Be to numatyti dar du papildomi specifiniai pagrindai: „<...> (7) užkirsti kelią įslaptintos informacijos atskleidimui arba (8) užtikrinti teisminės valdžios autoritetą ir nešališkumą“. Matytina, kad EŽTK nurodyti įvairūs teisių apribojimo pagrindai. Juos svarbu identifikuoti, nes pagal nusistovėjusią Europos Žmogaus Teisių Teismo (toliau – EŽTK) ir Europos Sąjungos Teisingumo Teismo (toliau – ESTT) praktiką, vertinant teisių apribojimų teisėtumą, būtina įvertinti jų proporcingumą ir būtinumą siekiant nustatytų tikslų. Pažymėtina, kad ESTT praktikoje taip pat svarstomas taikomo apribojimo tinkamumas.

2000 m. ES lygmeniu buvo priimta Europos Sąjungos pagrindinių teisių chartija (toliau – Chartija), kuri gina ES piliečių pagrindines teises⁵⁹. Šio dokumento svarba ES teisei pagrįsta ir tuo, kad Europos Sąjungos sutarties (toliau – ES sutartis) 6 straipsnio 1 dalyje

⁵⁸ Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija iš dalies pakeista protokolu Nr. 15 (konsoliduotas tekstas) (1950). TAR, 2022, 2432.

⁵⁹ Europos Sąjungos pagrindinių teisių chartija. OL C 202, 2016, p. 389–405.

skelbiama, jog Chartija turi tokią pat teisinę galią, kaip ir Sutartys, t. y. laikoma pirmine ES teise⁶⁰. Skirtingai nei EŽTK, joje įtvirtinamos ne tik pilietinės bei politinės teisės, bet ir nustatomos kitos naujos teisės. Tačiau Chartija jokiais aplinkybėmis nepakeičia ir neapriboja kitų pagrindinių teisių šaltinių, galiojančių tarptautiniu, Europos ar nacionaliniu lygmeniu. Chartijos 53 straipsnis nurodo, kad jokia šios Chartijos nuostata negali būti aiškinama kaip ribojanti ar kitaip varžanti žmogaus teises ir pagrindines laisves, kurias atitinkamoje taikymo srityje pripažįsta Sąjungos teisė ir tarptautinė teisė bei tarptautiniai susitarimai, kurių šalys yra Sąjunga arba visos valstybės narės, įskaitant EŽTK, taip pat valstybių narių konstitucijos. Pastebėtina, kad Chartija sistemingai aiškinama kartu su EŽTK bei ESTT ir EŽTT praktika. Nors Chartija gali suteikti platesnę apsaugą nei EŽTK, jos 52 straipsnio 3 dalyje nurodyta, kad tais atvejais, kai Chartija numato teises, atitinkančias teises, garantuojamas EŽTK, tai šių teisių esmė ir taikymo sritis sutampa su tomis, kurias joms suteikia EŽTK. Tačiau ši nuostata nekliudo Chartijai ar kitiems ES teisės šaltiniams numatyti didesnę apsaugą. Chartija, kaip ir EŽTK, įtvirtina teisę į privatą ir šeimos gyvenimą (Chartijos 7 straipsnis) bei saviraiškos ir informacijos laisvę (Chartijos 11 straipsnis). Pastebėtina, kad skirtingai nei EŽTK, Chartijoje saviraiškos ir informacijos laisvė papildoma reikalavimu gerbti žiniasklaidos laisvę ir pliuralizmą (Chartijos 11 straipsnio 2 dalis).

Aktuali ir Chartijos 8 straipsnyje įtvirtinta teisė į asmens duomenų apsaugą, kuri numato, kad duomenys turi būti tvarkomi sąžiningai, konkrečiais tikslais ir remiantis asmens sutikimu arba kitu teisėtu pagrindu. Šios teisės įgyvendinimą užtikrina BDAR, kurio išsamesnė analizė bus pateikta 2.2 poskyryje. Jis konkretizuoja Chartijoje įtvirtintą asmens duomenų apsaugos teisę, nustatydamas išsamius duomenų subjektų teises, duomenų tvarkymo principus ir priežiūros mechanizmus, taip paverčiant šią pagrindinę teisę realiai veikiančia.

Greta standartinės normų analizės, verta pažymėtina, kad ir pati teisė laisvai naudotis internetu įgyja prigimtinės žmogaus teisės statusą ir tampa lygiavertė kitoms tradiciškai įtvirtintoms teisėms. 2007 m. Europos Tarybos Ministrų Komitetas priėmė Rekomendaciją „Dėl priemonių, skirtų skatinti interneto, kaip viešosios paslaugos, vertę“, kurioje pabrėžiama, kad prieiga prie interneto bei gebėjimas ir galimybė juo naudotis turi būti laikomi būtinomis sąlygomis, siekiant informacinėje visuomenėje visapusiškai įgyvendinti bei užtikrinti žmogaus teises ir pagrindines laisves. Be to, šioje rekomendacijoje įtvirtintas draudimas nutraukti vartotojo prieigą prie interneto (išskyrus atvejus, kai yra teismo

⁶⁰ Europos Sąjungos sutarties suvestinė redakcija. OL C 202, 2016, p. 13–46.

sprendimas arba tai numatyta įstatyme), taip pat draudimas diskriminuoti dėl bet kokių požymių. Kartu pabrėžiama būtinybė užtikrinti interneto prieinamumą nepriklausomai nuo vartotojo gyvenamosios vietos ar pajamų lygio⁶¹. Akivaizdu, kad ši teisė į prieigą prie interneto yra glaudžiausiai susijusi su laisve gauti ir skleisti informaciją, kas garantuota EŽTK 10 straipsniu.

Požiūris į teisę naudotis internetu kaip į vieną iš prigimtinių žmogaus teisių pastebimas ir EŽTT praktikoje. Pavyzdžiui, EŽTT byloje *Ahmet Yildirim prieš Turkiją* teismas nurodė, kad prieigos prie interneto apribojimas sukelia reikšmingas pasekmes, nes internetas tapo viena pagrindinių priemonių asmenims įgyvendinti savo teisę į saviraiškos ir informacijos laisvę, kadangi jis suteikia būtinas sąlygas dalyvauti diskusijose bei veikloje, susijusioje su politinėmis aktualijomis ir visuomenės interesais⁶². Taigi, teismas šioje byloje teisę naudotis internetu priskyrė saviraiškos laisvei, kuri garantuojama EŽTK 10 straipsnyje. Byloje *Delfi AS prieš Estiją* EŽTT nusprendė, kad valstybė gali riboti žodžio laisvę, jei tai yra teisėta ir proporcinga. Ši byla įdomi ir tuo, kad joje buvo įtvirtinta taisyklė, jog interneto platformos privalo filtruoti komentarus ir įrašus, kurie skelbiami jų portaluose ir kursto neapykantą⁶³. Šis sprendimas buvo ginčytinas ir turėjo didelę įtaką priimant DSA, nes dabar jame tiksliai nurodyta, kad interneto platformos neatsako už neteisėtą vartotojų turinį, jei jos nežino apie jo neteisėtumą. Tačiau vos gavusios tokią informaciją (pavyzdžiui, per skundą), jos privalo nedelsdamos pašalinti tokį turinį arba apriboti prieigą prie jo (DSA 6 straipsnis). Byloje *Taganrog LRO ir kiti prieš Rusiją* EŽTT nurodė, kad priemonės, ribojančios veiklą internete (pavyzdžiui, svetainių turinio pašalinimas ar jų blokavimas), turi būti ne tik proporcingos, bet ir užtikrinamos pakankamomis procesinėmis garantijomis. Tuo tarpu Rusijos teisinė sistema tokių saugiklių neužtikrino: svetainių savininkai nedalyvavo blokavimo procedūroje, neturėjo galimybės iš anksto pašalinti pažeidimų, o valstybės institucijos neįvertino priemonių proporcingumo bei galimų pasekmių. Tai lėmė pernelyg didelius apribojimus bei pažeidė EŽTK 10 straipsnį⁶⁴. Analizuojant EŽTT argumentaciją, matyti, kad ribojant teisę į saviraiškos laisvę, reikia taikyti trijų etapų testą. Pirma, bet koks apribojimas turi būti nustatytas įstatymu, kuris privalo būti viešai paskelbtas ir suformuluotas pakankamai aiškiai, kad asmuo galėtų juo vadovautis. Antra,

⁶¹ Council of Europe (2007-11-07). *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet (Adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies)* [interactyvus]. <https://search.coe.int/cm?i=09000016805d4a39>.

⁶² *Ahmet Yildirim prieš Turkiją* [EŽTT], Nr. 3111/10, [2012-12-18]. ECLI:CE:ECHR:2012:1218JUD000311110.

⁶³ *Delfi AS prieš Estiją* [EŽTT], Nr. 64569/09, [2015-06-16]. ECLI:CE:ECHR:2015:0616JUD006456909.

⁶⁴ *Taganrog LRO ir kiti prieš Rusiją* [EŽTT], Nr. 32401/10 [2022-09-07]. ECLI:CE:ECHR:2022:0607JUD003240110.

apribojimu privaloma siekti teisėto tikslo, nurodyto EŽTK (pavyzdžiui, EŽTK 10 straipsnio 2 dalyje išvardytų septynių tikslų). Tik šie pagrindai laikomi pagrįstomis saviraiškos laisvės ribojimo priežastimis. Trečia, apribojimas būtinas demokratinėje visuomenėje, t. y. proporcingas siekiamam teisėtam tikslui. Jei prieiga prie tam tikros informacijos ribojama, turi būti įrodyta, kad tokios informacijos skleidimas neabejotinai pakenktų teisėtam tikslui, nustatytam EŽTK 10 straipsnyje. Apibendrinant, EŽTT pozicija rodo, kad palaipsniui pripažįstamas ypatingas interneto vaidmuo, jis tampa pagrindine erdve, kurioje įgyvendinama saviraiškos laisvė. EŽTT siekia išlaikyti pusiausvyrą, kad ribojimai skaitmeninėje erdvėje netaptų neproporcingos kontrolės priemone. Šiame kontekste itin svarbus ne tik ribojimų proporcingumas, bet ir efektyvios procesinės priemonės, kurios galėtų užkirsti kelią savavališkam prieigos prie informacijos ribojimui.

ES lygmeniu taip pat vyksta diskusijos dėl skaitmeninio turinio ribojimų. Europos Komisija 2021 m. metinėje ataskaitoje dėl ES pagrindinių teisių chartijos taikymo nurodė, kad valstybė privalo ne tik susilaikyti nuo nepagrįstų ribojimų taikymo, bet ir priimti pozityvią pareigą sudaryti palankią aplinką įtraukiančioms bei pliuralistinėms viešosioms diskusijoms (ypač rinkimų laikotarpiu) bei užtikrinti veiksmingą žiniasklaidos laisvės įgyvendinimą. Pabrėžiama, kad tokios priemonės peržengia vien tik turinio moderavimo ribas ir apima platesnius veiksmus švietimo bei visuomenės informavimo srityse⁶⁵.

Nors ES nėra prisijungusi prie EŽTK, nagrinėdamas ginčus, susijusius su informacijos skelbimu internete, ESTT aktyviai remiasi EŽTK praktika, ją taikydamas Pagrindinių teisių chartijoje įtvirtintoms teisėms aiškinimui. Sujungtoje byloje *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* ESTT nagrinėjo klausimą dėl žemės ūkio subsidijų gavėjų duomenų skelbimo internete ir priėjo prie išvados, kad toks skelbimas pažeidžia Chartijos 7 ir 8 straipsniuose įtvirtintas teises į privataus gyvenimo gerbimą bei asmens duomenų apsaugą⁶⁶. Tuo pačiu ESTT rėmėsi EŽTT praktika, ypač bylomis *Amann prieš Šveicariją*⁶⁷ ir *Rotaru prieš Rumuniją*⁶⁸, kuriose ESTT pabrėžė, kad privatumo sąvoka turi būti aiškinama plačiai: ji apima bet kokią informaciją, susijusią su identifikuotu ar identifikuojamu asmeniu. Be to, vertindamas kišimosi proporcingumą, ESTT rėmėsi EŽTT artimu požiūriu, ir konstatavo, kad ES teisės aktų leidėjas neužtikrino tinkamos interesų

⁶⁵ Europos Komisija (2021-12-10). *Komisijos ataskaita Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Pagrindinių teisių apsauga skaitmeniniame amžiuje, 2021 m. metinė ES pagrindinių teisių chartijos taikymo ataskaita, COM(2021) 819 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52021DC0819>.

⁶⁶ *Volker und Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen* [ESTT], Nr. C-92/09 ir C-93/09, [2010-11-09]. ECLI:EU:C:2010:662.

⁶⁷ *Amann prieš Šveicariją* [EŽTT], Nr. 27798/95, [2000-02-16]. ECLI:CE:ECHR:2000:0216JUD002779895.

⁶⁸ *Rotaru prieš Rumuniją* [EŽTT], Nr. 28341/95, [2000-05-04]. ECLI:CE:ECHR:2000:0504JUD002834195.

nepakanka, nes kol kas nėra vieno bendro kodifikuoto teisės akto, kuris, panašiai kaip EŽTK ar Chartija, įtvirtintų visuotines skaitmenines teises. Šiuo metu šios teisės dar tik formuojasi ir yra fragmentiškai išsibarsčiusios skirtinguose teisės aktuose bei teismų praktikoje. Todėl darytina išvada, kad ateityje yra būtina įtvirtinti skaitmenines teises tarptautiniu lygmeniu, pavyzdžiui, tarptautinės sutarties forma.

Toks normų kodifikavimas būtų tikslingas dėl kelių priežasčių. Pirmą, dėl skaitmeninių teisių fragmentiško išsidėstymo skirtinguose teisės aktuose ir teismų praktikoje jų turinys nėra pakankamai aiškus ir gali būti taikomas nevienodai. Vieningas kodifikuotas tarptautinis dokumentas užtikrintų nuoseklumą, teisinį aiškumą ir vienodą standartų taikymą. Antra, skaitmeninė erdvė iš esmės yra tarptautinė, todėl nacionalinis ar net regioninis reguliavimas (pavyzdžiui, ES lygmeniu) ne visada yra pakankamas. Tarptautinis susitarimas leistų nustatyti bendrus minimalius standartus ir užtikrinti platesnę žmogaus teisių apsaugą tarptautiniu mastu. Trečia, toks dokumentas sustiprintų žmogaus teisių apsaugą, aiškiai apibrėždamas skaitmenines teises, o tai leistų orientuoti technologijų plėtrą į žmogaus teises. Paola Coletti, Sesilia Ducci ir Francesco Nikolo Moro moksliniame tyrime nurodo, kad ES, siekdama užimti pirmaujančias pozicijas skaitmeninės erdvės reglamentavime, turėtų bendradarbiauti su valstybėmis, kurios laikosi tų pačių fundamentalų vertybių⁷³. Tiina Pajuste taip pat pabrėžia skaitmeninio bendradarbiavimo svarbą. Ji pažymi, kad skaitmeninis suverenitetas daro įtaką interneto veikimui visame pasaulyje, todėl svarbu, kad valstybės bendradarbiautų, siekdamos parengti bendras normas ir standartus, kurie gerbtų žmogaus teises ir kartu atsižvelgtų į saugumo aspektus. Pabrėžiama, kad bendros pastangos gali padėti užkirsti kelią interneto reguliavimo fragmentacijai ir skatinti visuotinį požiūrį į interneto valdymą⁷⁴. Taigi manytina, kad kodifikuoto tarptautinio dokumento inicijavimas taptų šio bendradarbiavimo išraiška.

2.2. Privatumo ir asmens duomenų apsaugos stiprinimas kaip skaitmeninio suvereniteto tikslas

⁷³ COLETTI, Paola, DUCCI, Cecilia ir MORO, Francesco Niccolo (2025). Digital Sovereignty and the EU's Identity between Technological Innovation and European Values. *JCMS: Journal of Common Market Studies*, p. 1-19 [interaktyvus]. <https://doi.org/10.1111/jcms.70074>. p. 12.

⁷⁴ PAJUSTE, Tiina (2025). Digital Sovereignty and Human Rights: Balancing Security and Freedom. *Working paper: Technological change and international law: ESIL annual conference, Vilnius, 5-6 September 2024*, p. 78-84 [interaktyvus]. https://www.researchgate.net/publication/396975294_Digital_Sovereignty_and_Human_Rights_Balancing_Security_and_Freedom. p. 83.

Asmens duomenų apsaugos užtikrinimas išlieka viena sudėtingiausių ir aktualiausių problemų šiuolaikinėje ES skaitmeninėje darbotvarkėje. Ursula von der Leyen pabrėžia, kad norint visapusiškai išnaudoti skaitmeninių technologijų potencialą ES, būtinas specifinis modelis, grindžiamas laisvu duomenų judėjimu ir aktyviu jų naudojimu, kuris kartu užtikrintų aukštus privatumo bei saugumo standartus ir pagrindines europietiškas vertybes⁷⁵. Šiame kontekste ji akcentuoja BDAR sėkmę ir nurodo, kad minėta pusiausvyra buvo sėkmingai įgyvendinta būtent šiame reglamente, tapusiame veiksmingo reguliavimo pavyzdžiu bei gairėmis daugeliui pasaulio valstybių⁷⁶.

Tačiau ES valstybės narės vis dar išreiškia susirūpinimą dėl nepakankamos ES generuojamų duomenų kontrolės. Pagrindinė tuo priežastis – duomenų saugojimas JAV jurisdikcijoje, ypač naudojantis užsienio bendrovių teikiamomis debesijos ir kitomis duomenų tvarkymo paslaugomis⁷⁷. Pastebima tendencija, kad ES pralaimi konkurencinę kovą debesijos paslaugų srityje, nes šioje rinkoje dominuoja JAV ir Azijos bendrovės. Šios rinkos lyderės yra minėtose šalyse įsikūrusios įmonės, remiantis 2025 m. statistiniais duomenimis, tai: „Amazon“ (37,7 %), „Microsoft“ (23,9 %), „Google“ (9,0 %), „Alibaba Group“ (7,2 %) ir „Huawei“ (4,1 %)⁷⁸. Stebina ir kolosalūs duomenų saugojimo kiekio skirtumai kitose jurisdikcijose. Pavyzdžiui, pagal 2019 m. vertinimus, apie 92 % Vakarų pasaulyje sukurtų duomenų šiuo metu saugomi JAV, ir tik 4 % – Europoje⁷⁹.

Tad siekdama ilgalaikio šių problemų sprendimo, ES įgyvendina keletą iniciatyvų pagal vadinamąją „Europos duomenų strategiją“⁸⁰. Šios strategijos pagrindinis uždavinys yra užtikrinti laisvą duomenų judėjimą tarp ES valstybių narių, kartu griežtai taikant europinius standartus, ypač konfidencialumo, duomenų apsaugos bei prieigos prie jų ir naudojimo srityse. Šios strategijos tekste pabrėžiama, kad ES siekia: (1) sukurti skaidrias taisykles, reglamentuojančias prieigą prie duomenų ir jų pakartotinį naudojimą; (2)

⁷⁵ European Commission (n.d.). *Political Guidelines. Ursula von der Leye. Candidate for the European Commission President* [interaktyvus]. https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf.

⁷⁶ *Ibid.*

⁷⁷ LEDWON, Benjamin ir DAVID, Torben (2019-11-15). *A sovereign cloud and data infrastructure for Germany and Europe* [interaktyvus]. https://www.bitkom.org/sites/default/files/2019-11/20191115_key-points-for-a-sovereign-cloud-infrastructure-in-germany-and-_.pdf.

⁷⁸ Gartner (2025-08-06). *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5% in 2024* [interaktyvus]. <https://www.gartner.com/en/newsroom/press-releases/2025-08-06-gartner-says-worldwide-iaas-public-cloud-services-market-grew-22-point-5-percent-in-2024>.

⁷⁹ KALFF, Donald ir RENDA, Andrea (2019). *Hidden Treasures. Mapping Europe's sources of competitive advantage in doing business* [interaktyvus]. Brussels: Centre for European Policy Studies (CEPS). <https://www.sipotra.it/wp-content/uploads/2019/09/Hidden-Treasures.-Mapping-Europe's-sources-of-competitive-advantage-in-doing-business.pdf>. p. 173.

⁸⁰ Europos Komisija (2020-02-19). *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Europos duomenų strategija, COM(2020) 66 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52020DC0066>.

investuoti į duomenų saugojimo bei tvarkymo priemonių ir infrastruktūros plėtrą, įskaitant pastangų koordinavimą plėtojant Europos debesijos technologijas; (3) skatinti bendrą Europos duomenų erdvių kūrimą strateginiuose sektoriuose; bei (4) užtikrinti vartotojams teises, priemones ir žinias, būtinas duomenų kontrolei⁸¹. Strategija orientuota į bendros ES duomenų erdvės sukūrimą, sujungiant į vieningą informacinę sistemą devynis strateginius sektorius: sveikatos priežiūrą, žemės ūkį, pramonę, energetiką, finansus, viešąjį administravimą, aplinkos apsaugą, susisiekimą ir darbo rinką.

Esminiai šios strategijos principai vėliau buvo teisiškai įtvirtinti dviejuose ES reglamentuose: Duomenų valdymo akte ir Duomenų akte. Abu dokumentai yra glaudžiai susiję ir kartu su BDAR bei kitais teisės aktais sudaro bendrą ES duomenų apyvartos reguliavimo sistemą.

Duomenų valdymo aktas – tai ES reglamentas, kuris skirtas duomenų mainų organizavimui ir reguliavimui. Jis nereguliuoja pačių duomenų kaip apsaugos objekto. Pagal Duomenų valdymo akto 1 straipsnį šis dokumentas reguliuoja 4 aspektus: (1) pakartotinį naudojimą tam tikrų kategorijų duomenų, esančių viešojo sektoriaus įstaigų žinioje (t. y. valstybinėse duomenų bazėse); (2) pranešimo ir priežiūros sistemą, skirtą duomenų tarpininkavimo paslaugų teikimui; (3) registravimą organizacijų, kurios renka ir tvarko duomenis, teikiamus visuomenės interesų labui (t. y. altruistiniais tikslais); ir (4) Europos duomenų inovacijų valdybos įsteigimą. Svarbiausias šio akto uždavinys yra sumažinti priklausomybę strategiškai svarbiose ekonomikos srityse nuo didžiųjų skaitmeninių platformų, kurios kaupia ir kontroliuoja milžiniškus duomenų kiekius. Šiuo tikslu Duomenų valdymo aktas numato neutralių duomenų tarpininkų sukūrimą, kurie nenaudotų duomenų savo interesams, o tik užtikrintų jų perdavimą tarp turėtojų ir naudotojų (Duomenų valdymo akto 12 straipsnis). Taigi, pagrindinė šio akto idėja yra padaryti duomenis prieinamus ir naudojamus, tačiau kartu užtikrinti jų kontrolę bei saugumą. Pažymėtina, kad nors Duomenų valdymo aktas nėra teisės aktas, tiesiogiai skirtas žmogaus teisių apsaugai, jis atlieka svarbų vaidmenį užtikrinant jų netiesioginę apsaugą. Sukūrus sistemingą ir skaidrią duomenų mainų sistemą, sumažėja ES priklausomybė nuo didžiųjų skaitmeninių platformų, o tai padeda užtikrinti tinkamesnį duomenų kontrolės paskirstymą, mažina jų koncentraciją atskirų įmonių žinioje ir kartu prisideda prie teisės į privatumą apsaugos.

⁸¹ Europos Komisija (2025-11-19). *Europos duomenų strategija* [interaktyvus]. <https://digital-strategy.ec.europa.eu/lt/policies/strategy-data>.

Tuo tarpu, minėtas Duomenų aktas – tai ES reglamentas, kuriuo siekiama stiprinti duomenų ekonomiką, aiškiai apibrėžiant, kas, kokius duomenis ir kokiomis sąlygomis gali naudoti. Tai itin svarbu kalbant apie prie interneto prijungtus įrenginius. Įstatymas suteikia vartotojams teisę susipažinti su jų generuojamais duomenimis, juos naudoti ir perduoti tretiesiems asmenims, tuo pačiu nustatydamas duomenų turėtojams (t. y. įmonei, gaminančiai įrenginį) pareigą užtikrinti tokią prieigą (Duomenų akto II skyrius).

Komisijos 2022 m. pranešime spaudai apie Duomenų aktą, Thierris Bretonas nurodė, kad Duomenų aktas yra svarbus žingsnis siekiant dalytis Europoje sukauptais pramonės duomenimis. Tai, anot jo, yra naudinga įmonėms, vartotojams, viešosioms tarnyboms ir visai visuomenei. Pranešime akcentuojama, kad Duomenų aktas užtikrina pramonės duomenų dalijimąsi, kuriame duomenys yra saugomi ir tvarkomi laikantis Europos taisyklių. Pabrėžiama, kad Duomenų aktas yra tvirtos, novatoriškos ir suverenios Europos skaitmeninės ekonomikos kertinis akmuo⁸².

Kalbant apie debesijos technologijų srities plėtros galimybes, verta paminėti iniciatyvą „Gaia-X“, kuri yra viena ambicingiausių šioje srityje⁸³. Pagrindinis „Gaia-X“ tikslas yra sukurti universalias duomenų erdves, skirtas verslo informacijos mainams tarp vartotojų⁸⁴. Tokios erdvės turėtų užtikrinti: (1) vieningą duomenų mainų pagrindą, apimančią standartizuotus informacijos paieškos, prieigos ir naudojimo mechanizmus bei (2) suderinamumą tarp įvairių debesų technologijų ir jų teikėjų. Taip naudotojai galėtų gauti prieigą prie reikiamų duomenų be būtinybės pereiti iš vienos debesijų platformos į kitą. Visa tai atspindi pagrindinį pagrindinį „Gaia-X“ tikslą – užtikrinti aukštą suderinamumo lygį, kuris išplečia duomenų perkėlimo tarp skirtingų debesijos sprendimų galimybes.

Nors Duomenų valdymo aktas, Duomenų aktas ir „Gaia-X“ iniciatyva didžiąja dalimi yra skirti duomenų mainų sistemos plėtrai bei patikimos duomenų naudojimo aplinkos kūrimui, jų negalima laikyti priemonėmis, skirtomis išimtinai valstybės institucijoms. Šie sprendimai formuoja kompleksinį Europos duomenų valdymo modelį, orientuotą į viešojo bei privačiojo sektorių sąveiką ir pačių duomenų subjektų dalyvavimą. Esminė jų reikšmė yra įtvirtinti reikalavimus dėl skaidrumo, kontrolės, sąveikumo bei saugios prieigos prie duomenų. Todėl, net jei atskirų mechanizmų tiesioginiai adresatai yra valstybės struktūros ar verslas, galutinis reguliavimo poveikis pasireiškia plačiau: mažinama neteisėtos prieigos

⁸² Europos Komisija (2022-02-23). *Duomenų aktas. Komisija siūlo teisingos ir novatoriškos duomenų ekonomikos priemonės* [interaktyvus]. https://ec.europa.eu/commission/presscorner/detail/lt/ip_22_1113.

⁸³ Gaia-X (n.d.). About Gaia-X [interaktyvus]. <https://gaia-x.eu/about/>.

⁸⁴ AUTOLITANO, Simona ir PAWLOWSKA, Agnieszka (2021). Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study. IAI Papers, 21(14), 1-23 [interaktyvus]. <https://www.iai.it/sites/default/files/iaip2114.pdf>, p. 13.

rizika, didinamas tarpininkų atskaitingumas, užtikrinimas BDAR taisyklių taikymo taikymas bei plėtojama patikima skaitmeninė aplinka. Visa tai netiesiogiai stiprina ir fizinių asmenų duomenų apsaugą.

Teisė į asmens duomenų apsaugą ES teisėje įtvirtinta keliais lygmenimis. Pirminės ES teisės lygmeniu ji tiesiogiai nurodyta SESV 16 straipsnyje ir Chartijos 8 straipsnyje. SESV ši teisė turi funkcinį pobūdį, nes ji yra įtvirtinta kaip bendroji nuostata, kuria, kaip matyti iš šio straipsnio 2 dalies, siekiama sukurti teisinį pagrindą tolesnei ES reguliavimo veiklai duomenų tvarkymo srityje. Chartijoje ši teisė jau įgyja fundamentinį pobūdį, nes ji suformuluota kaip pagrindinė asmens teisė, turinti konkretų turinį bei apsaugos mechanizmus. Chartijos 8 straipsnio 2 dalyje nustatyta, kad asmens duomenys privalo būti tinkamai tvarkomi, tik konkrečioms tikslams ir remiantis asmens sutikimu arba jei tai leidžia įstatymas. Taip pat įtvirtinta asmens teisė susipažinti su surinktais jo asmens duomenimis bei teisė juos ištaisyti⁸⁵.

Kalbant apie BDAR, tai yra antrinis ES teisės aktas, kuris konkretizuoja šios teisės turinį ir nustato jos įgyvendinimo ir apsaugos mechanizmus. Šis reglamentas taikomas ES verslo subjektams bei viešos valdžios institucijoms, taip pat ne ES įmonėms, jei jos siūlo prekes ar paslaugas ES gyventojams arba stebi jų veiksmus internete. Pagrindinis šio reglamento tikslas yra apsaugoti asmens duomenis ir suteikti fiziniams asmenims daugiau galimybių kontroliuoti, kas ir koku tikslu juos naudoja. BDAR II skyriuje įtvirtinti pagrindiniai duomenų tvarkymo principai: teisėtumas, sąžiningumas ir skaidrumas. Šis reglamentas nustato, kad asmens duomenys privalo būti renkami tik nustatytais teisėtais tikslais, tvarkomi tik tiek, kiek būtina, taip pat turi būti užtikrintas jų tikslumas ir saugumas. Siekiant užtikrinti teisę į duomenų apsaugą, BDAR fiziniams asmenims nustato keletą konkrečių teisių, t. y. teisę būti informuotam apie duomenų rinkimą, teisę susipažinti su duomenimis, teisę reikalauti ištaisyti duomenis, teisę reikalauti ištrinti duomenis (vadinamoji „teisė būti pamirštam“), teisę apriboti duomenų tvarkymą, teisę į duomenų perkėlimą kitam duomenų valdytojui, teisę nesutikti su asmens duomenų tvarkymu bei teises, susijusias su automatizuotu sprendimų priėmimu ir profiliavimu. Be to, nustatyta, kad duomenų valdytojai, sprendžiantys „kodėl“ ir „kaip“ tvarkyti duomenis, ir duomenų tvarkytojai, veikiantys jų pavedimu, privalo užtikrinti saugumą bei skaidrumą, o įvykus rimtiems asmens duomenų nutekėjimams – pranešti apie incidentą priežiūros institucijoms, o tam tikrais atvejais ir patiems duomenų subjektams.

⁸⁵ Europos Sąjungos pagrindinių teisių chartija. OL C 202, 2016, p. 389–405.

BDAR reikalavimų laikymąsi kontroliuoja kiekvienos valstybės narės įsteigta pagal BDAR 51 straipsnį nepriklausoma priežiūros institucija, kuri gali atlikti patikrinimus ir skirti sankcijas, jei asmens duomenų tvarkymas neatitinka BDAR reikalavimų. Taip pat BDAR numato teisių gynimo priemonės duomenų subjektams, kurie mano, kad su jais susijęs asmens duomenų tvarkymas atliekamas pažeidžiant šį reglamentą. Pagal BDAR 77 straipsnį, toks duomenų subjektas gali pateikti skundą priežiūros institucijai. Reglamentas įtvirtina priežiūros sistemą, kurioje pagrindinį vaidmenį atlieka nacionalinės priežiūros institucijos, tačiau jų veiksmai derinami bei koordinuojami tarpusavyje ES lygmeniu. Būtent tokia struktūra leidžia gerbti valstybių narių institucinę sandarą ir kartu siekti vienodo reglamento taikymo.

Lietuvoje skundai teikiami Valstybinei duomenų apsaugos inspekcijai, kuri atlieka priežiūros instancijos funkcijas. Pastebima, kad gyventojai Lietuvoje vis dažniau kreipiasi į šią instituciją siekdami apginti savo teises į asmens duomenų apsaugą. Valstybinė duomenų apsaugos inspekcija 2025 m. veiklos ataskaitoje pažymi, kad per metus buvo gautas 2081 skundas, o tai yra 48 % daugiau nei 2024 m. Akcentuojama, kad skunduose dažniausiai nagrinėti klausimai buvo susiję su asmens duomenų atskleidimu, vaizdo stebėjimu, tiesiogine rinkodara, asmens duomenų rinkimu bei teise susipažinti su duomenimis⁸⁶. Pabrėžtina, kad Lietuvos teismai taip pat aktyviai nagrinėja bylas dėl duomenų apsaugos pažeidimų. Pavyzdžiui, Lietuvos vyriausiasis administracinis teismas (toliau – LVAT) 2014 m. spalio 23 d. sprendime administracinėje byloje konstatavo, kad duomenų tvarkytojai yra atsakingi už tvarkomos sistemų saugą, konfidencialumą, vientisumą ir prieinamumą bei turi pareigą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju⁸⁷. Be to, LVAT 2025 m. kovo 26 d. nutartyje administracinėje byloje konstatavo, kad sisteminis asmens duomenų peržiūrėjimas nesant teisėto pagrindo bei tikslo pažeidžia BDAR, nes taip pažeidžiamas duomenų subjekto asmens duomenų saugumas ir konfidencialumas⁸⁸. Taigi galima daryti išvadą, kad BDAR nustatyta teisių apsaugos sistema ne tik formaliai įtvirtina asmens duomenų apsaugos mechanizmus, bet ir veiksmingai veikia praktikoje, o tai patvirtina augantis skundų skaičius. Nors, ši tendencija rodo didėjančią visuomenės teisinį sąmoningumą bei pasitikėjimą priežiūros institucijomis, tačiau kartu tai liudija ir apie

⁸⁶ Valstybinė duomenų apsaugos inspekcija (2026-03-05). *2025 m. veiklos ataskaita* [interaktyvus]. https://vdai.lrv.lt/public/canonical/1772605397/1298/2025m_VDAI_veiklos_ataskaita_galutinis.pdf

⁸⁷ Lietuvos vyriausiojo administracinio teismo 2024 m. spalio 23 d. sprendimas administracinėje byloje Nr. eA-1740-525/2024.

⁸⁸ Lietuvos vyriausiojo administracinio teismo 2025 m. kovo 26 d. nutartis administracinėje byloje Nr. eA-483-821/2025.

išliekančias problemas duomenų apsaugos srityje, kurios reikalauja tolimesnio teisinio reguliavimo bei jo taikymo tobulinimo.

Toliau apžvelgiamos konkrečios bylos, kuriose išsamiau nagrinėjamos su duomenų apsauga susijusios žmogaus teisės. Pavyzdžiui, viena iš pastarojo meto bylų padėjo paaiškinti BDAR 22 straipsnio taikymą, kuriame įtvirtintas draudimas priimti automatizuotus sprendimus. 2023 m. byloje *OQ prieš Land Hessen* ESTT nurodė, kad BDAR 22 straipsnio nuostata turi būti taikoma, kai: (1) yra priimamas sprendimas, (2) šis sprendimas grindžiamas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, ir (3) jis turi turėti teisinių pasekmių suinteresuotajam asmeniui arba daryti jam panašiu būdu didelį poveikį. Išnagrinėjęs bylos aplinkybes, ESTT konstatavo, kad BDAR 22 straipsnio 1 dalis turi būti aiškinama taip, kad komercinę informaciją teikiančios bendrovės atliekamas automatizuotas asmens mokumo tikimybės rodiklio nustatymas (reitingavimas), pagrįstas asmens duomenimis apie jo finansinį pajėgumą vykdyti įsipareigojimus, laikomas „automatizuotu atskiru sprendimu“. Kadangi, nuo šio tikimybės rodiklio iš esmės priklauso trečiosios šalies sprendimas pradėti, vykdyti ar nutraukti sutartinius santykius su šiuo asmeniu⁸⁹. Teigiamas šio sprendimo aspektas yra tai, kad ESTT nustatytas aukštas algoritminio duomenų tvarkymo standartas, stiprina duomenų subjekto apsaugą, užtikrindamas, kad sprendimai nebūtų priimami vien tik remiantis automatizuotais susistemintais duomenimis.

Tikslinga apžvelgti ir BDAR 17 straipsnyje įtvirtintą vadinamąją „teisę būti pamirštam“. Ši teisė ESTT praktikoje buvo atpažįstama dar iki BDAR priėmimo. Pavyzdžiui, 2014 m. byloje *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* ESTT, nors dar nevartojo sąvokos „teisė būti pamirštam“, o analizavo teisę ištrinti asmens duomenys per Chartijos 7 ir 8 straipsnių prizmę (teisė į privataus gyvenimo gerbimą ir teisė į asmens duomenų apsaugą), ESTT konstatavo, kad „Google“, kaip paieškos sistema, yra laikoma duomenų valdytoja ir privalo, esant tam tikroms sąlygoms, iš paieškos rezultatų pašalinti nuorodas į asmens duomenis, net jei jie buvo teisėtai paskelbti trečiųjų asmenų tinklalapiuose. Pažymėtina, kad šioje byloje ESTT konstatavo, jog teisė į privatumą ir duomenų apsaugą paprastai turi viršenybę prieš visuomenės interesą gauti informaciją, tačiau šios teisės gali būti ribojamos, jei dėl konkrečių aplinkybių, ypač kai kalbama apie viešą asmenį, visuomenės interesas turi didesnę reikšmę⁹⁰. Plėtodamas šią praktiką, 2019 m. byloje *Google LLC prieš Commission*

⁸⁹ *OQ prieš Land Hessen* [ESTT], Nr. C-634/21, [2023-12-07]. ECLI:EU:C:2023:957.

⁹⁰ *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* [ESTT], Nr. C-131/12, [2014-05-13]. ECLI:EU:C:2014:317.

nationale de l'informatique et des libertés (CNIL) ESTT patikslino šios teisės veikimo teritoriją, nurodydamas, kad „Google“ turi pašalinti paieškos rezultatus tik ES teritorijoje, t. y. už ES ribų šie rezultatai gali likti⁹¹. Taip pat, byloje *GC, AF, BH, ED prieš Commission nationale de l'informatique et des libertés (CNIL)*, ESTT patikslino minėtų teisių balansą jautrių duomenų kontekste. Teismas nurodė, kad nuorodos į informaciją apie baudžiamąjį procesą turi būti pašalintos iš paieškos rezultatų, jeigu ši informacija yra pasenusi arba yra perteklinė, išskyrus atvejus, kai jos išlaikymas yra būtinas siekiant užtikrinti visuomenės teisę gauti informaciją⁹². Darytina išvada, kad kiekvienu atveju, kai susikerta Chartijos 7 ir 8 straipsnių saugomos teisės, ESTT, prieš priimdamas sprendimą, turi atlikti teisių pusiausvyros testą. Minėtuose pavyzdžiuose pirmenybė yra teikiama asmens teisėms (Chartijos 7 ir 8 straipsniai), nebent konkrečiomis aplinkybėmis viršesnis yra visuomenės interesas (Chartijos 11 straipsnis).

Svarbu pažymėti, kad šiandien neįmanoma įsivaizduoti pasaulio be tarptautinių duomenų srautų. Todėl BDAR nustato nuoseklią teisinę sistemą, pagal kurią asmens duomenų perdavimas į trečiąsias šalis leidžiamas tik tuo atveju, jei nepažeidžiamas ES garantuojamas apsaugos lygis (BDAR V skyrius). Tai laikytina ES skaitmeninio suvereniteto įgyvendinimu, nes pasauliniai duomenų srautai nėra draudžiami, tačiau jie griežtai reglamentuojami ES teisės aktais. Todėl, siekdamas užtikrinti perduodamų duomenų apsaugą, kai kurios šalys sudaro dvišalius susitarimus dėl duomenų perdavimo. Pavyzdžiui, tarp ES ir JAV buvo sudarytas susitarimas „Privatumo skydas“ (angl. EU – U.S. Privacy Shield), kuris sudarė sąlygas keistis duomenimis tarp ES ir JAV, kol 2020 m. ESTT, išnagrinėjęs *Data Protection Commissioner prieš Facebook Ireland Limited ir Maximillian Schrems* bylą (dar vadinama „*Schrems II*“ byla), šį susitarimą panaikino. Šioje byloje ESTT suformulavo keletą esminių taisyklių.

Pirma, konstatuota, kad priežiūros institucija negali uždrausti duomenų perdavimo vien savo nuožiūra sprendama, jog nėra užtikrinamas tinkamas apsaugos lygis, nes galiojo Komisijos 2016 m. liepos 12 d. įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB⁹³. Tačiau kartu ESTT pabrėžė, kad priežiūros institucija vis

⁹¹ *Google LLC prieš Commission nationale de l'informatique et des libertés (CNIL)* [ESTT], Nr. C-507/17, [2019-09-24]. ECLI:EU:C:2019:772.

⁹² *GC, AF, BH, ED prieš Commission nationale de l'informatique et des libertés (CNIL)* [ESTT], Nr. C-136/17, [2019-09-24], ECLI:EU:C:2019:773.

⁹³ Komisijos 2016 m. liepos 12 d. įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB. OL L 207/1, 2016, p. 1-112.

tiesiog turi savarankiškai išnagrinėti skundą, o jei abejonės yra pagrįstos, ji turi kreiptis į teisumą⁹⁴.

Antra, ESTT pabrėžė, kad nepakanka vien formalaus pareiškimo, jog kitoje šalyje užtikrinama duomenų apsauga. Būtina nustatyti, ar toje valstybėje garantuojamas apsaugos lygis iš esmės yra lygiavertis tam, kuris numatytas ES teisėje⁹⁵.

Trečia, ESTT nustatė, kad JAV įstatymai neatitinka minimalių proporcingumo reikalavimų, t. y. JAV teisės aktai leido per plačią prieigą prie perduotų duomenų, o tai prieštarauja Chartijos 7 ir 8 straipsniams. Be to, ESTT nustatė, kad perduotų duomenų subjektams nebuvo užtikrinta veiksminga teisių gynība, o tai iš esmės pažeidžia Chartijos 47 straipsnį⁹⁶.

Atsižvelgdama į ESTT išaiškinimus, 2023 m. Europos Komisija priėmė Komisijos 2023 m. liepos 10 d. įgyvendinimo sprendimą (ES) 2023/1795, priimtą pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamo asmens duomenų apsaugos lygio pagal ES ir JAV duomenų privatumo sistemą. Šio sprendimu JAV vėl pripažinta tinkama trečiąja šalimi asmens duomenų perdavimui iš ES organizacijoms, sertifikuotoms pagal naują ES ir JAV duomenų apsaugos susitarimą – ES ir JAV duomenų privatumo sistemą (angl. EU – US Data Privacy Framework)⁹⁷. Be to, Europos Komisija 2024 m. atliko pirmąją šios sistemos veikimo peržiūrą, įtvirtindama vadinamąjį „dinaminio adekvatumo“ principą. Juo remiantis, apsaugos lygiavertiškumas turi būti nuolat vertinamas ir užtikrinamas kintančiomis technologinėmis ir politinėmis sąlygomis⁹⁸. Šio mechanizmo priėmimas rodo, jog ES turi ieškoti pusiausvyros tarp griežtų teisinių standartų ir ekonominės būtinybės užtikrinti tarptautinius duomenų srautus. Šis atvejis atskleidžia ES padėties dvilypumą: viena vertus, ji nuosekliai stiprina teisių apsaugą skaitmeninėje erdvėje bei siekia įtvirtinti skaitmeninį suverenitetą, kita vertus, ES išlieka priklausoma nuo tarptautinių duomenų mainų, o tai lemia nuolatinį teisinių mechanizmų peržiūrėjimą ir jų tobulinimą.

⁹⁴ *Data Protection Commissioner prieš Facebook Ireland Limited ir Maximilian Schrems* [ESTT], Nr. C-311/18, [2020-07-16]. ECLI:EU:C:2020:559.

⁹⁵ *Ibid.*

⁹⁶ *Ibid.*

⁹⁷ Komisijos 2023 m. liepos 10 d. įgyvendinimo sprendimas (ES) 2023/1795, priimtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679, dėl tinkamo asmens duomenų apsaugos lygio pagal ES ir JAV duomenų privatumo sistemą. OL L 231/118, 2023, p. 118-229.

⁹⁸ European Commission (2024-10-09). *Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, COM(2024) 451 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0451>.

Apibendrinant, Europos duomenų strategija atspindi ES siekį sukurti skaitmeninę ekonomiką, orientuotą į žmogų ir jo teises, kadangi jos pagrindinis bruožas yra tai, kad technologijų ir duomenų ekonomikos plėtra tiesiogiai siejama su pagrindinių teisių ir ES vertybių apsauga. Bendrosios ES duomenų erdvės sukūrimas skatina platesnį informacijos naudojimą tokiose srityse kaip sveikatos priežiūra, transportas ir energetika, o tai gerina piliečių gyvenimo kokybę bei didina visuomeninių gėrybių prieinamumą. Be to, sukurti mechanizmai, leidžia asmenims patiems kontroliuoti savo duomenis, o tai stiprina jų autonomiją ir saugumą skaitmeninėje aplinkoje.

Strategijos įgyvendinimą lydi specialiųjų teisės aktų, pavyzdžiui, Duomenų valdymo akto ir Duomenų akto, priėmimas. Šie dokumentai skirti užtikrinti saugų keitimąsi duomenimis. Minėtos priemonės didina pasitikėjimą skaitmenine aplinka dėl naujai nustatomų skaidrių taisyklių.

Verta paminėti, kad esminį vaidmenį šioje sistemoje atlieka BDAR, kuris įtvirtina pagrindines asmens duomenų bei privatumo apsaugos garantijas. Jis nustato aiškius duomenų tvarkymo principus ir suteikia asmenims realias teisių gynimo priemones. Praktikoje BDAR pasitvirtino kaip veiksmingas instrumentas, tapęs orientyru kitoms valstybėms. Šiame kontekste svarbu paminėti vadinamąjį „Briuselio efektą“, kuris reiškia, kad ES teisės normos daro įtaką ir už Sąjungos ribų. Dėl didelės rinkos bei griežtų standartų tarptautinės įmonės dažnai yra priverstos taikyti ES taisykles visame pasaulyje, kad išlaikytų prieigą prie ES rinkos. Būtent BDAR tapo faktiniu tarptautiniu duomenų apsaugos standartu, paveikusiu daugelio kitų šalių įstatymus. Tai stiprina žmogaus teisių apsaugą ne tik ES viduje, bet ir pasauliniu mastu.

Apibendrinant galima teigti, kad Europos duomenų strategija formuoja skaitmeninės erdvės reguliavimo modelį, kuriame technologijų plėtra derinama su žmogaus teisių apsauga, o ES veikla peržengia jos jurisdikcijos ribas, nustatydamą aukštesnius teisinius standartus skaitmeninėje erdvėje visame pasaulyje.

2.3. Technologijų reguliavimas kaip žmogaus teisių apsaugos priemonė

Europos skaitmeninio suvereniteto kontekste technologijų reguliavimas, kaip pagrindinių teisių apsaugos priemonė, įgyja ypatingą reikšmę. Akivaizdu, kad nekontroliuojamas dirbtinio intelekto sistemų, automatizuoto sprendimų priėmimo bei kitų inovatyvių technologijų plitimas kelia grėsmę teisei į privatumą, asmens duomenų apsaugai, nediskriminavimui ir veiksmingai teisinei gynybai. Reaguodama į šiuos iššūkius, ES formuoja unikalų reguliavimo modelį, pagal kurį technologijų plėtra yra reglamentuojama įstatymais, grindžiamais ES vertybėmis, o tai reiškia, kad technologijų reguliavimą galima laikyti neatsiejama skaitmeninio suvereniteto dalimi, garantuojančia aukštą žmogaus teisių apsaugos lygį.

Analizuojant interneto ribojimo galimybes, pažymėtina 2011 m. Jungtinių Tautų specialiojo pranešėjo Franko La Rue ataskaita „Nuomonės ir saviraiškos laisvės skatinimas ir apsauga“. Specialusis pranešėjas nurodo, kad, internetas, kaip ir bet kurie kiti technologiniai išradimai, gali būti naudojamas netinkamai, darant žalą kitiems asmenims. Analogiškai kaip ir neinternetinėje erdvėje, ribojimai internetinėje erdvėje privalo būti išimtinė priemonė ir turi atitikti tam tikrus reikalavimus⁹⁹.

Pirma, jie turi būti nustatyti aiškiu ir visiems prieinamu įstatymu¹⁰⁰. Čia pranešėjas remiasi teisinio reguliavimo aiškumo ir skaidrumo principais.

Antra, teisinis reguliavimas turi būti nukreiptas į Pakto 19 straipsnio 3 dalyje numatytų tikslų siekimą, o būtent į: i) kitų asmenų teisių ar reputacijos apsaugą; ii) valstybės saugumo, viešosios tvarkos, visuomenės sveikatos ar moralės apsaugą. Čia išvelgiama teisingumo principo išraiška.

Trečia, ji turi būti laikoma būtina ir mažiausiai ribojančia priemone, reikalinga nurodytam tikslui pasiekti¹⁰¹. Šiuo atveju reguliavimą reikia vertinti per būtinumo ir proporcingumo principus.

Be to, pranešėjas pažymi, kad bet kokius saviraiškos laisvę ribojančius teisės aktus, privalo taikyti institucijos, kurios nėra politinio, komercinio ar kito nepagrįsto poveikio įtakoje. Taip užtikrinama apsauga nuo savavališkumo ar diskriminacijos. Pranešėjas taip pat akcentuoja vykdymo priežiūros sistemos ir asmenų teisės į gynybą svarbą. Jo teigimu,

⁹⁹ United Nations (2011-05-16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)* [interaktyvus]. <https://docs.un.org/en/A/HRC/17/27>.

¹⁰⁰ *Ibid.*

¹⁰¹ *Ibid.*

būtina numatytos tinkamos apsaugos priemonės nuo piktnaudžiavimo taikomais apribojimais, įskaitant galimybę ginčyti jų neteisėtą taikymą ir pašalinti pasekmes¹⁰².

Analizuojant skaitmeninę erdvę, akivaizdu, kad dezinformacija yra didžiausių jos problemų. ES Žiniasklaidos ir informacinės visuomenės valdymo komitetas pažymi, kad dezinformacijos pobūdis nuolat kinta, todėl būtina operatyviai prisitaikyti tiek prie šios problemos supratimo, tiek prie jai spręsti reikalingų priemonių. Taip pat pabrėžiama, kad daugelyje šalių auga susirūpinimas, jog nauji iššūkiai, susiję su dirbtinio intelekto pagrindu sugeneruota klaidinančia informacija, pavyzdžiui, „deepfake“, gali dar labiau sustiprinti kai kurių valstybių narių šiuo metu taikomus staigius ir fragmentiškus reguliavimo metodus¹⁰³. Remiantis Europos Tarybos aiškinimu, „dezinformacija“ reiškia patvirtintą melagingą, netikslią arba klaidinančią informaciją, kuri sąmoningai sukurta ir platinama siekiant padaryti žalą arba gauti ekonominės ar politinės naudos, klaidinant visuomenę¹⁰⁴. Tačiau populiarėja nuomonė, kad dezinformacija peržengia siaurą melagingos žinios sampratą ir apima platesnį reiškinių spektrą: propagandą, manipuliavimą informacija, užsienio šalių intervencijas į informacinę erdvę, kurios silpnina visuomenės pasitikėjimą.

Atsižvelgiant į tai, susiformavo „informacinio vientisumo“ koncepcija. Jos pagrindas tai kūrimas tokios informacinės aplinkos, kuri užtikrintų prieigą prie patikimos, įvairiapusės ir patikrintos informacijos, kuri padėtų priimti apgalvotus ir sąmoningus sprendimus¹⁰⁵. Pavyzdžiui, minėtasis Žiniasklaidos ir informacinės visuomenės iniciatyvinis komitetas rekomenduoja kovoti su dezinformacija kompleksiniu būdu. Jis skatina parengti nacionalines normas, pagrįstas naujų technologijų tyrimais ir siūlo jas derinti su visuomenės skaitmeninio raštingumo ugdymu bei kokybiškų žiniasklaidos organizacijų rėmimu. Tai būtų užtikrinama skaitmeninių platformų atskaitomybė, nepažeidžiant teisės į saviraiškos laisvę¹⁰⁶.

Europos Komisija irgi įvardija kovą su dezinformacija kaip vieną iš skaitmeninio suvereniteto tikslų. Greta dezinformacijos apibrėžties, kuri sutampa su Europos Tarybos

¹⁰² United Nations (2011-05-16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)* [interaktyvus]. <https://docs.un.org/en/A/HRC/17/27>.

¹⁰³ Steering Committee on Media and Information Society (CDMSI) (2025-12-05). *Resisting Disinformation: ten building blocks to strengthen information integrity* [interaktyvus]. <https://rm.coe.int/cdmsi-2025-17rev-clean-resisting-disinformation-10-building-blocks-f/488029df7d>.

¹⁰⁴ Council of Europe (2022-04-06). *Recommendation of the Committee of Ministers to member States CM/Rec(2022)11 on principles for media and communication governance* [interaktyvus]. <https://search.coe.int/cm?i=09125948802680f5>.

¹⁰⁵ Steering Committee on Media and Information Society (CDMSI) (2025-12-05). *Resisting Disinformation: ten building blocks to strengthen information integrity* [interaktyvus]. <https://rm.coe.int/cdmsi-2025-17rev-clean-resisting-disinformation-10-building-blocks-f/488029df7d>.

¹⁰⁶ *Ibid.*

pateikta samprata, Europos Komisija išskiria ir klaidingos informacijos sąvoką. Remiantis Europos Komisijos išaiškinimu, klaidinga informacija – tai melagingas ar klaidinantis turinys, kuriuo dalijamasi neturint žalingų ketinimų, nors jo poveikis visuomenei vis tiek gali būti žalingas¹⁰⁷.

ES kovoja su dezinformacija pasitelkdama ne pavienius įstatymus, o visapusišką priemonių sistemą, t. y. ES nesiekia tiesiog uždrausti dezinformaciją, bet kuria mechanizmus, pagal kuriuos platformos tampa atsakingos už rizikos mažinimą, politinė reklama tampa skaidresnė, stebimas užsienio valstybių kišimasis į informacinę erdvę, o piliečiai ugdomi geriau atpažinti nepatikimą informaciją.

Pagrindinis teisės aktas, skirtas kovai su dezinformacija, yra Skaitmeninių paslaugų aktas, kuris įpareigoja dideles interneto platformas mažinti dezinformacijos sklaidą skaitmeninėje erdvėje. Taip pat, pažymėtinas 2018 m. sukurtas Kovos su dezinformacija elgesio kodeksas, kuris 2025 m. buvo integruotas į Skaitmeninių paslaugų aktą¹⁰⁸. Šis kodeksas nėra privalomas visoms valstybėms ar visiems rinkos dalyviams, tačiau jis yra privalomas jį pasirašiusioms didelėms interneto platformoms ir paieškos sistemoms, kurioms taikomas Skaitmeninių paslaugų aktas. Tokiems subjektams minėtas kodeksas tampa standartu, kurio jie privalo laikytis vykdydami teisinę prievolę mažinti sisteminės rizikas. Šio kodekso laikymasis vertinamas atliekant platformų auditą, o atsisakius juo vadovautis, privaloma įrodyti, kad taikomos alternatyvios, lygiavertės kovos su dezinformacija priemonės. Kovos su dezinformacija elgesio kodeksas yra reguliavimo priemonė, įpareigojanti interneto platformas ir skaitmeninės rinkos dalyvius savarankiškai imtis priemonių kovai su dezinformacija. Visa tai vykdoma griežtomis ES priežiūros sąlygomis. Pažymėtina, kad pagrindinis Kovos su dezinformacija elgesio kodekso tikslas nėra ištrinti visą abejotiną informaciją be jokios atrankos. Tikslas yra siekti sumažinti sisteminės dezinformacijos atsiradimo rizikas, apribojant dezinformacijos finansavimą, užtikrinant skaidrią rinkimų reklamą, teikiant duomenis dezinformacijos tyrėjams, bendradarbiaujant su nepriklausomais faktų tikrintojais, suteikiant vartotojams galimybę skųstis dėl nepatikimo turinio ir naudojant kitokiais priemonės¹⁰⁹.

Šiuo metu ES aktyviai plėtojamas dirbtinio intelekto (toliau – DI) technologijų teisinis reguliavimas. ES parengė pirmąją istorijoje teisės aktą, kuris apima daugumą problemų,

¹⁰⁷ Europos Komisija (2025-11-12). *Kova su internetine dezinformacija* [interaktyvus]. <https://digital-strategy.ec.europa.eu/lt/policies/online-disinformation>.

¹⁰⁸ Europos Komisija (2025-11-19). *Elgesio kodeksai pagal Skaitmeninių paslaugų aktą* [interaktyvus]. <https://digital-strategy.ec.europa.eu/lt/policies/dsa-codes-conduct>.

¹⁰⁹ European Union (2025). *Code of Conduct on Disinformation with Overview* [interaktyvus]. Luxembourg: Publications Office of the European Union. <https://ec.europa.eu/newsroom/dae/redirection/document/112678>.

kylančių dėl DI sistemų naudojimo – Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas (ES) 2024/1689, 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) (toliau – Dirbtinio intelekto aktas)¹¹⁰. ES vertina DI plėtrą kaip strategiškai svarbią sritį ir pagrindinį ekonomikos vystymosi variklį, todėl taiko rizika grindžiamą požiūrį į šios srities reguliavimą. Dirbtinio intelekto akte išskiriami keturi rizikos lygiai: nepriimtinos rizikos sistemos, didelės rizikos sistemos, ribotos rizikos sistemos ir nedidelės rizikos sistemos.

Nepriimtinos rizikos DI sistemos draudžiamos. Šiai kategorijai priskiriamos visos DI sistemos, kurios naudojamos Dirbtinio intelekto akto 5 straipsnyje nurodytai praktikai įgyvendinti, t. y. tokie veiksmai, kaip (1) žalingas DI grindžiamas manipuliavimas, apgaulė, pažeidžiamumų išnaudojimas, (2) socialinių reitingų kūrimas, (3) nusikalstamų veiklų rizikos vertinimas arba prognozė, (4) veido atpažinimo duomenų bazių kūrimas, netikslingai renkant veido atvaizdus iš interneto, (5) DI grindžiamos sistemos, kurios skirtos asmens emocijoms darbo ir švietimo įstaigų srityse numanyti, (6) biometrinio kategorizavimo sistemų kūrimas bei (7) tikralaikis nuotolinis biometrinis tapatybės nustatymas teisėsaugos tikslais viešosiose erdvėse.

Didelės rizikos DI sistemoms priskiriami tokie technologijų naudojimo atvejai, kai kyla esminis pavojus visuomenės gyvybei ir sveikatai bei kai tai gali pažeisti žmogaus teisės, tokiose srityse kaip kritinė infrastruktūra, švietimas, sveikatos priežiūra, užimtumas, prieiga prie viešųjų ir privačių paslaugų, biometrinis atpažinimas, teisėsauga, migracija bei teisingumo ir demokratiniai procesai (konkretų sąrašą pateikia Dirbtinio intelekto akto III priedas). Iš esmės Dirbtinio intelekto aktas nustato griežtą reguliavimą būtent šioms didelės rizikos DI sistemoms.

Ribotos rizikos DI sistemoms nustatomos atitinkamos skaidrumo pareigos, kurių esminis tikslas yra užtikrinti, kad tokios sistemos būtų projektuojamos bei kuriamos informuojant fizinius asmenis apie tai, kad jie sąveikauja su atitinkama DI sistema (Dirbtinio intelekto akto IV skyrius). Minimalios rizikos sistemos nėra reglamentuojamos šio aktu.

¹¹⁰ Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas (ES) 2024/1689, 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). OL L 2024/1689, 2024.

Taigi, matytina, kad ES formuoja požiūrį, kuris nesustabdo technologijų plėtros ir kartu užtikrina ES vertybių bei žmogaus teisių ir laisvių apsaugą, nes taisyklės nustatomos tik specifinėms, riziką keliančioms sistemoms.

Kadangi Dirbtinio intelekto aktas yra naujas teisės aktas, ESTT dar nespėjo suformuoti išsamios teismų praktikos, susijusios su šio akto taikymu ir aiškinimu. Šia tema ESTT nagrinėjamos dvi bylos. Pavyzdžiui, 2024 m. Bulgarijos teismas padavė prašymą ESTT dėl prejudicinio sprendimo byloje *YETTEL BULGARIA EAD prieš FB*. Šioje byloje keliami keli svarbūs klausimai dėl automatizuoto sprendimų priėmimo, vartotojų teisių ir algoritmų skaidrumo, galintys turėti tiesioginės įtakos DI sistemų naudojimui ES. Šioje byloje telekomunikacijų paslaugų vartotojas teigia, kad automatizuotas mokesčio apskaičiavimo būdas yra laikytinas automatizuoto sprendimų priėmimo sistema, kuriai taikoma Dirbtinio intelekto akto 86 straipsnio 1 dalis, bei iškėlė klausimus dėl tokios sistemos naudojimo skaidrumo, žmogaus peržiūros privalomumo ir priimtų sprendimų teisėtumo bei teisingumo. Bulgarijos teismas suformulavo 17 klausimų, susijusių su Dirbtinio intelekto akto taikymu. Pavyzdžiui, ar verslininkas privalo informuoti vartotoją, kad sprendimas priimtas automatizuotai, ar vartotojas turi teisę reikalauti, kad jam būtų paaiškintas sprendimų priėmimo algoritmas, ar vartotojas turi teisę į žmogiškąją sprendimų kontrolę ir ar tokia kontrolė turi būti vykdoma per teismo procesą¹¹¹. Nors šiame darbe jau paminėta reikšminga byla dėl automatizuotomis sistemomis grindžiamų sprendimų teisėtumo, t. y. *OQ prieš Land Hessen*, vis dėlto ji buvo nagrinėjama BDAR kontekste, kadangi Dirbtinio intelekto aktas dar nebuvo priimtas¹¹². Taigi ši nauja byla turėtų atskleisti išsamesnius DI sistemų naudojimo aspektus.

Aktuali ir kita byla taip pat kilusi iš Bulgarijos teismo, 2025 m. *DZI – OBSHTO ZASTRAHOVANE EAD prieš ZK LEV INS AD*, susijusi su ginčo dėl eismo įvykio sprendimu. Bylą nagrinėjantis teismas pavedė eismo įvykių teismo ekspertui atlikti kompiuterinį avarijos modeliavimą, siekiant ją atkurti ir vizualizuoti. Ekspertas savo darbe naudojo programą „Virtual Crash“. Ieškovas užginčijo ekspertinę išvadą ir pareikalavo pateikti išsamų visų skaičiavimų aprašymą, kad būtų galima juos patikrinti rankiniu būdu. Ieškovo nuomone, be tokio aprašymo neįmanoma patikrinti ekspertinės išvados teisingumo, o programa gali turėti techninių klaidų. Teismas pastebėjo, kad ši programinė įranga, analizuojanti duomenis, formuojanti išvadas ir pateikianti galutinius rezultatus, turi dirbtinio intelekto elementų, kaip apibrėžta Dirbtinio intelekto akto III priedo 8 punkte,

¹¹¹ *YETTEL BULGARIA EAD prieš FB* [ESTT], Nr. C-806/24, [2025-02-07]. Application (OJ).

¹¹² *OQ prieš Land Hessen* [ESTT], Nr. C-634/21, [2023-12-07]. ECLI:EU:C:2023:957.

arba yra automatizuoto sprendimų priėmimo sistema. Taigi, kad priimti byloje sprendimą Bulgarijos teismas kreipėsi į ESTT su tokiais klausimais kaip: ar programinė įranga, kurią ekspertas naudoja išvadai parengti, ir kuri vėliau naudojama teismui priimant sprendimą, yra „didelės rizikos DI sistema“ pagal Dirbtinio intelekto įstatymo III priedo 8 punktą; ar laikoma, kad laikomasi žmogaus priežiūros principo, jei ekspertas rankiniu būdu patikrino sistemos gautą rezultatą, palygindamas jį su nustatytais faktais ir profesine patirtimi; ar aiškumą ir atsekamumą principai reikalauja pateikti išsamų algoritmo aprašymą, visus skaičiavimus ir prielaidas (įskaitant elementarius skaičiavimus); ar teisė į teisingą teismo procesą leidžia teismui naudoti ekspertinę išvadą, parengtą naudojant DI, jei ekspertas patikrino rezultatą remdamasis profesine patirtimi.¹¹³ Ši byla turės esminę reikšmę naujai formuojamai praktikai, nes joje bus nustatyta DI ir automatizuotų sprendimų priėmimo sistemų vaidmuo bei jų naudojimo leistinas mastas renkant įrodymus, reikalingus teismo sprendimams priimti. Taigi ši byla gali sukurti teisinį precedentą DI naudojimui nagrinėjant teismo įvykių bylas. Ji taip pat leis nustatyti, ar ekspertų naudojami įrankiai patenka į didelės rizikos DI sistemų kategoriją, ar jiems taikomi griežti Dirbtinio intelekto akto reikalavimai, taip pat bus nustatyta kokie etiniai standartai turėtų būti taikomi tokioms sistemoms jų kūrimo, diegimo, naudojimo ir kontrolės etapuose, jei jos bus pripažintos didelės rizikos sistemomis. Žmogaus teisių apsaugos požiūriu, ši byla yra esminė teisei į teisingą teismo procesą užtikrinti, kadangi teismas savo sprendimą grindžia ekspertų išvadomis, todėl naudojimų DI sistemų sugeneruotų įrodymų patikimumas, patikrinimas bei skaidrumas tampa prioritetiniais kriterijais.

Pažymėtina, kad DI sistemų priimamų sprendimų skaidrumas buvo akcentuojamas dar iki Dirbtinio intelekto akto priėmimo. Europos Komisija savo ataskaitoje remiasi 2020 m. Nyderlandų teisme nagrinėtą bylą, kurioje teismas, vadovaudamasis EŽTK įtvirtinta teise į privataus gyvenimo gerbimą, pripažino negaliojančiu Nyderlandų teisės aktą, kuriuo nustatoma sukčiavimo socialinės apsaugos srityje aptikimo sistema „Systeem Risico Indicatie“ („SyRI“). Ši sukčiavimo aptikimo sistema buvo naudojama analizuojant įvairių valdžios institucijų surinktus duomenis, siekiant nustatyti asmenis, galimai neteisėtai besinaudojančius socialinėmis išmokomis. Nors sistema analizavo didelius duomenų masyvus ir prognozavo piktnaudžiavimo tikimybę, nustatyta, kad patikros neproporcingai dažnai buvo nukreipiamos į socialiai pažeidžiamas asmenų grupės, o tai vertintina kaip diskriminacija. Be to, asmenys neturėjo galimybės suprasti, kaip priimami sprendimai šioje

¹¹³ *DZI – OBSHTO ZASTRAHOVANE EAD prieš ZK LEV INS AD* [ESTT], Nr. C-245/25, [2026-01-26]. Application (OJ).

sistemoje. Dėl minėtų priežasčių visumos, Nyderlandų teismas konstatavo, kad „SyRi“ sistema neatitiko skaidrumo reikalavimų, o ja įtvirtinti teisės į privatų gyvenimą ribojimai nebuvo proporcingi siekiamam tikslui, t. y. išaiškinti sukčiavimo atvejus¹¹⁴.

Atlikta analizė leidžia daryti išvada, kad DI reguliavimas ES yra santykinai nauja teisinio reguliavimo sritis, kurios raidą lemia sparti technologinė plėtra ir augimas. Remdamasi skaitmeninio suvereniteto koncepcija, ES siekia nustatyti tokias taisykles, kurios, užtikrintų pagrindinių žmogaus teisių – visų pirma teisės į asmens privatų gyvenimą ir asmens duomenų – apsaugą, kartu sudarant palankias sąlygas inovacijoms ir technologiniam progresui. ES teisėkūros strategija grindžiama būtinumo ir proporcingumo principais, kurie leidžia sukurti subalansuotą reguliavimą, t.y. riboti tik tas DI naudojimo praktikas, kurios kelia realią grėsmę saugumui ar fundamentalioms teisėms, tai skatinant atsakingą technologijų vystymąsi. Akivaizdu, kad ši reguliavimo sritis yra dar tik pradiniam etape, todėl artimiausioje ateityje numatoma intensyvi šios srities plėtra.

¹¹⁴ Europos Komisija (2021). *Komisijos ataskaita Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Pagrindinių teisių apsauga skaitmeniniame amžiuje, 2021 m. metinė ES pagrindinių teisių chartijos taikymo ataskaita, COM(2021) 819 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52021DC0819>.)

3. SKAITMENINIO SUVERENITETO KELIAMOS GRĖSMĖS ŽMOGAUS TEISĖMS

3.1. Prioritetų disbalansas tarp technologijų plėtros ir žmogaus teisių apsaugos

Didžioji skaitmeninio suvereniteto politikos dalis yra orientuota į ES technologinės nepriklausomybės užtikrinimą. Šiame darbe jau aptarta nepriklausomų technologijų plėtros svarba ES, vertinant geopolitinį kontekstą bei didžiųjų skaitmeninių platformų daromą spaudimą. Todėl darytina prielaida, kad tokios lenktynės dėl inovacijų praktikoje gali kelti pavojų pagrindinėms žmogaus teisėms. Šią mintį patvirtina įvairių žmogaus apsaugą stebinčių nevyriausybinių organizacijų ataskaitos.

Toliau darbe pateikiamas pavyzdys, kuris nėra laikytinas tiesioginiu ES skaitmeninės politikos aktu, tačiau jis iliustruoja ES požiūrį, kai tenka priimti sprendimą tarp dviejų prioritetų – ES konkurencingumo didinimo ir griežtų žmogaus teisių apsaugos mechanizmų užtikrinimo.

2024 m. buvo priimta Europos Parlamento ir Tarybos 2024 m. birželio 13 d. direktyva (ES) 2024/1760, dėl įmonių tvarumo išsamaus patikrinimo, kuria iš dalies keičiama Direktyva (ES) 2019/1937 ir Reglamentas (ES) 2023/2859 (toliau – Įmonių tvarumo išsamaus patikrinimo direktyva). Šios direktyvos tikslas yra užtikrinti, kad įmonės identifikuotų ir šalintų neigiamą poveikį žmogaus teisėms bei aplinkai visoje savo veiklos grandinėje¹¹⁵. Šis reguliavimas labiausiai paveikė įmones, turėjusias daugiau nei 1000 darbuotojų ir kurių pasaulinė grynoji apyvarta viršijo 450 mln. eurų (Įmonių tvarumo išsamaus patikrinimo direktyvos 2 straipsnio 1 dalies a punktas).

Tačiau 2025 m. vasario mėn. Europos Komisija paskelbė „Omnibus 1“ pasiūlymų rinkinį, kuris apėmė reikšmingus Įmonių tvarumo išsamaus patikrinimo direktyvos pakeitimus. 2026 m. šie pakeitimai buvo įgyvendinti priėmus Europos Parlamento ir Tarybos 2026 m. vasario 24 d. direktyvą (ES) 2026/470, kuria iš dalies keičiamos direktyvos 2006/43/EB, 2013/34/ES, (ES) 2022/2464 ir (ES) 2024/1760, kiek tai susiję su tam tikrais įmonių tvarumo atskaitomybės ir tvarumo išsamaus patikrinimo reikalavimais. Šia direktyva buvo padidinta Įmonių tvarumo išsamaus patikrinimo direktyvos nuostatų taikymo riba ir nustatyta, kad ji bus taikoma įmonėms, turinčioms daugiau nei 5000

¹¹⁵ Europos Parlamento ir Tarybos 2024 m. birželio 13 d. direktyva (ES) 2024/1760, dėl įmonių tvarumo išsamaus patikrinimo, kuria iš dalies keičiama Direktyva (ES) 2019/1937 ir Reglamentas (ES) 2023/2859. OL L 2024/1760, 2024.

darbuotojų bei 1,5 mlrd. eurų pasaulinės grynosios apyvartos¹¹⁶. Būtent šis pakeitimas sulaukė didžiausios kritikos iš žmogaus teisių apsaugos organizacijų. Pavyzdžiui, „Human Rights Watch“ nurodo, kad subjektų, kuriems taikomas reglamentas, skaičius sumažėjo daugiau nei 72 %. Tai paveikia žmogaus teisių apsaugos lygį, nes galimi žmogaus teisių pažeidimo atvejai tampa mažiau pastebimi atvejais¹¹⁷. Akivaizdu, kad šių pakeitimų priėmimas žymiai susiaurino direktyvos taikymo sritį.

Be to, minėta organizacija pažymėjo, kad pilietinės visuomenės organizacijos vykdė tyrimą, kuriame užfiksavo reikšmingą pramonės asociacijų ir Europos bei JAV iškastinio kuro įmonių vaidmenį skatinant „Omnibus I“ pasiūlymų priėmimą. Kartu atliktos apklausos parodė, kad ES piliečiai pritaria griežtų įmonių deramo patikrinimo reikalavimų išlaikymui, kurie užtikrintų, kad kuo daugiau įmonių būtų atsakingi už žmogaus teisių pažeidimus ir žalą aplinkai visoje savo veiklos grandinėje¹¹⁸. Tai dar išsamiau vertinti, kam iš tikrųjų teikiamas prioritetas ES politikoje ir teisėkūroje.

Pažymėtina, kad šis pokytis yra glaudžiai susijęs su skaitmeniniu suverenitetu. Vienas iš skaitmeninio suvereniteto tikslų yra didinti ES pajėgumus debesijos, puslaidininkių, dirbtinio intelekto, duomenų centrų, telekomunikacijų infrastruktūros ir kritinių išteklių srityse. Visi šie sektoriai tiesiogiai priklauso nuo sudėtingų tarptautinių tiekimo grandinių bei rangovų. Jei ES lygiagrečiai sušvelnina deramo patikrinimo reikalavimus būtent šių sudėtingų grandinių atžvilgiu, ji iš esmės sumažina teisių apsaugos garantijas vardan savo technologinio pranašumo, taip skatindama greitesnį skaitmeninio suvereniteto tikslų įgyvendinimą.

Šis ryšys matomas ir oficialioje retorikoje. Europos Taryba oficialiame pranešime apie galutinį „Omnibus I“ priėmimą tiesiogiai pagrindė šią reformą konkurencingumo tikslų bei autonomiškesnės sąjungos siekiu¹¹⁹. Kitaip tariant, reikalavimų verslui supaprastinimas yra siejamas su ES siekiu užsitikrinti savarankiškumą. Skaitmeninis suverenitetas paprastai pateikiamas kaip vertybėmis pagrįstas suverenitetas, t. y. kaip gebėjimas didinti technologinį pajėgumą neatsisakant žmogaus teisių. Tačiau „Omnibus I“ pavyzdys rodo,

¹¹⁶ Europos Parlamento ir Tarybos 2026 m. vasario 24 d. direktyvą (ES) 2026/470, kuria iš dalies keičiamos direktyvos 2006/43/EB, 2013/34/ES, (ES) 2022/2464 ir (ES) 2024/1760, kiek tai susiję su tam tikrais įmonių tvarumo atskaitomybės reikalavimais ir tam tikrais įmonių tvarumo išsamaus patikrinimo reikalavimais. OL L 2026/470, 2026.

¹¹⁷ RENGERVE, Helene (2025-10-13). *Changes to EU Law Will Undermine Corporate Accountability. Reduced Scope, Obstacles to Civil Liability Hollow Out Law's Effectiveness* [interaktyvus]. <https://www.hrw.org/news/2025/10/13/changes-to-eu-law-will-undermine-corporate-accountability>.

¹¹⁸ Ibid.

¹¹⁹ European Council (2026-02-24). *Council signs off simplification of sustainability reporting and due diligence requirements to boost EU competitiveness* [interaktyvus]. <https://www.consilium.europa.eu/en/press/press-releases/2026/02/24/council-signs-off-simplification-of-sustainability-reporting-and-due-diligence-requirements-to-boost-eu-competitiveness/>.

kad kilus konfliktui tarp sparčios plėtros ir žmogaus teisių apsaugos garantijų, prioritetas gali būti suteiktas verslo interesams bei konkurencingumui. Tai leidžia abejoti teiginiu, kad ES skaitmeninė autonomija visada grindžiama aukštesniais žmogaus teisių apsaugos standartais. Pažymėtina, kad didžioji dalis skaitmeninių technologijų ir jų veikimą užtikrinanti infrastruktūra yra beveik išimtinai privačių įmonių rankose. Nathalie A. Smuha, analizuodama privačiojo sektoriaus įtaką skaitmeninėje srityje, nurodo, kad didžiosios technologijų bendrovės daro reikšmingą įtaką skaitmeninėje erdvėje, todėl jos literatūroje net vadinamos „kvazisuverenėmis“. Ji taip pat pažymi, kad valstybės su šiomis įmonėmis bendrauja tarsi su atskirais valstybių vadovais, pateikdama pavyzdį, kad „OpenAI“ generalinis direktorius buvo pakviestas į keletą oficialių susitikimų su valstybių vadovais bei Europos Komisijos pirmininke¹²⁰. Natūralu, kad glaudus bendradarbiavimas su lyderiaujančiomis technologijų srityje įmonėmis ir ES noras perimti jų sėkmę gali turėti įtakos teisiniam reguliavimui.

Kitas žmogaus teisių apsaugos normų susilpninimo pavyzdys, susijęs su teisės aktu keitimu, yra vadinamasis Skaitmeninio sektoriaus bendrasis rinkinys, kuris nors dar nėra oficialiai priimtas, jau spėjo sukelti nerimą visuomenėje ir sulaukti kritikos¹²¹. Europos Komisija Skaitmeninio sektoriaus bendrąjį rinkinį oficialiai pristato kaip ES skaitmeninių normų techninį supaprastinimą, tačiau čia galima įžvelgti ir kitą šio reiškinio pusę. Siūlomi pakeitimai paliečia svarbiausius teisės aktus, reguliuojančius žmogaus teises skaitmeninėje erdvėje.

Reaguojant į šiuos pasiūlymus, „European Digital Rights“ paskelbė laišką, kuriame daugiau nei 130 organizacijų šiuos pakeitimus jau vadina „paslėptu stipriausių ES garantijų nuo skaitmeninių grėsmių griovimu“ ir „didžiausiu fundamentalių skaitmeninių teisių žlugimu ES istorijoje“. Jos prašo skubiai sustabdyti bandymus peržiūrėti BDAR, Dirbtinio intelekto aktą, Skaitmeninių rinkų aktą, Skaitmeninių paslaugų aktą bei kitus teisės aktus, reguliuojančius žmogaus pagrindinių teisių užtikrinimą skaitmeninėje erdvėje¹²². Kartu

¹²⁰ SMUHA, Nathalie A. Digital Sovereignty In The European Union: Five Challenges From A Normative Perspective. Iš: BARRETT, Gavin (red.); MÜLLER-GRAFF, Peter-Christian (red.); RAGEADE, Jean-Philippe (red.) ir kt. (2024). *European Sovereignty: The Legal Dimension*. Cham: Springer Cham. <https://doi.org/10.1007/978-3-031-71851-9>. p. 127-149. p. 136.

¹²¹ Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys), COM/2025/837 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0837>.

¹²² European Digital Rights (EDRi) (2025-11-13). *Forthcoming Digital Omnibus would mark point of no return* [interaktyvus]. <https://edri.org/our-work/forthcoming-digital-omnibus-would-mark-point-of-no-return/#:~:text=reform%20of%20the%20EU's%20digital,other%20core%20digital%20rights%20protection%20>

pažymėtina, kad Dirbtinio intelekto aktui peržiūrėti yra skirtas taip vadinamas Bendrasis skaitmeninės srities dokumentų rinkinys dėl dirbtinio intelekto, kurio tikslas yra supaprastinti Dirbtinio intelekto akto taikymą¹²³.

Toliau darbe apžvelgiami esminiai Skaitmeninio sektoriaus bendrojo rinkinio pasiūlymai. Vienas jų, tai asmens duomenų apibrėžties tikslinimas. Pakeitimuose numatyta, kad duomenys nėra laikomi asmeniniais konkretaus subjekto atžvilgiu, jei šis neturi priemonių asmeniui identifikuoti, net jei asmenys ir subjektai tokias galimybes turi¹²⁴. Manytina, kad šis pakeitimas yra ginčytinas, nes jis nukrypsta nuo nusistovėjusios ESTT praktikos. Pavyzdžiui, 2023 m. byloje *Gesamtverband Autoteile-Handel e.V. prieš Scania CV AB.*, teismas konstatavo, kad duomenys laikytini asmens duomenimis, jei jų gavėjas turi priemonių, leidžiančių identifikuoti fizinį asmenį, net jei perduodanti šalis tokios galimybės neturi¹²⁵. Taigi, Skaitmeninio sektoriaus bendrajame rinkinyje pateiktas susiaurintas asmens duomenų apibrėžimas faktiškai apriboja BDAR taikymo sritį ir didina apsaugos lygio mažėjimo riziką, nes, pavyzdžiui, tam tikros sekimo technologijos (slapukai, įrenginių identifikatoriai ir kt.) gali būti nebepriskiriamos asmens duomenų kategorijai ir pašalintos iš BDAR reguliavimo srities.

Kitas akivaizdus asmens duomenų apsaugos susilpninimo pavyzdys yra siūlymas nustatyti, kad asmens duomenų tvarkymas kuriant ir naudojant DI sistemas gali būti vykdomas remiantis teisėtu interesu, kuris yra numatytas BDAR 6 straipsnio 1 dalies f punkte¹²⁶. Šis pakeitimas numatomas siekiant paspartinti DI sistemų vystymą bei jų diegimą. Minėtas pakeitimas sudarytų prielaidas DI teikėjams beveik be didesnių apribojimų rinkti didelius kiekius vartotojų duomenų, o tai gali reikšmingai susilpninti jų teisinę apsaugą, kadangi DI sistemos nėra techniškai stabilios, nėra garantijų, kad tvarkymas „apmokant“ sistemas bus saugus, o asmens duomenys apsaugoti.

¹²³ Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo dėl suderintų dirbtinio intelekto taisyklių įgyvendinimo supaprastinimo iš dalies keičiami Reglamentai (ES) 2024/1689 ir (ES) 2018/1139, (Bendrasis skaitmeninės srities dokumentų rinkinys dėl dirbtinio intelekto)* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0836>.

¹²⁴ Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys), COM/2025/837 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0837>.

¹²⁵ *Gesamtverband Autoteile-Handel e.V. prieš Scania CV AB* [ESTT], Nr. C-319/22, [2023-11-09]. ECLI:EU:C:2023:837.

¹²⁶ Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys), COM/2025/837 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0837>.

Kitas siūlomas pakeitimas tai BDAR 15 straipsnyje numatyta duomenų subjekto teisė susipažinti su duomenimis apribojimas. Nors juo siekiama sumažinti piktnaudžiavimą šia teise, praktiškai taip ribojama asmens kontrolę savo duomenų atžvilgiu. Taip pat pastebimas pakeitimas, susijęs su BDAR 22 straipsniu, kuriuo išplečiamos automatizuoto sprendimų priėmimo galimybės bei kiti pakeitimai¹²⁷. Taigi akivaizdu, kad tai itin plataus masto pakeitimų projektas, kuriuo mažinami grėžti teisių apsaugos standartai dėl palankesnių sąlygų įmonėms. Manytina, kad priėmus Skaitmeninio sektoriaus bendrąjį rinkinį, iš esmės pasikeis pakeis skaitmeninės aplinkos reguliavimas, o tai neišvengiamai turės įtakos žmogaus teisių apsaugai.

N. A. Smuha pažymi, kad ES skatina valstybes nares skaitmeninti ir automatizuoti viešąjį sektorių. Ji kritikuoja tokį sprendimą, nurodyma, kad mokslininkai vis dažniau nustato automatizuotų sprendimų priėmimo sistemų aktyvaus naudojimo neigiamas pasekmes, ypač viešajame sektoriuje. Tai apima diskriminacijos, duomenų manipuliavimo, masinio sekimo ir privatumo pažeidimų riziką¹²⁸.

Susirūpinimą dėl galimos disproporcijos tarp technologijų plėtros ir žmogaus teisių užtikrinimo išreiškia ir teisės mokslininkai. Analizuodamas valstybių pasirašytą Berlyno deklaraciją dėl skaitmeninio suvereniteto, ES duomenų ir skaitmeninio suvereniteto srities tyrėjas Michalas Czerniawskis išskiria keletą šio dokumento esminių trūkumų. Jis pabrėžia, kad šioje deklaracijoje nėra aiškiai įtvirtintas pagrindinių teisių centrinis vaidmuo, nepaisant jų esminės svarbos ES teisinei sistemai. Pasak tyrėjo, Berlyno deklaracijoje demokratinių vertybių paminėjimas yra labiau deklaratyvaus pobūdžio, ir nėra numatyta konkrečių joms įgyvendinti skirtų mechanizmų, o tai gali kelti abejonių dėl šių vertybių realios reikšmės formuojant skaitmeninę ES politiką. Galima manyti, kad skaitmeninis suverenitetas iš esmės suprantamas per technologijų plėtros ir konkurencingumo didinimo prizmę, o žmogaus teisių apsauga lieka antraeilė¹²⁹. Todėl čia pastebimas normatyvinis disbalansas, kai žmogaus teisės įtvirtinamos tik retorikos lygmenyje, nesuteikiant joms pakankamo institucinio ir teisinio užtikrinimo. Tai kelia riziką, kad skaitmeninis

¹²⁷ Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys), COM/2025/837 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0837>.

¹²⁸ SMUHA, Nathalie A. Digital Sovereignty In The European Union: Five Challenges From A Normative Perspective. Iš: BARRETT, Gavin (red.); MÜLLER-GRAFF, Peter-Christian (red.); RAGEADE, Jean-Philippe (red.) ir kt. (2024). *European Sovereignty: The Legal Dimension*. Cham: Springer Cham. <https://doi.org/10.1007/978-3-031-71851-9>. p. 127-149. p. 142.

¹²⁹ CZERNIAWSKI, Michal (2025-12-03). *EU's Digital Sovereignty and the Rights-Based Imperative* [interaktyvus]. <https://verfassungsblog.de/digital-sovereignty-and-the-rights/>.

suverenitetas taps tik techniniu ir ekonominiu projektu, neintegruotu į ES demokratinių bei konstitucinių vertybių sistemą.

M. Czerniawski pabrėžia, kad didesnis dėmesys žmogaus teisėms suteiktų papildomą pranašumą įgyvendinant skaitmeninį suverenitetą. Tai, anot jo, padėtų ES pagrįsti savo reikalavimus ne tik ekonominių vertybių ir saugumo perspektyva, bet ir remiantis visuotinai pripažintomis vertybėmis¹³⁰. Iš tiesų, orientavimasis į tarptautiniu mastu pripažintus žmogaus teisių standartus gali sustiprinti teisinį pagrįstumą ES reguliavimo mechanizmų, ypač jei jie bus taikomi už ES ribų. Taip pat sustiprėtų ir ES pozicijos globaliame skaitmeninės erdvės valdyme.

Tad galima daryti išvadą, kad siekiant įgyvendinti skaitmeninį suverenitetą, būtina skirti pagrindinį dėmesį žmogaus teisių apsaugos ir užtikrinimo aspektams, nes, priešingu atveju, skaitmeninio suvereniteto politikos nepavyks tinkamai integruoti į ES teisinę sistemą. Neįtvirtinus aiškių užtikrinimo mechanizmų, skaitmeninio suvereniteto politika išlieka orientuota tik į technologijų plėtrą ir nėra visiškai suderinama su ES demokratinėmis vertybėmis. ES svarbu išlaikyti maksimalias žmogaus teisių garantijas, parodant reguliavimo pavyzdį ir kitoms valstybėms. Atsižvelgiant į tai, kad po BDAR priėmimo buvo pasiektas vadinamasis „Briuselio efektas“, visos ES rinkoje veikiančios įmonės prisitaikė prie šių normų ir išplėtė jų veikimą tarptautiniu mastu. Todėl ES nėra būtinybės silpninti ar praktiškai atsisakyti griežtų žmogaus teisių apsaugos standartų, priešingai, esamus trūkumus reikėtų aiškinti per žmogaus teisių apsaugos ir jų užtikrinimo bei įgyvendinimo prizmę.

3.2. Skaitmeninio suvereniteto piktnaudžiavimai: cenzūra ir masinė stebėseną.

Kuriant skaitmeninį suverenitetą priimti teisės aktai padėjo apsaugoti įvairias žmogaus teises, visų pirma teisę į asmens privataus gyvenimo gerbimą, teisę į žodžio laisvę, teisę į asmens duomenų apsaugą ir teisę į veiksmingą teisių gynimą. Tačiau, vis dar pastebimi tam tikri trūkumai, kurie sudaro sąlygas galimiems minėtų teisių pažeidimams. A. Chanderis ir H. Sun, analizuodami skaitmeninio suvereniteto dvejopumą, nurodo, kad jis yra tuo pačiu metu būtinas ir pavojingas. Viena vertus, jis būtinas tam, kad įprasti įstatymai mus lydėtų skaitmeninėje erdvėje. Kita vertus, skaitmeninis suverenitetas gali kelti grėsmę, nes

¹³⁰ CZERNIAWSKI, Michal (2025-12-03). *EU's Digital Sovereignty and the Rights-Based Imperative* [interaktyvus]. <https://verfassungsblog.de/digital-sovereignty-and-the-rights/>.

interneto reguliavimas suteikia valstybėms dar daugiau galių įsiterpti į žmonių privatų gyvenimą¹³¹.

Matytina, kad skaitmeninėje srityje susiduriama su atvejais, kai tenka rinktis tarp griežtos duomenų apsaugos ir valstybės interesų užtikrinimo, siekiant kontroliuoti šią sritį. Šiame kontekste labai svarbi yra 2024 m. ESTT byla *La Quadrature du Net ir kt. prieš Premier ministre ir Ministère de la Culture*. Šioje byloje keliamas klausimas, ar galima saugoti IP adresus ir suteikti prieigą prie jų valstybės institucijoms, siekiant tirti nesunkius teisės pažeidimus, visų pirma susijusius su autorių teisėmis¹³². Ginčytinas tapo Europos Parlamento ir Tarybos 2002 m. liepos 12 d. direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (Toliau – Direktyva dėl privatumo ir elektroninių ryšių) taikymas, kurioje 5 straipsnyje įtvirtintas pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai teikiamas elektroninių ryšių paslaugas, konfidencialumas. Tačiau Direktyvos dėl privatumo ir elektroninių ryšių 15 straipsnio 1 dalys nurodo, kad valstybės narės gali patvirtinti teises priemones, ribojančias 5 straipsnyje nustatytų teisių ir pareigų taikymą jeigu toks ribojimas „<...> yra būtina, tinkama ir adekvati demokratinės visuomenės priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą <...>“. Ten pat nurodyta, kad „valstybės narės gali, *inter alia*, patvirtinti teises priemones, leidžiančias ribotą laikotarpį saugoti duomenis, remiantis aukščiau nurodytais motyvais, tačiau visos priemonės turi atitikti bendruosius ES teisės principus <...>“¹³³. Remiantis šia nuostata Prancūzijoje buvo sukurta „HADOPI“ sistema, skirta kovoti su neteisėtu kūrinių, kuriems taikomos autorių teisių apsauga, platinimu internete. Teisių turėtojai rinko ir vėliau perduodavo valstybinei institucijai informaciją apie įtartinus IP adresus. Gavusi šiuos duomenis, „HADOPI“ galėjo prašyti interneto paslaugų teikėjų pateikti duomenis apie vartotojo tapatybę, kad galėtų jiems išsiųsti įspėjimus. Jei pažeidimas kartojosi, byla galėjo

¹³¹ CHANDER, Anupam ir SUN, Haochen. Digital Sovereignty as Double-Edged Sword. Iš: CHANDER, Anupam (red.) ir SUN, Haochen (red.) (2023). *Data Sovereignty. From the Digital Silk Road to the Return of the State*. New York: Oxford University Press, p.72-88. DOI: 10.1093/oso/9780197582794.001.0001, p. 88.

¹³² *La Quadrature du Net ir kt. prieš Premier ministre ir Ministère de la Culture* [ESTT], Nr. C-470/21, [2024-04-30]. ECLI:EU:C:2024:370.

¹³³ Europos Parlamento ir Tarybos 2002 m. liepos 12 d. direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OL, L 201, 2002, p. 37-47.

būti perduota net teismui¹³⁴. Būtent šios sistemos teisėtumas ir suderinamumas su Chartijos 7, 8 ir 11 straipsniais tapo bylos nagrinėjimo pagrindu.

Analizuojant šią bylą, galima pastebėti, kaip sušvelnėjo ESTT pozicija. Pavyzdžiui, byloje *Tele2 Sverige AB prieš Post- och telestyrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.* ESTT nurodė, kad tik kova su sunkiais nusikaltimais gali pateisinti rimtą pagrindinių teisių ribojimą, o bendras ir nediferencijuotas srauto bei buvimo vietos duomenų saugojimas negali būti pripažinti būtinais nusikaltimų prevencijos tikslais, t. y. pats savaime nesuderinamas su Chartijos 7, 8 straipsniais¹³⁵. Tokia pati išvada padaryta 2020 m. byloje *La Quadrature du Net ir kt. prieš Premier ministre ir kt.*, kurioje ESTT papildomai pažymėjo, kad IP adresai leidžia atsekti interneto vartotojo skaitmeninius pėdsakus ir, atitinkamai, daryti tiksliai išvadas apie jo privatų gyvenimą; todėl bendras nediferencijuotas IP adresų saugojimas yra leistinas tik kovai su sunkiais nusikaltimais¹³⁶. Tačiau minėtoje 2024 m. byloje ESTT atsisakė savo ankstesnės pozicijos ir nurodė, kad IP adresų saugojimas gali būti leidžiamas ir kovai su nesunkiais teisės pažeidimais, jei nacionaliniai teisės aktai ir techninė saugojimo sistema realiai pašalina galimybę iš duomenų daryti tiksliai išvadas apie asmens privatų gyvenimą. ESTT suformulavo tam tikrus kriterijus dėl tokių duomenų saugojimo ir pareikalavo, kad skirtingos duomenų kategorijos, t. y. IP adresai, civilinės tapatybės duomenys, kiti nei IP adresai srauto duomenys ir įvairūs vietos nustatymo duomenys, būtų saugomi visiškai atskirai, be to, šis atskyrimas turi būti techniškai veiksmingas, patikimas ir saugus. Taip pat ESTT nurodė, kad „<...> šio veiksmingo atskyrimo patikimumą turi reguliariai tikrinti kita valdžios institucija nei ta, kuri siekia gauti prieigą prie elektroninių ryšių paslaugų teikėjų saugomų asmens duomenų“¹³⁷. Būtent čia kyla pagrindinis klausimas dėl pagrindinių teisių apsaugos. Formaliai ESTT siekia užtikrinti asmenų privatumą, nes leidžia saugoti asmenį identifikuoti leidžiančius duomenis tik esant griežtoms techninėms garantijoms. Kita vertus, leistino valstybės teisių pribojimo sritis plečiasi, kadangi IP adresų saugojimas dabar leidžiamas ne tik sunkių nusikaltimų atvejais. Šią nuomonę palaiko ir teisės mokslininkai, nurodydami, kad ESTT tokiu būdu sukūrė modelį, kuriame teisių apsauga priklauso nuo to, kiek techniškai gerai organizuotas duomenų saugojimas. Kartu reiškiamos

¹³⁴ *La Quadrature du Net and Others v Premier ministre and Ministère de la Culture* [ESTT], Nr. C-470/21, [2024-04-30]. ECLI:EU:C:2024:370.

¹³⁵ *Tele2 Sverige AB prieš Post- och telestyrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.* [ESTT], Nr. C-203/15, [2016-12-21]. ECLI:EU:C:2016:970.

¹³⁶ *La Quadrature du Net ir kt. prieš Premier ministre ir kt.* [ESTT], Nr. C-511/18, [2020-10-06]. ECLI:EU:C:2020:791.

¹³⁷ *La Quadrature du Net ir kt. prieš Premier ministre ir Ministère de la Culture* [ESTT], Nr. C-470/21, [2024-04-30]. ECLI:EU:C:2024:370.

abejonės, ar tokį aiškų duomenų atskyrimą iš tiesų galima užtikrinti praktikoje. Taip pat kyla klausimas, ką daryti tuo atveju, jei dėl saugumo pažeidimo taps įmanoma gauti prieigą prie kelių atskirai saugomų duomenų kategorijų¹³⁸.

ESTT taip pat nusprendė, kad „HADOPI“ prieiga prie duomenų apie vartotojo tapatybę pagal IP adresą iš esmės nelaikytina rimtu pagrindinių teisių ribojimu. Teismo vertinimu, tokia prieiga savaime nesuteikia išsamaus vaizdo apie asmens privatų gyvenimą¹³⁹. Šią poziciją kritikai taip pat vertina skeptiškai, pažymėdami, kad net vienas duomenų įrašas konkrečiame kontekste gali atskleisti privačią informaciją apie asmenį¹⁴⁰. Kitaip tariant, pavojus žmogaus teisėms priklauso ne tik nuo duomenų tipo, bet ir nuo to, kaip šie duomenys naudojami ir su kuo jie palyginami. Panašią kritiką išsako ir EDRI, kuri, remdamasi EŽTT praktika, nurodo, kad teisėsaugos institucijos gali jau turėti papildomos informacijos, kuri padėtų atskleisti asmens privataus gyvenimo detales, todėl šis teisių ribojimas turėtų būti laikomas rimtu¹⁴¹. Taip, 2018 m. *Benedik prieš Slovėniją* byloje EŽTT pažymėjo, kad policijos prašomi duomenys, t. y. abonento vardas ir adresas, kartu su anksčiau egzistavusia internete informacija gali atskleisti daug informacijos apie asmens veiklą internete, įskaitant konfidencialias detales asmens interesus, įsitikinimus ir privatų gyvenimą¹⁴².

Tai tiesiogiai susiję su ES formuojama skaitmeninio suvereniteto politika. Viena vertus, skaitmeninis suverenitetas gali būti suprantamas kaip ES vertybių ir nepriklausomybės apsauga. Kita vertus, jis gali reikšti valstybės kontrolės stiprinimą vartotojų ir jų komunikacijos atžvilgiu. Būtent antrasis išskirtas pavojus 2024 m. byloje *La Quadrature du Net ir kt. prieš Premier ministre ir Ministère de la Culture* byloje gali kelti didžiausią nerimą. EDRI nurodo, kad metaduomenys yra šiuolaikinės valstybinės stebėjimo sistemos pagrindas. Dėl šios priežasties, duomenų saugojimo klausimas

¹³⁸ DEKHUIJZEN, Elisabeth (2025). La Quadrature du Net II and Data Retention under Article 15(1) ePrivacy Directive: CJEU Walks a Tightrope on IP Addresses Retention and Access for Public Authorities in NonSerious Crime. *European Data Protection Law Review*, 11(2), 253-258 [interaktyvus]. https://cris.maastrichtuniversity.nl/ws/portalfiles/portal/280951111/Dekhuijzen-2025-La-Quadrature-du-Net_II-and-.pdf. p. 255-256.

¹³⁹ *La Quadrature du Net ir kt. prieš Premier ministre ir Ministère de la Culture* [ESTT], Nr. C-470/21, [2024-04-30]. ECLI:EU:C:2024:370.

¹⁴⁰ DEKHUIJZEN, Elisabeth (2025). La Quadrature du Net II and Data Retention under Article 15(1) ePrivacy Directive: CJEU Walks a Tightrope on IP Addresses Retention and Access for Public Authorities in NonSerious Crime. *European Data Protection Law Review*, 11(2), 253-258 [interaktyvus]. https://cris.maastrichtuniversity.nl/ws/portalfiles/portal/280951111/Dekhuijzen-2025-La-Quadrature-du-Net_II-and-.pdf. p. 257.

¹⁴¹ European Digital Rights (EDRi) (2025-04-03). *CJEU saved the HADOPI: what implications for the future of data retention in the EU?* [interaktyvus]. <https://edri.org/our-work/cjeu-saved-the-hadopi-what-implications-for-the-future-of-data-retention-in-the-eu/>.

¹⁴² *Benedik prieš Slovėniją* [EŽTT], Nr. 62357/14, [2018-04-24]. ECLI:CE:ECHR:2018:0424JUD006235714.

artimiausiais metais išliks kaip viena iš esminių skaitmeninių teisių problemų¹⁴³. Tad ši byla iš esmės keičia tolesnį pagrindinių teisių apsaugos lygį. Jei anksčiau ESTT požiūris buvo labiau ginantis ir grindžiamas tuo, kad masinis IP adresų saugojimas yra leistinas tik išimtiniais atvejais, dabar atsiranda švelnesnė konstrukcija: saugojimas galimas ir dėl nesunkių teisės pažeidimų, jei valstybė sukurs technines garantijas. Toks modelis yra palankesnis valstybėms, nes leidžia plėsti skaitmeninį teisėsaugos priemonių taikymą, formaliai neatsisakant žmogaus teisių apsaugos. Tačiau kyla pavojus, kad priemonės, kurios anksčiau buvo laikomos išimtinėmis, palaipsniui taps įprastu skaitmeninės erdvės valdymo įrankiu. Tad, šiame kontekste ES turėtų išlaikyti balansą ir kurti skaitmeninę autonomiją ne silpninant žmogaus teisių apsaugą, o jas stiprinant.

Bandymas sušvelninti reguliavimą matomas ir analizuojant anksčiau minėtą Skaitmeninio sektoriaus bendrąjį rinkinį, kuriame yra pasiūlymas pakeisti Direktyvos dėl privatumo ir elektroninių ryšių 5 straipsnio 3 dalį, kuri atlieka itin svarbų vaidmenį, nes būtent joje nustatyta, kad negalima rinkti vartotojo saugoma įrenginyje informaciją be jo sutikimo (pavyzdžiui, naudojant slapukus). Taigi ši nuostata nurodo, kada galima pereiga prie asmeninių ir neasmeninių duomenų, o tik po šios informacijos surinkimo pradeda veikti, pavyzdžiui BDAR, kuriame nustatyta, kaip reikia tvarkyti gautus asmeninius duomenis.

Tačiau dabar siūloma šį griežtą mechanizmą keisti, nustatant naujus duomenų rinkimo ir tvarkymo pagrindus be asmens sutikimo (pavyzdžiui, viešojo intereso ginimas, saugumo tikslais ir kt). EDRI nurodo, kad toks pakeitimas paverčia aiškią taisyklę labiau leidžiančia sistema. Sutikimas ilgą laiką buvo įrenginių privatumo apsaugos pagrindas, todėl jo papildymas plačiomis išimtimis, suteikia įmonėms žymiai daugiau galimybių stebėti vartotojų elgesį bei analizuoti paslaugų naudojimą tiesiogiai jų įrenginiuose. Be to, tai silpnina tradicinę skaitmeninių komunikacijų konfidencialumo apsaugą, nes daugelis veiksmų, kuriems anksčiau buvo būtinas sutikimas, dabar galės būti atliekami be jo¹⁴⁴.

Pagrindinių teisių požiūriu tokie pokyčiai silpnina Chartijos 7 ir 8 straipsniuose įtvirtintą apsaugą. Mažėja sutikimo, kaip pagrindinės garantijos, reikšmė, tad išauga neskaidraus ir slapto duomenų rinkimo rizika. Manytina, kad ES neturėtų atsisakyti griežtų

¹⁴³ European Digital Rights (EDRi) (2025-04-03). *CJEU saved the HADOPI: what implications for the future of data retention in the EU?* [interaktyvus]. <https://edri.org/our-work/cjeu-saved-the-hadopi-what-implications-for-the-future-of-data-retention-in-the-eu/>.

¹⁴⁴ European Digital Rights (EDRi) (2025-11-19). *Why the Digital Omnibus puts GDPR and ePrivacy at risk* [interaktyvus]. https://edri.org/wp-content/uploads/2025/11/202511-Eexplaining-GDPR_eprivacy-Digital-Omnibus.pdf.

garantijų, nes toks reglamentavimo sušvelninimas sudaro galimybę piktnaudžiauti teise, kas pastiebiama ir šiomis dienomis.

Pavyzdžiui, Nepriklausomos organizacijos 2021 m. atliko tyrimą, kurio metu paaiškėjo, kad daugelis šalių, įskaitant ES valstybes nares, įsigijo ir naudojo kompanijos NSO Group sukurtas šnipinėjimo programas „Pegasus“ ir „Predator“¹⁴⁵. Tai sukėlė didelį skandalą, todėl 2023 m. Europos Parlamentas pagal SEVS 226 straipsnį įsteigė tyrimo komisiją PEGA. Oficialioje Europos Parlamento 2023 m. ataskaitoje dėl tyrimo dėl įtariamų pažeidimų ir netinkamo administravimo taikant Sąjungos teisę, susijusių su „Pegasus“ ir jam lygiaverčių stebėjimo programų naudojimu (toliau – PEGA ataskaita) patvirtinamas šių programų naudojimas. Ataskaitoje nurodoma, kad valstybėse narėse šnipinėjimo programinė įranga buvo taikoma ne kaip išimtinis įrankis kovai su rimtomis grėsmėmis, o kaip politinės kontrolės priemonė bei spaudimo žurnalistams, opozicijai ir valdžios kritikams įrankis¹⁴⁶. Konkrečiai PEGA ataskaitoje minimos tokios šalys, kaip Ispanija, Lenkija, Graikija, Vengrija, Kipras. Labiausiai kritikuojama yra Lenkija, kurioje nacionalinė teisinė sistema buvo pertvarkyta taip, kad iš esmės neteisėtas stebėjimas atrodytų priimtinas vidaus teisės požiūriu¹⁴⁷. Tokios praktikos yra tiesiogiai siejamos su demokratijos, privatumo, saviraiškos laisvės, žiniasklaidos laisvės ir teisės į veiksmingą gynybą pažeidimais. Tačiau, PEGA ataskaitoje nurodoma, kad daugelis valstybių atsisakė pateikti išsamią informaciją, remdamosi konfidencialumu arba nacionaliniu saugumu. Reaguodama į tai PEGA primena nusistovėjusią ESTT poziciją, kad vien tik nuoroda į nacionalinį saugumą nereiškia, jog ES teisė netaikoma, ir tai nėra pakankamas pagrindas pagrindinių teisių apribojimui pateisinti¹⁴⁸.

Nors fiksuojami masiniai galimi pagrindinių teisių pažeidimai, PEGA ataskaitoje nurodoma, kad Europos Komisija neparodė pakankamo sąmoningumo ir susirūpinimo dėl šnipinėjimo programinės įrangos keliamų grėsmių. Visgi, pažymėtina, kad nors Europos Komisija formaliai remiasi įgaliojimų trūkumu nacionalinio saugumo srityje, ji pripažįsta svarbią taisyklę, kad nacionalinis saugumas neturi tapti neribota išimtimi iš ES teisės aktų ir sutarčių ar piktnaudžiavimo sritimi¹⁴⁹.

¹⁴⁵ Article19 (2024-09-03). *EU: Civil society demands action against spyware threats* [interaktyvus]. <https://www.article19.org/resources/eu-civil-society-demands-action-against-spyware-threats/>.

¹⁴⁶ Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (2023-05-22). *Report A9-0189/2023 of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI))* [interaktyvus]. https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

¹⁴⁷ *Ibid.*

¹⁴⁸ *Ibid.*

¹⁴⁹ *Ibid.*

Pastebėtina, kad PEGA Ataskaitos pranešėja ir buvusi Europos Parlamento narė, Sophie In't Veld nurodo, jog ES aktyviai remiama šnipinėjimo programinės įrangos rinka¹⁵⁰. Nors oficialios ES institucijos stengiasi vengti šios temos, žiniasklaidoje apie tai aktyviai diskutuojama. Pavyzdžiui, yra duomenų, kad ES įsikūrusios įmonės gamina šnipinėjimo programinę įrangą ir vykdo aktyvų jos eksportą¹⁵¹. Nors toks eksportas yra ribojamas, PEGA ataskaitoje pažymima, kad šie apribojimai taikomi silpnai ir nenuosekliai¹⁵².

Pažymėtina, kad po PEGA ataskaitos 2023 m. Europos Parlamentas priėmė rekomendacijas, raginančias Europos Komisiją griežčiau reguliuoti šnipinėjimo programinės įrangos naudojimą, gamybą ir pardavimą. Taip pat raginama atidžiau stebėti, kaip laikomasi galiojančių įstatymų, ir aiškiai apibrėžti sąvoką „nacionalinis saugumas“¹⁵³. Tačiau Europos Komisija teigia, kad valstybių narių valdžios institucijos pačios turi užtikrinti ES įstatymų ir standartų laikymąsi¹⁵⁴. Toks Europos Komisijos požiūris rodo jos pasyvumą, nes neaišku, kaip galima patikėti atsakomybės klausimą pačiai valstybei narei, kuri pažeidžia ES teisę.

Manytina, kad PEGA tyrimas leidžia daryti gilesnę išvadą, jog masinio sekimo ir piktnaudžiavimo teise problema yra tiesioginė skaitmeninio suvereniteto siekio pasekmė. Nors formaliai skaitmeninis suverenitetas grindžiamas pagrindinių teisių apsauga, praktikoje matytina, kad valstybės įgyja vis platesnius įgaliojimus kontroliuoti skaitmeninę erdvę. Panašiai teigia A. Chanderis ir H. Sun. Analizuodami skaitmeninio suvereniteto padarinius, jie prieina prie išvados, kad panašiai kaip būtina kruopščiai reguliuoti skaitmeninių korporacijų galią, taip pat būtina kontroliuoti ir pačių valstybių galią¹⁵⁵.

Pirmiausia, skaitmeninį suverenitetą įgyvendina pačios valstybės narės. Kol nėra griežtų viršvalstybinių apribojimų bei realios kontrolės, šis procesas neišvengiamai kels

¹⁵⁰ IN'T VELD, Sophie (2025-01-31). *An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?* [interaktyvus]. <https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/>.

¹⁵¹ ROUSSI, Antoaneta (2023-11-25). *How Europe became the Wild West of spyware* [interaktyvus]. <https://www.politico.eu/article/how-europe-became-wild-west-spyware/>.

¹⁵² Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (2023-05-22). *Report A9-0189/2023 of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI))* [interaktyvus]. https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

¹⁵³ European Parliament (2024-01-23). *European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)) (C/2024/494)* [interaktyvus]. <https://eur-lex.europa.eu/eli/C/2024/494/oj/eng/pdf>.

¹⁵⁴ ROUSSI, Antoaneta (2023-11-25). *How Europe became the Wild West of spyware* [interaktyvus]. <https://www.politico.eu/article/how-europe-became-wild-west-spyware/>.

¹⁵⁵ CHANDER, Anupam ir SUN, Haochen. *Digital Sovereignty as Double-Edged Sword*. Iš: CHANDER, Anupam (red.) ir SUN, Haochen (red.) (2023). *Data Sovereignty. From the Digital Silk Road to the Return of the State*. New York: Oxford University Press, p.72-88. DOI: 10.1093/oso/9780197582794.001.0001, p. 88.

pavojų žmogaus teisėms. Kontrolę gali vykdyti ir teismai, tačiau šnipinėjimo sistemos jų taikiniams yra nepastebimos, o jei asmuo nežino apie savo teisių pažeidimą, jis negali jų veiksmingai apginti. Iš to darytina išvada, kad kol nebus priimtas aiškus įstatymas dėl šnipinėjimo programinės įrangos draudimo, piktnaudžiavimo atvejų tik daugės.

Taip pat šiuo metu aktyviai svarstomas pasiūlymas priimti reglamentą, kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės. Šis dokumentas yra žinomas kaip „Chat Control“¹⁵⁶. Juo siekiama įvesti internetinių paslaugų teikėjams pareigą pasitelkiant automatinio nustatymo technologijas, nustatyti, pranešti ir pašalinti medžiagą, susijusią su seksualine prievarta prieš vaikus, nuskaitant vartotojų komunikacijas, išskaitant asmenų susirašinėjimus, kurie apsaugoti išsistinių šifravimų (angl. end-to-end encryption).

Europos duomenų apsaugos valdyba (toliau – EDAV) ir Europos duomenų apsaugos priežiūros pareigūnas 2022 m. bendroje nuomonėje nurodė, kad siūlomos priemonės pažeidžia vartotojų pagrindines teises, įskaitant teisę į privatų gyvenimą, konfidencialumą, asmens duomenų apsaugą ir saviraiškos laisvę. Be to, nuomonėje pabrėžiama, kad tokie apribojimai turi atitikti Chartijos 52 straipsnio 1 dalies reikalavimus, ir išreiškiama rimtų abejonų dėl reglamento proporcingumo¹⁵⁷.

Europos Komisijos Teisės tarnyba 2023 m. balandžio 26 d. išvadose pažymėjo, kad privalomas komunikacijos skenavimas pažeidžia Chartijos 7 ir 8 straipsniuose įtvirtintas teises ir turi būti vertinamas atsižvelgiant į ESTT praktiką, kuri draudžiančią bendrą ir nediferencijuotą duomenų rinkimą. ES Taryboje vis nepavyksta pasiekti kvalifikuotos daugumos, todėl derybos dėl šio reglamento tęsiasi kelerius metus. Pavyzdžiui, Prancūzija, Ispanija, Italija, Lietuva bei kitos šalys pasisako už privalomo komunikacijų skenavimą, pabrėždamos būtinybę stiprinti kovą su vaikų prievarta internete. Tačiau Nyderlandai, Austrija, Vokietija ir kitos šalys pasisako prieš šio įstatymo priėmimą, nes jo dabartinė redakcija gali pažeisti nusistovėjusią ESTT praktiką, pagal kurią, kaip jau buvo minėta, draudžiama vykdyti stebėseną per bendrą ir nediferencijuotą duomenų rinkimą¹⁵⁸.

Analizuojant galias galimybes, kurias skaitmeninis suverenitetas suteikia valstybėms, galima paminėti ir 2019 m. ESTT bylą *Eva Glawischnig-Piesczek prieš*

¹⁵⁶ Europos Komisija (2022-05-11). *Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės*, COM/2022/209 final [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM%3A2022%3A209%3AFIN>.

¹⁵⁷ Europos duomenų apsaugos valdyba (2022-07-28). *EDAV-EDAPP Bendra nuomonė 4/2022 dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės* [interaktyvus]. https://www.edpb.europa.eu/system/files/2023-02/edpb_edps_jointopinion_202204_csam_lt.pdf.

¹⁵⁸ European Digital Rights (EDRi) (2025-01-08). *CSA Regulation Document Pool* [interaktyvus]. <https://edri.org/our-work/csa-regulation-document-pool/>.

Facebook Ireland Limited. Austrijos teismas paprašė priimti prejudicinį sprendimą byloje dėl vartotojo įžeidžiančio komentaro apie viešą asmenį, kuris buvo paskelbtas „Facebook“ platformoje, pašalinimo. ESTT konstatavo, kad nacionalinis teismas gali įpareigoti „Facebook“, kuri yra prieglobos paslaugų teikėja, panaikinti informaciją, kurią jis saugo ir kurios turinys tapatus prieš tai neteisėta pripažintos informacijos turiniui. Be to, ESTT nurodė, kad taip pat galima įpareigoti prieglobos paslaugų teikėją panaikinti tokią informaciją arba užblokuoti prieigą prie jos pasaulio mastu pagal atitinkamą tarptautinę teisę¹⁵⁹. Toks sprendimas gali būti vertinamas dviprasmiškai. Viena vertus, taip ginama garbė ir orumas (apsaugoti Chartijos 1 straipsniu) ne tik nacionaliniu, bet ir tarptautiniu lygmeniu. Kita vertus, išreiškiami susirūpinimai, kad toks reguliavimas gali pažeisti teisę į saviraiškos laisvę (Chartijos 11 straipsnis). A. Chanderis ir H. Sun teigia, kad reikalavimas tarptautiniu mastu iš „Facebook“ pašalinti tapataus turinio įrašus, matyt, reikalaus automatizuotų sistemų naudojimo, kurios, tikėtina, gali padaryti daug klaidų¹⁶⁰. Taip gali būti pašalintas ir teisėtas turinys, pavyzdžiui, minint šią teismo bylą. Be to, jie pažymi, kad galimybė priimti sprendimą dėl visuotinio pašalinimo, ypač kritikos (pagrįstos ar ne) politikui kontekste, tik paskatins kitas valstybes kelti panašius reikalavimus. Todėl manytina, kad galiojantys reglamentavimas gali apsunkinti politikų kritiką dėl baimės, kad jie gali kreiptis į teismą¹⁶¹. T. Pajuste pastebi, kad valstybės gali riboti politinį turinį, cenzūruoti opoziciją arba skleisti dezinformaciją siekdamas manipuliuoti viešąja nuomone. Be to, valstybės kontroliuojamas sekimas ir duomenų rinkimas gali įbauginti rinkėjus, ypač tuos, kurie reiškia nepritariančią požiūrį. Tai sukelia atgrasomąjį poveikį dalyvavimui politiniame gyvenime, kas gali pakenkti rinkimų teisingumui ir skaidrumui bei sumažinti visuomenės pasitikėjimą demokratiniu procesu¹⁶².

Apibendrinant galima teigti, kad aptarti pavyzdžiai atskleidžia esminę problemą: ji slypi ne pačiame valstybių siekyje užtikrinti skaitmeninį suverenitetą, o jo įgyvendinamo būduose. Jei skaitmeninis suverenitetas yra suprantamas pirmiausia kaip galimybė kontroliuoti vartotojus, gauti prieigą prie jų komunikacijos ir kaupti duomenis, jis nutolsta

¹⁵⁹ *Eva Glawischnig-Piesczek prieš Facebook Ireland Limited* [ESTT], Nr. C-18/18, [2019-10-03]. ECLI:EU:C:2019:821.

¹⁶⁰ CHANDER, Anupam ir SUN, Haochen. Digital Sovereignty as Double-Edged Sword. Iš: CHANDER, Anupam (red.) ir SUN, Haochen (red.) (2023). *Data Sovereignty. From the Digital Silk Road to the Return of the State*. New York: Oxford University Press, p.72-88. DOI: 10.1093/oso/9780197582794.001.0001, p. 79.

¹⁶¹ *Ibid.*, p. 79.

¹⁶² PAJUSTE, Tiina (2025). Digital Sovereignty and Human Rights: Balancing Security and Freedom. *Working paper: Technological change and international law: ESIL annual conference, Vilnius, 5-6 September 2024*, p. 78-84 [interaktyvus]. https://www.researchgate.net/publication/396975294_Digital_Sovereignty_and_Human_Rights_Balancing_Security_and_Freedom. p. 82.

nuo savo pradinės idėjos ir tampa per didelės kontrolės įrankiu. Tada tokie argumentai, kaip, pavyzdžiui, saugumas, vaikų apsauga ar kova su nusikalstamumu, palaipsniui pradeda pateisinti vis platesnio masto stebėjimo priemones. Taip ištrinama riba tarp tikslinio pagrindinių teisių ribojimo ir masinio stebėjimo. Todėl pavojus žmogaus teisėms kyla ne tik dėl pavienių piktnaudžiavimo atvejų, bet ir dėl bendros tendencijos, kai veiksmingumas vis dažniau vertinamas aukščiau už asmens privatumą bei duomenų saugumą.

Manytina, kad ilgalaikis požiūris į skaitmeninį suverenitetą turi būti grindžiamas ne kontrolės priemonių plėtra, o teisinių garantijų stiprinimu. Praktikoje būtina nustatyti aiškias ribas, t. y. įtvirtinti draudimą naudoti bendrą ir nediferencijuotą duomenų kaupimą, priimti teisės aktą, kuris uždraustų naudoti šnipinėjimo programinę įrangą. Taip pat privalu užtikrinti naudojamų technologijų skaidrumą ir realią galimybę ginti pažeistas teises. Taigi, skaitmeninį suverenitetą vertėtų suvokti kaip gebėjimą apsaugoti skaitmeninę aplinką užtikrinant aukščiausius žmogaus teisių standartus. Tik tada jis atitiks teisinės valstybės principus ir užkirs kelią pagrindinių teisių apsaugos silpnėjimui skaitmeninėje erdvėje.

3.3. Teisinės gynybos trūkumas skaitmeninėje erdvėje

ES skaitmeninis suverenitetas suprantamas kaip Sąjungos gebėjimas savarankiškai veikti skaitmeninėje erdvėje ir nustatyti joje savo taisykles. Vis dėlto pastebima tendencija, kad įgyvendinant šį suverenitetą didžiausias dėmesys skiriamas vis naujų reguliavimo normų kūrimui, skaitmeninės aplinkos priežiūros stiprinimui, atsakomybės platformoms ir infrastruktūrai nustatymui. Tuo tarpu asmenų, kurių teisės galėjo būti pažeistos, procesinių galimybių stiprinimas sulaukia mažiau dėmesio. Skaitmeninę aplinką reglamentuojantys teisės aktai formaliai įtvirtina teisę susipažinti su duomenimis bei galimybę teikti skundus priežiūros institucijoms ar kreiptis teismus. Tačiau praktinis šių garantijų realizavimas išlieka sudėtingas ir kelia nemažai iššūkių. Toliau šiame darbe analizuojamos kliūtys, su kuriomis susiduria asmenys, siekiantys apginti savo pažeistas teises skaitmeninėje erdvėje.

Formaliuoju požiūriu asmuo, kurio teisės pažeistos, turi platų gynybos priemonių pasirinkimą. Chartijos 47 straipsnis garantuoja teisę į veiksmingą teisinę gynybą ir teisingą teismo procesą. Šias garantijas detalizuoja specialieji teisės aktai. Pavyzdžiui, BDAR įtvirtina teisę pateikti skundą priežiūros institucijai (BDAR 77 straipsnis), teisę į veiksmingą teisminę gynybą prieš priežiūros instituciją (BDAR 78 straipsnis), teisę pareikšti ieškinį duomenų valdytojui ar tvarkytojui (BDAR 79 straipsnis), taip pat teisę į materialinės ir nematerialinės žalos atlyginimą (BDAR 82 straipsnis). Skaitmeninių paslaugų aktas sukuria vidinius platformų sprendimų apskundimo ir neteismo ginčų

sprendimo mechanizmus. Nors teisėkūros lygmeniu ši sistema atrodo pakankamai veiksminga, kiek asmuo realiai geba ja pasinaudoti nepatirdamas neproporcingų sunkumų.

Būtent šiame etape skaitmeninėje erdvėje kyla esminių problemų. Teisė pateikti skundą neužtikrina gebėjimo kompetentingai apibūdinti pažeidimą, teisė į ieškinį negarantuoja įrodymų prieinamumo, o teisė į kompensaciją realios galimybės įrodyti žalą. Nors ES kuria autonominę skaitmeninės teisės normų sistemą, pastaroji vis dar remiasi prielaida, kad asmuo savarankiškai identifikuos pažeidimą bei supras jo techninę prigimtį. Taip pat tikimasi, kad nekentėjusysis pats surinks įrodymus ir ras tinkamą procesinį kelią savo teisėms apginti.

Pavyzdžiui, BDAR 15 straipsnyje yra įtvirtinta, duomenų subjektų teisė susipažinti su savo duomenimis, kuri įgyvendinama kreipiantis į duomenų valdytoją. Ši teisė laikytina pagrindiniu mechanizmu, sudarančiu sąlygas naudotis kitomis duomenų subjekto teisėmis. Asmuo, negavęs informacijos apie asmens duomenų tvarkymą, iš esmės netenka galimybės veiksmingai gintis.

EDAV 2024 m. atliko tyrimą, sekdamą įvertinti, kaip duomenų valdytojai įgyvendina teisę susipažinti su duomenimis. Tyrimo metu išryškėjo kelios neigiamos tendencijos. Pirma, EDAV nustatė, kad duomenų valdytojams trūksta kompetencijos identifikuoti duomenų apimtį, kurią privalu gavus prašymą. Ataskaitoje nurodoma, kad duomenų valdytojai dažnai teikė per mažai informacijos, neįtraukdami visų konkrečiam prašymui aktualių duomenų. Taip pat pastebima, kad duomenų valdytojai neretai sudaro papildomų kliūčių, pavyzdžiui, reikalauja duomenų subjektams siųsti prašymus tik per tam tikras sistemas arba raštu, taip pat taiko perteklinius asmens tapatybės identifikavimo reikalavimus. Be to, EDAV pažymėjo, kad duomenų valdytojai linkę plačiai aiškina BDAR 12 straipsnio 5 dalį, kurioje nurodyta duomenų valdytojo teisė atsisakyti pateikti duomenis, jei prašymas yra akivaizdžiai nepagrįstas ar neproporcingas, BDAR 15 straipsnio 4 dalį, kurioje yra nurodyta kitų asmenų teisių ir laisvių apsauga, ir nacionalines teises normas, kurios gali apriboti teisę susipažinti su duomenimis pagal BDAR 23 straipsnį¹⁶³. Minėti duomenų valdytojų pažeidimai daro esminę įtaką veiksmingam teisių gynimui. Kai duomenų valdytojai nepagrįstai apsunkina ar apriboja prieigą prie duomenų, šių duomenų subjektas faktiškai netenka galimybės ginti savo teises, nes jis negali nei identifikuoti pažeidimo, nei surinkti įrodymų, reikalingų pagrįstam skundui pateikti. Tai atskleidžia esminę ES skaitmeninės erdvės reguliavimo problemą: nors formaliai teisė į veiksmingą

¹⁶³ European Data Protection Board (2025-01-16). *2024 Coordinated Enforcement Action; Implementation of the right of access by controllers* [interaktyvus]. https://www.edpb.europa.eu/system/files/2025-01/edpb_cef-report-2024_20250116_rightofaccess_en.pdf.

gynybą egzistuoja, praktikoje nėra garantijos, kad ją bus įmanoma įgyvendinti, nes asmuo priklauso nuo duomenų valdytojo veiksmų.

Analizuojant duomenų apsaugos aspektus, svarbu pabrėžti, kad DI technologijos, ypač mašininis mokymasis ir didžiųjų duomenų analizė, leidžia išgauti papildomą informaciją bei identifikuoti asmenį net naudojant tuos duomenis, kurie anksčiau buvo laikomi neasmeniniais. Todėl tokia informacija faktiškai leidžia, nustatyti asmens tapatybę, bet lieka už duomenų apsaugos teisės aktų taikymo sritis ribų¹⁶⁴. Tokiu atveju įrodyti pažeidimą ir apginti teises tampa dar sudėtingiau.

Ne mažiau aktualus yra skaitmeninių technologijų reguliavimo sankirtų klausimas. ES jau priėmė ne vieną skaitmeninę erdvę reglamentuojantį teisės aktą ir toliau aktyviai tęsia reguliavimo procesą. Dėl gausaus atskirų skaitmeninių dokumentų skaičiaus atsiranda rizika, kad atskiri reguliavimai gali sutapti arba dubliuotis. Situaciją dar labiau komplikuoja pačių paslaugų tarpusavio sąveika, todėl praktiškai neišvengiama, kad ta pati technologija patenka į kelis teisinius režimus. Pavyzdžiui, ta pati paslauga ar organizacija gali būti vienu metu klasifikuojama kaip internetinė platforma, DI operatorius, duomenų tvarkytojas ir vaizdo įrašų mainų platforma¹⁶⁵.

Intensyvėjant teisėkūrai, gausėja ir skaitmeninei sričiai įgaliotų institucijų, todėl reguliavimo procese neišvengiamai atsiranda kompetencijų sankirtų. Tinkamas horizontalaus kompetencijų persidengimo pavyzdys viršvalstybiniu lygmeniu yra „Meta“ „mokėk arba sutik“ modelis. Taikant šį modelį, vartotojas privalo arba mokėti už platformos naudojimą be reklamų, arba sutikti, kad jo asmens duomenys būtų tvarkomi personalizuotai reklamai. Tokia praktika buvo vertinama pagal skirtingus teisinius režimus. Viena vertus, EDAV ją analizuoja pagal BDAR, vertindama varduotojo sutikimo laisvumą ir informuotumą. Kita vertus, Europos Komisija tą pačią praktiką nagrinėja pagal Skaitmeninių rinkų aktą, siekdama nustatyti, ar nepažeidžiamas draudimas nesąžiningai naudoti duomenis ir nepiktnaudžiaujama rinkos galia. Pažymėtina, kad abi institucijos gali savarankiškai atlikti tos pačios veiklos teisinį vertinimą, neatsižvelgdamos į viena kitos išvadas. Dėl šios priežasties atsiranda rizika, kad ta pati situacija bus vertinama

¹⁶⁴ Privacy International (PI) (2024-03-01). *Privacy International's submission for the UNSR on racism's thematic report on artificial intelligence (AI) and racial discrimination* [interaktyvus]. https://privacyinternational.org/sites/default/files/2024-05/PI%20submission%20on%20AI%20and%20racial%20discrimination%20to%20UNSR%20on%20racism%20on%20AI_March%202024.pdf.

¹⁶⁵ DE GREGORIO, Giovanni ir VICINANZA, Anna (2026). The Enforcement of European Digital Regulation: Overlaps and Pathways. *Yearbook of European Law*, 44, 1-28 [interaktyvus]. <https://doi.org/10.1093/yel/yeag002>, p. 4.

lygiagrečiai, o priimti sprendimai gali būti priešaringi¹⁶⁶. Šis pavyzdys aiškiai rodo, kad įvairių ES viršvalstybinių institucijų kompetencijų sutapimas lemia teisės taikymo nenuoseklumą. Teisės taikymo fragmentacija kenkia veiksmingam ES teisės aktų vykdymui. Galimas procedūrų dubliavimas didina neveiksmingumą ir didina administracines išlaidas bei atitikties reikalavimams išlaidas tiek reguliavimo institucijoms, tiek reguliuojamiems subjektams.

Tuo pačiu metu įgaliojimų sutapimas gali pakenkti teisinio tikrumo principui. Esant fragmentiškam reguliavimui, fiziniai asmenys ir įmonės gali susidurti su sunkumais spręsdami, kokios taisyklės taikomos, kaip jos bus aiškinamos ir kuri institucija turi galutinę jurisdikciją. Toks neapibrėžtumas kelia pavojų, kad teisė bus taikoma nenuosekliai, taip pat silpnina pasitikėjimą teisine sistema ir mažina skaidrumą bei nuspėjamumą. Be to, teisinis neapibrėžtumas gali daryti neigiamą poveikį ekonomikos sričiai, stabdydamas investicijas ir trukdydamas ES vidaus rinkos plėtrai. Tokia fragmentacija mažina žmogaus teisių apsaugos veiksmingumą: asmuo atsiduria situacijoje, kai jo teisių apsauga priklauso ne nuo vieningos sistemos, o nuo daugybės tarpusavyje nesusijusių lygiagrečių procedūrų.

Taigi, nors naujausi teisės aktai išplėtė teisinės gynybos mechanizmų spektrą, jų išskaidymas tarp skirtingų institucijų ir teisinių sistemų tampa kliūtimi. Esant teisinių režimų persidengimui, tai silpnina teisės taikymo efektyvumą ir apsunkina teisės į veiksmingą teisinę gynybą įgyvendinimą.

Atsižvelgiant į tai, toliau tikslinga analizuoti ne teisinio, o socialinio pobūdžio problemą. Jos sprendimas leistų iš esmės sustiprinti skaitmeninių teisių apsaugą bei padidinti gynybos priemonių prieinamumą.

Skaitmeninio suvereniteto plėtros laikotarpiu buvo sukurta gausi reguliavimo mechanizmų sistema, įtvirtinanti priemones skaitmeninėje erdvėje pažeidžiamoms teisėms ginti. Vis dėlto, manytina, kad didelė dalis asmenų, įmonių ir net pačių institucijų negeba efektyviai naudotis šiomis priemonėmis: neatpažįsta pažeidimų, nežino, kur kreiptis, kaip rinkti įrodymus ir kaip formuluoti prašymus. Pavyzdžiui, 2025 m. tik 59 % ES piliečių teigė, jog supranta, kad jų teisės „realiame gyvenime“ (angl. offline) privalo būti taip pat gerbiamos saugomos „skaitmeninėje erdvėje“ (angl. online)¹⁶⁷. Tuo tarpu 88 % gyventojų

¹⁶⁶ DE GREGORIO, Giovanni ir VICINANZA, Anna (2026). The Enforcement of European Digital Regulation: Overlaps and Pathways. Yearbook of European Law, 44, 1-28 [interaktyvus]. <https://doi.org/10.1093/yel/yeag002>, p. 17.

¹⁶⁷ Council of the European Union (2025-06-19). *Commission staff working document Monitoring of the European Declaration on Digital Rights and Principles Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and*

tikėjosi iš viešosios valdžios tinkamos paramos, padedančios susiorientuoti skaitmeninimo procese¹⁶⁸. Todėl darytina išvada, kad normatyvinis reguliavimas plečiasi sparčiau nei visuomenės teisinis ir praktinis gebėjimas juo naudotis.

Teisinis ir skaitmeninis neapsišvietimas yra kompleksinė problema. N. A. Smuha pažymi, kad skaitmeninis raštingumas apima ne tik skaitmeninius įgūdžius, bet taip pat reikšia gebėjimą kritiškai vertinti skaitmenines technologijas bei jų poveikį. Pabrėžiama, pavyzdžiui, DI sistemų ir tokių klausimų kaip jų aiškumas, skaidrumas bei patikimumas supratimo svarba. Tokio supratimo stoka mažina žmonių gebėjimą suvokti, kokią poveikį skaitmeninės technologijos gali turėti jų gyvenimui. Tai riboja jų gebėjimą sudaryti nuomonę apie tai, kokios pasekmės yra suderinamos su visuomeninėmis vertybėmis, bei daryti įtaką politiniams sprendimams¹⁶⁹. Manytina, kad tai gali turėti įtakos asmenų gebėjimui ginti pažeistas teises. Pirma, asmenys dažnai nepajėgia tiksliai identifikuoti pažeidimo pobūdžio skaitmeninėje erdvėje. Antra, atpažinus problemą, dažnai trūksta procesinio suvokimo: neaišku, ar pirmenybę teikti kreipimuisi į duomenų valdytoją, nacionalinę priežiūros instituciją, teismą, vartotojų teisių gynimo instituciją, ar naudoti šių būdų derinį. Trečia, tinkamo skaitmeninės žalos dokumentavimo įgūdžių stoka vėliau sukelia esminių sunkumų įrodinėjimo ir žalos vertinimo procesuose.

Tačiau būtina stiprinti ne tik fizinių asmenų kompetencijas. Praktikoje didelė rizika kyla pačiose įmonėse, ypač mažosiose ir vidutinėse įmonėse, kurios aktyviai diegia skaitmenines technologijas, tačiau dažnai neturi reikiamos teisinės ir techninės infrastruktūros. Remiantis Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) 2025 m. duomenimis, net du trečdaliai mažųjų ir vidutinių įmonių netaiko patikimų skaitmeninių saugumo praktikų: tik 27 % įmonių turėjo pažangias skaitmeninio saugumo sistemas, 9 % apskritai neturėjo jokių apsaugos priemonių, o reguliarius darbuotojų mokymai bei išoriniai kibernetinio saugumo vertinimai buvo taikomi itin retai. EBPO pabrėžia, kad šie rodikliai rodo būtinybę didinti subjektų sąmoningumą, kadangi dauguma kibernetinių incidentų kyla dėl žmogiško faktoriaus klaidų. Kitas reikšmingas rodiklis – tik 21 % mažųjų ir vidutinių įmonių žinojo apie valstybines skaitmeninimo rėmimo programas.

digital future (10407/25 ADD 32) [interaktyvus]. <https://data.consilium.europa.eu/doc/document/ST-10407-2025-ADD-32/en/pdf>.

¹⁶⁸ European Commission (2024-07-02) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – State of the Digital Decade 2024; Com (2024) 260 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2024:260:FIN>.

¹⁶⁹ SMUHA, Nathalie A. Digital Sovereignty In The European Union: Five Challenges From A Normative Perspective. Iš: BARRETT, Gavin (red.); MÜLLER-GRAFF, Peter-Christian (red.); RAGEADE, Jean-Philippe (red.) ir kt. (2024). *European Sovereignty: The Legal Dimension*. Cham: Springer Cham. <https://doi.org/10.1007/978-3-031-71851-9>. p. 127-149. p. 146.

Sudėtingos paraiškų teikimo procedūros bei nebepakankamas programų atitikimas realiems verslo poreikiams yra įvardijamas kaip pagrindinės kliūtys šiame procese¹⁷⁰. Pabrėžtina, kad formuojasi ryškus atotrūkis tarp teisinio reguliavimo ir realių gebėjimų jį įgyvendinti. Kol įmonėms trūksta reikiamos informacijos bei įgūdžių, formaliai griežtos normos veiks arba selektyviai, arba reaktyviai, t. y. tik jau įvykus incidentui.

Be to, kompetencijų ugdymas yra aktualus ne tik asmenims, kurių teisės pažeidžiamos, bet ir duomenų valdytojams. EDAV pažymi, kad pagrindinė priemonė, leidžianti užkirsti kelią pažeidimams ar netinkamam skundų dėl teisės susipažinti su duomenimis nagrinėjimui, yra duomenų valdytojų konsultavimas ir reguliavimo nuostatų aiškinimas¹⁷¹.

Nors teisiniame diskurse įprasta manyti, kad valstybės institucijos turi reikiamą kompetenciją, praktikoje pastebimos priešingos tendencijos. Skaitmeninė erdvė kinta itin sparčiai, o reguliavimas įgyja tarpsektorinį pobūdį, todėl su žinių trūkumu susiduria ir viešojo sektoriaus subjektai. Akivaizdu, kad valstybė negali veiksmingai užtikrinti skaitmeninių teisių apsaugos, jei pati neįgyvendina nuoseklaus ir nuolatinio savo tarnautojų bei institucijų kvalifikacijos kėlimo.

Matytina, kad šiandien skaitmeninis raštingumas yra esminis subjektyvumo skaitmeninėje erdvėje elementas. Jungtinio tyrimų centro „DigComp 3.0“ gairėse skaitmeninė kompetencija tiesiogiai siejama ne tik su gebėjimu naudotis technologijomis, bet ir su įgūdžiais, leidžiančiais užtikrintai, kritiškai ir atsakingai dalyvauti skaitmeninėje aplinkoje¹⁷².

Remiantis „Digital Decade 2025“ ataskaita, Lietuva užima aukštas pozicijas skaitmeninių viešųjų paslaugų srityje. Tačiau toje pačioje ataskaitoje nurodomos ir silpnosios vietos: pažangių technologijų diegimas įmonėse, ypač mažosiose ir vidutinėse įmonėse, išlieka netolygus, o pagrindinėmis kliūtimis įvardijami procedūriniai sudėtingumai ir nepakankamas žinių lygis¹⁷³. Taigi, aukštas skaitmeninių viešųjų paslaugų plėtros lygis tiesiogiai negarantuoja efektyvios skaitmeninių teisių apsaugos. Priešingai, skaitmeniškai pažengusioje valstybėje teisių pažeidimai tampa sunkiai identifikuojami ir techniškai sudėtingesni.

¹⁷⁰ BIANCHINI, Marco ir SANCHO, Marta Lasheras (2025). *SME digitalisation for competitiveness: The 2025 OECD D4SME Survey* [interaktyvus]. Paris: OECD Publishing. <https://doi.org/10.1787/197e3077-en>.

¹⁷¹ European Data Protection Board (2025-01-16). *2024 Coordinated Enforcement Action; Implementation of the right of access by controllers* [interaktyvus]. https://www.edpb.europa.eu/system/files/2025-01/edpb_cef-report-2024_20250116_rightofaccess_en.pdf.

¹⁷² CENTENO, Clara ir COSGROVE, Judith (2025). *Ten Years of DigComp: A Framework more essential than ever* [interaktyvus]. *JRC Research Reports JRC143430*, Joint Research Centre. <https://publications.jrc.ec.europa.eu/repository/handle/JRC143430>, p. 4.

¹⁷³ European Commission (2025-06-18). *Lithuania 2025 Digital Decade Country Report* [interaktyvus]. <https://digital-strategy.ec.europa.eu/en/factpages/lithuania-2025-digital-decade-country-report>.

Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) 2024 m. asmens duomenų priežiūros Lietuvoje apžvalgoje nurodyta, kad per metus VDAI gavo 1 408 skundus – beveik 15 % daugiau nei 2023 m. Tuo pačiu metu VDAI suteikė 4 334 konsultacijas: 1 852 duomenų valdytojams, 2 377 duomenų subjektams ir 105 duomenų tvarkytojams¹⁷⁴. 2025 m. VDAI ataskaitoje nurodoma, kad per metus buvo gautas 2081 skundas, kas yra 48 % daugiau nei 2024 m. Tačiau 2025 m. konsultacijų skaičius neišaugo – buvo suteikta 4301 konsultacija¹⁷⁵. Ši statistika rodo, kad visuomenė aktyviai domisi teisių apsaugos priemonėmis ir siekia jas realizuoti. Visgi, vertinant šiuos duomenis Lietuvos gyventojų skaičiaus kontekste, manytina, kad kreipimusi į institucijas kiekis išlieka santykinai nedidelis.

Tokią tendenciją iš dalies paaiškina ES skaitmeninės politikos kryptys. Analizuojant 2023 m. ES skaitmeninę strategiją matyti, kad visuomenės švietimas yra aptariamas, tačiau pagrindiniu šio skaitmeninio švietimo tikslas yra skatinti gyventojus įgyti aukštus skaitmeninius įgūdžius. Skaitmeninėje strategijoje prioritetas teikiamas specialistų, turinčių aukšto lygio skaitmeninių įgūdžių, ugdymui, nes tai laikoma esmine skaitmeninės ekonomikos plėtros ir spartesnio jos vystymosi prielaida¹⁷⁶. Taigi, gali susidaryti įspūdis, kad ES prioritetą vėlgi teikia kuo spartesniam naujų technologijų bei paslaugų kūrimui, o ne teisių pažeidimų prevencijai ir tiesioginei asmens apsaugai skaitmeninėje erdvėje. Tiesa, ES būtinų skaitmeninių įgūdžių rinkinyje „DigComp 3.0“ formaliai yra aptariamas skaitmeninių teisių įgyvendinimo klausimas. Iš šio kompetencijų rinkinio, matyti, kad asmeniui būtina žinoti savo teises, susijusias su asmens duomenimis bei privatumu, gebėti jomis naudotis ir valdyti kylančias rizikas¹⁷⁷. Tačiau manytina, kad šios nuostatos yra tik deklaratyvios, nes jos nėra papildomos praktinių teisinių įgūdžių ugdymu, pavyzdžiui, kreipimusi į priežiūros institucijas, gynybos būdo pasirinkimu, skundų ar procesinių dokumentų rengimu. Dėl šios priežasties susidaro atotrūkis tarp teorinio teisių pripažinimo ir realios galimybės jas veiksmingai įgyvendinti praktikoje.

¹⁷⁴ Valstybinė duomenų apsaugos inspekcija (2025-08-08). *2024 m. asmens duomenų apsaugos priežiūros Lietuvoje apžvalga* [interaktyvus].

https://vdai.lrv.lt/public/canonical/1754559815/1040/Ataskaita_EDAV_2024.pdf.

¹⁷⁵ Valstybinė duomenų apsaugos inspekcija (2026-03-05). *2025 m. veiklos ataskaita* [interaktyvus]. https://vdai.lrv.lt/public/canonical/1772605397/1298/2025m_VDAI_veiklos_ataskaita_galutinis.pdf.

¹⁷⁶ Europos Komisija (2021-03-09). *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: 2030 m. skaitmeninės politikos kelrodis: Europos skaitmeninio dešimtmečio kelias, COM(2021) 118 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52021DC0118>.

¹⁷⁷ COSGROVE, J. ir CACHIA, R. (2025). *DigComp 3.0: European Digital Competence Framework – Fifth Edition JRC144121* [interaktyvus]. Luxembourg: Publications Office of the European Union. <https://data.europa.eu/doi/10.2760/0001149>, p. 48-51.

Siekiant veiksmingai plėtoti praktines žinias skaitmeninių teisių srityje, būtina pereiti nuo deklaratyvaus pobūdžio nuostatų prie sisteminio teisinio ir skaitmeninio švietimo modelio, kuris būtų integruotas į ES skaitmeninio suvereniteto politiką.

Visų pirma, reikia pakeisti akcentą nuo abstrakčių skaitmeninių kompetencijų prie praktinių teisių įgyvendinimo įgūdžių. Asmuo turi ne tik žinoti apie savo teisių egzistavimą, bet ir realiai suprasti, kur kreiptis, kokį priežiūros subjektą pasirinkti (duomenų valdytoją, nacionalinę priežiūros instituciją, teismą ar kt.), kaip parengti prašymą ar skundą, kaip ir kokius įrodymus surinkti ir kokių rezultatų tikėtis. Tam švietimo iniciatyvos turėtų apimti praktinius scenarijus, grįstus „mokymusi iš konkrečių pavyzdžių“ (angl. case-based learning), standartizuotus kreipimosi šablonus ir aiškius veiksmų algoritmus, prieinamus tiek piliečiams, tiek verslui.

Taip pat būtina supaprastinti institucinę apsaugos struktūrą: priežiūros institucijos turėtų veikti orientuodamosi į vartotoją, siūlydamos skaidrius teisių gynimo būdus ir koordinuodamos funkcijas taip, kad teisinės sistemos sudėtingumas netaptų našta teisių turėtojui. Esminis elementas yra privalomas valstybės tarnautojų, teisėjų bei reguliavimo institucijų darbuotojų kvalifikacijos kėlimas, nes būtent nuo jų kompetencijos priklauso realus teisės į veiksmingą gynimą įgyvendinimas skaitmeninėje erdvėje. Be to, svarbu ugdymą susieti su skaitmeniniu saugumu, kadangi dauguma pažeidimų kyla dėl žmogiškojo faktoriaus klaidų ir technologinių rizikos veiksmų sankirtos.

Visa tai tiesiogiai susiję su žmogaus teisių apsauga. Be galimybės praktiškai įgyvendinti teisę į veiksmingą gynimą, skaitmeninės teisės lieka formalios. Todėl ES skaitmeninis suverenitetas turi būti suvokiamas ne tik kaip infrastruktūros plėtra, duomenų kontrolė ir darbuotojų skaitmeninių įgūdžių lavinimas, bet ir kaip gebėjimas užtikrinti realų kiekvieno žmogaus teisių įgyvendinimą. Nepakankamai vystantis praktinėms kompetencijoms, gyventojai išlieka pasyvūs skaitmeninėje erdvėje. Todėl ES turėtų formuoti tokią skaitmeninio vystymosi politiką, kuri skatintų aktyvios ir teisiškai veiksnios visuomenės, gebančios savarankiškai ginti savo teises, kūrimą.

IŠVADOS IR PASIŪLYMAI

1. Atlikta skaitmeninio suvereniteto sąvokos analizė leidžia daryti išvadą, kad skaitmeninis suverenitetas – tai politikos kryptis, kurią plėtoja ES. Jis transformavosi iš klasikinės valdžios tam tikroje teritorijoje kategorijos į skaitmeninės erdvės reguliavimo mechanizmą, kuris šiuo metu apima gausų teisės aktų, reguliuojančių skaitmeninę erdvę, sąrašą. Autorės nuomone, pagrindinis skaitmeninio suvereniteto tikslas yra nepriklausomas ES skaitmeninės erdvės reguliavimo nustatymas, kuris atitiks ES interesus bei bus kildinamas iš ES teisės ir vertybių. Tyrimo metu nustatyta, kad ši sąvoka apima ne tik teisėkūros procesą, bet ir veiksmus, kuriais siekiama ES technologinės, ekonominės ir socialinės plėtros skaitmeninėje erdvėje.
2. Moksliniame darbe nustatyta, kad EŽTK ir Chartijoje įtvirtintos žmogaus teisės (visų pirma teisė į privatus gyvenimo gerbimą, saviraiškos laisvę, duomenų apsaugą ir veiksmingą teisinę gynybą) taikomos ir skaitmeninėje erdvėje. Todėl valstybės privalo užtikrinti jų apsaugą ir šioje srityje. ES, plėtodama skaitmeninį suverenitetą, priima teisės aktus ir kuria mechanizmus, kurie užtikrina veiksmingą šių teisių apsaugą. Autorės nuomone, skaitmeninio suvereniteto įgyvendinimas padeda išplėsti subjektų galimybes kontroliuoti savo duomenis, užtikrina į žmogų orientuotą technologijų plėtrą. Be to, tyrimo metu padaryta išvada, kad dėka nustatytų taisyklių tarptautinės įtakos, žmogaus teisių apsauga stiprinama ne tik ES viduje, bet ir už jos ribų.
3. Autorės nuomone, skaitmeninio suvereniteto vystymas gali kelti iššūkius žmogaus teisių apsaugai. Atlikta analizė rodo, kad neigiamas poveikis susijęs ne su siekiu sukurti skaitmeninį suverenitetą, o su jo įgyvendinimo būdais. Nustatyta, kad ES pagrindinis dėmesys kreipiamas į ES techninės plėtros spartinimą ir nepriklausomybės skaitmeninėje erdvėje užtikrinimą. Tai gali lemti prioritetų pasikeitimą nuo žmogaus teisių apsaugos prie tarptautinės konkurencijos didinimo. Atlikta analizė taip pat rodo, kad, nors ES priėmė gausų teisės aktų, reguliuojančių skaitmeninę erdvę, skaičių, vis dar išlieka tam tikrų spragų, kurios suteikia galimybę piktnaudžiauti teise. Darbe nustatyta, kad didelis teisės aktų skaičius apsunkina žmogaus teisių apsaugos sistemą. Jie, nors ir sukurti atskirų sričių reguliavimui, dažnai persipina, o tai galiausiai veikia galimybę veiksmingai pasinaudoti nustatytomis garantijomis.
4. Autorė pabrėžia, kad žmogaus teisių apsauga skaitmeninėje erdvėje reikalauja kompleksinio požiūrio. Jos nuomone, tikslinga būtų priimti visuotinį tarptautinį dokumentą, kuriuo būtų nustatytos pagrindinės skaitmeninės teisės. ES skaitmeninis

suverenitetas turėtų būti įgyvendinamas stiprinant žmogaus teisių apsaugos garantijas, o bet kokie šių teisių apribojimai turi atitikti teisėtumo, būtinumo ir proporcingumo kriterijus. Taip pat, būtina nustatyti aiškius ir veiksmingus tam tikrų technologijų naudojimo ribojimus, įskaitant draudimą kaupti bei naudoti nediferencijuotus duomenis ir vykdyti masinį stebėjimą. Darbo metu nustatyta skaitmeninių teisių įgyvendinimo praktinių įgūdžių ugdymo būtinybė.

ŠALTINIŲ SĄRAŠAS

Teisės aktai:

1. Europos Parlamento Ir Tarybos 2002 m. liepos 12 d. direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OL, L 201, 2002, p. 37-47.
2. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119/1, 2016, p. 1-88.
3. Europos Parlamento ir Tarybos 2018 m. lapkričio 14 d. reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų. OL L 303/59, 2018, p. 59–68.
4. Europos Parlamento ir Tarybos 2022 m. gegužės 30 d. reglamentas (ES) 2022/868 dėl Europos duomenų valdymo, kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1724 (Duomenų valdymo aktas). OL L 152/1, 2022, p. 1-44.
5. Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. direktyva (ES) 2022/2555, dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva). OL L 333/80, 2022, p. 80-152.
6. Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. sprendimas (ES) 2022/2481 kuriuo nustatoma 2030 m. Skaitmeninio dešimtmečio politikos programa. OL L 323, 2022, p. 4-26.
7. Europos Parlamento ir Tarybos 2022 m. rugsėjo 14 d. reglamentas (ES) 2022/1925 dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828 (Skaitmeninių rinkų aktas). OL L 265/1, 2022, p. 1–66.
8. Europos Parlamento ir Tarybos 2022 m. spalio 19 d. reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas). OL L 277/1, 2022, p. 1–102.
9. Europos Parlamento ir Tarybos 2023 m. gruodžio 13 d. reglamentas (ES) 2023/2854 dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/2394 ir Direktyva (ES) 2020/1828 (Duomenų aktas). OL L 2023/2854, 2023.

10. Europos Parlamento ir Tarybos 2023 m. kovo 15 d. reglamentas (ES) 2023/588, kuriuo nustatoma 2023–2027 m. Sąjungos saugaus junglumo programa. OL L 79/1, 2023, p. 1-39.
11. Europos Parlamento ir Tarybos 2023 m. rugsėjo 13 d. reglamentas (ES) 2023/1781, kuriuo nustatoma Europos puslaidininkių ekosistemos stiprinimo priemonių sistema ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Lustų aktas). OJ L 229/1, 2023, p. 1-53.
12. Europos Parlamento ir Tarybos 2024 m. birželio 13 d. direktyva (ES) 2024/1760, dėl įmonių tvarumo išsamaus patikrinimo, kuria iš dalies keičiama Direktyva (ES) 2019/1937 ir Reglamentas (ES) 2023/2859. OL L 2024/1760, 2024.
13. Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas (ES) 2024/1689, 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). OL L 2024/1689, 2024.
14. Europos Parlamento ir Tarybos 2025 m. vasario 11 d. reglamentas (ES) 2025/327, dėl Europos bendros sveikatos duomenų erdvės, kuriuo iš dalies keičiama Direktyva 2011/24/ES ir Reglamentas (ES) 2024/2847. OL L 2025/327, 2025.
15. Europos Parlamento ir Tarybos 2026 m. vasario 24 d. direktyvą (ES) 2026/470, kuria iš dalies keičiamos direktyvos 2006/43/EB, 2013/34/ES, (ES) 2022/2464 ir (ES) 2024/1760, kiek tai susiję su tam tikrais įmonių tvarumo atskaitomybės reikalavimais ir tam tikrais įmonių tvarumo išsamaus patikrinimo reikalavimais. OL L 2026/470, 2026.
16. Europos Sąjungos pagrindinių teisių chartija. OL C 202, 2016, p. 389–405.
17. Europos Sąjungos sutarties suvestinė redakcija. OL C 202, 2016, p. 13–46.
18. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija iš dalies pakeista protokolu Nr. 15 (konsoliduotas tekstas) (1950). TAR, 2022, 2432.
19. Komisijos 2016 m. liepos 12 d. įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB. OL L 207/1, 2016, p. 1-112.
20. Komisijos 2023 m. liepos 10 d. įgyvendinimo sprendimas (ES) 2023/1795, priimtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679, dėl tinkamo asmens duomenų apsaugos lygio pagal ES ir JAV duomenų privatumo sistemą. OL L 231/118, 2023, p. 118-229.

21. Lietuvos Respublikos Konstitucija. Lietuvos Respublikos piliečių priimta 1992 m. spalio 25 d. referendume. *Valstybės žinios*, 1992, 33–1014.
22. Lietuvos Respublikos Konstitucijos papildymo Konstituciniu aktu „Dėl Lietuvos Respublikos narystės Europos Sąjungoje“ ir Lietuvos Respublikos Konstitucijos 150 straipsnio papildymo įstatymas. *Valstybės žinios*, 2004-07-17, Nr. 111-4123.
23. Lietuvos Respublikos Konstitucinio Teismo 2006 m. kovo 14 d. nutarimas. *Valstybės žinios*, 2006-03-16, 30-1050.
24. Lietuvos Respublikos Konstitucinio Teismo 2014 m. kovo 18 d. nutarimas. TAR, 2014-03-19, 3226.
25. Lietuvos Respublikos Konstitucinio Teismo 2014 m. sausio 24 d. nutarimas. TAR, 2014-01-24, 478.
26. Lietuvos Respublikos Konstitucinio Teismo 2017 m. gruodžio 20 d. sprendimas. KT21-S11/2017.
27. Sutarties dėl Europos Sąjungos veikimo suvestinė redakcija. OL C 202, 2016, p. 47–360.
28. Tarptautinis pilietinių ir politinių teisių paktas (1966). *Valstybės žinios*, 2002-08-02, Nr. 77-3288.
29. Visuotinė žmogaus teisių deklaracija (1948). *Valstybės žinios*, 2006-06-17, 68-2497.

Specialioji literatūra:

30. ANDREW, Edward (2011). Jean Bodin on Sovereignty. *Republics of Letters: A Journal for the Study of Knowledge, Politics, and the Arts*, 2(2), 75-84 [interaktyvus]. https://shc.stanford.edu/sites/default/files/2011-03/roflv02i02_Andrew_060111_0.pdf.
31. AUTOLITANO, Simona ir PAWLOWSKA, Agnieszka (2021). Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study. *IAI Papers*, 21(14), 1-23 [interaktyvus]. <https://www.iai.it/sites/default/files/iaip2114.pdf>.
32. BARTELSON, Jens (2006). The Concept of Sovereignty Revisited. *The European Journal of International Law*, 17(2), 463-474 [interaktyvus].
33. BIANCHINI, Marco ir SANCHO, Marta Lasheras (2025). *SME digitalisation for competitiveness: The 2025 OECD D4SME Survey* [interaktyvus]. Paris: OECD Publishing. <https://doi.org/10.1787/197e3077-en>.
34. CENTENO, Clara ir COSGROVE, Judith (2025). Ten Years of DigComp: A Framework more essential than ever [interaktyvus]. *JRC Research Reports*

35. CHANDER, Anupam ir SUN, Haochen. Digital Sovereignty as Double-Edged Sword. Iš: CHANDER, Anupam (red.) ir SUN, Haochen (red.) (2023). Data Sovereignty. From the Digital Silk Road to the Return of the State. New York: Oxford University Press, p.72-88. DOI: 10.1093/oso/9780197582794.001.0001.
36. CHRISTAKIS, Theodore (2020). *“European Digital Sovereignty”: Successfully Navigating Between the Brussels Effect and Europe’s Quest for Strategic Autonomy* [interaktyvus]. Multidisciplinary Institute on Artificial Intelligence / Grenoble Alpes Data Institute. <http://dx.doi.org/10.2139/ssrn.3748098>.
37. COLETTI, Paola, DUCCI, Cecilia ir MORO, Francesco Niccolo (2025). Digital Sovereignty and the EU’s Identity between Technological Innovation and European Values. *JCMS: Journal of Common Market Studies*, p. 1-19 [interaktyvus]. <https://doi.org/10.1111/jcms.70074>.
38. COSGROVE, J. ir CACHIA, R. (2025). *DigComp 3.0: European Digital Competence Framework – Fifth Edition JRC144121* [interaktyvus]. Luxembourg: Publications Office of the European Union. <https://data.europa.eu/doi/10.2760/0001149>
39. DE GREGORIO, Giovanni ir VICINANZA, Anna (2026). The Enforcement of European Digital Regulation: Overlaps and Pathways. *Yearbook of European Law*, 44, 1-28 [interaktyvus]. <https://doi.org/10.1093/yel/yeag002>.
40. DEKHUIJZEN, Elisabeth (2025). La Quadrature du Net II and Data Retention under Article 15(1) ePrivacy Directive: CJEU Walks a Tightrope on IP Addresses Retention and Access for Public Authorities in NonSerious Crime. *European Data Protection Law Review*, 11(2), 253-258 [interaktyvus]. https://cris.maastrichtuniversity.nl/ws/portalfiles/portal/280951111/Dekhuijzen-2025-La-Quadrature-du-Net_II-and-.pdf.
41. European Union (2025). *Code of Conduct on Disinformation with Overview* [interaktyvus]. Luxembourg: Publications Office of the European Union. <https://ec.europa.eu/newsroom/dae/redirection/document/112678>.
42. JARAŠIŪNAS, Egidijus. Valstybės suvereniteto kategorija tarpsisteminės sąveikos srityje: konstitucinio tapatumo alternatyva ar jo esminis elementas?. Iš: TVARONAVIČIENĖ, Agnė (red.), MILIUVIENĖ, Jolita (red.) ir VEČERSKYTĖ, Juta (red.) (2021). *Konstitucija ir teisinė sistema. Liber Amicorum Vytautui Sinkevičiui*. Vilnius: Mykolo Romerio universitetas.

43. KALFF, Donald ir RENDA, Andrea (2019). *Hidden Treasures. Mapping Europe's sources of competitive advantage in doing business* [interaktyvus]. Brussels: Centre for European Policy Studies (CEPS). <https://www.sipotra.it/wp-content/uploads/2019/09/Hidden-Treasures.-Mapping-Europe's-sources-of-competitive-advantage-in-doing-business.pdf>.
44. LANZA, Edison (2017-03-15). *Standards for a Free, Open and Inclusive Internet* [interaktyvus]. http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf.
45. LEWIS, James Andrew (2010). *Sovereignty and the Role of Government in Cyberspace*. Brown Journal of World Affairs, 16(2), 55-65 [interaktyvus].
46. LIAROPOULOS, Andrew (2017). Cyberspace Governance and State Sovereignty. Iš: BITROS, George C. (red.) and KYRIAZIS, Nicholas C. (red.) *Democracy and an Open-Economy World Order* (2017). Cham: Springer International Publishing AG. DOI10.1007/978-3-319-52168-8
47. LITVINENKO, Anna (2021). Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. *Media and Communication*, 9(4), 5-15 [interaktyvus]. <https://doi.org/10.17645/mac.v9i4.4292>.
48. MAKOVETSKA, Nelia, DUBOV, Gennadii, DIDYCH, Taras ir kt. (2024). Global challenges to state sovereignty in the 21st century. *Salud, Ciencia y Tecnología - Serie de Conferencias*, 3 [interaktyvus]. <https://doi.org/10.56294/setconf2024.661>.
49. MARITAIN, Jacques (1950). The Concept of Sovereignty. *The American Political Science Review*, 44(2), 343-357 [interaktyvus]. <https://doi.org/10.2307/1950275>.
50. PAJUSTE, Tiina (2025). Digital Sovereignty and Human Rights: Balancing Security and Freedom. *Working paper: Technological change and international law: ESIL annual conference, Vilnius, 5-6 September 2024*, p. 78-84 [interaktyvus]. https://www.researchgate.net/publication/396975294_Digital_Sovereignty_and_Human_Rights_Balancing_Security_and_Freedom.
51. ROBERTS, Huw, COWLS, Josh, CASOLARI, Federico ir kt. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet policy review*, 10(3) [interaktyvus]. DOI10.14763/2021.3.1575
52. SMUHA, Nathalie A. Digital Sovereignty In The European Union: Five Challenges From A Normative Perspective. Iš: BARRETT, Gavin (red.); MÜLLER-GRAFF, Peter-Christian (red.); RAGEADE, Jean-Philippe (red.) ir kt. (2024). *European*

Sovereignty: The Legal Dimension. Cham: Springer Cham.
<https://doi.org/10.1007/978-3-031-71851-9>. p. 127-149.

53. TOTH, Zoltan (2023). Theories on sovereignty. *Central European Journal of Comparative Law*, 4(1), 175-195 [interaktyvus].
<https://doi.org/10.47078/2023.1.175-195>.

Teismų praktika:

54. *Data Protection Commissioner prieš Facebook Ireland Limited ir Maximillian Schrems* [ESTT], Nr. C-311/18, [2020-07-16]. ECLI:EU:C:2020:559.
55. *DZI – OBSHTO ZASTRAHOVANE EAD prieš ZK LEV INS AD* [ESTT], Nr. C-245/25, [2026-01-26]. Application (OJ).
56. *GC, AF, BH, ED prieš Commission nationale de l'informatique et des libertés (CNIL)* [ESTT], Nr. C-136/17, [2019-09-24], ECLI:EU:C:2019:773.
57. *Gesamtverband Autoteile-Handel e.V. prieš Scania CV AB* [ESTT], Nr. C-319/22, [2023-11-09]. ECLI:EU:C:2023:837.
58. *Google LLC prieš Commission nationale de l'informatique et des libertés (CNIL)* [ESTT], Nr. C-507/17, [2019-09-24]. ECLI:EU:C:2019:772.
59. *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* [ESTT], Nr. C-131/12, [2014-05-13]. ECLI:EU:C:2014:317.
60. *La Quadrature du Net ir kt. prieš Premier ministre ir kt.* [ESTT], Nr. C-511/18, [2020-10-06]. ECLI:EU:C:2020:791.
61. *La Quadrature du Net ir kt. prieš Premier ministre ir Ministère de la Culture* [ESTT], Nr. C-470/21, [2024-04-30]. ECLI:EU:C:2024:370.
62. Lietuvos vyriausiojo administracinio teismo 2024 m. spalio 23 d. sprendimas administracinėje byloje Nr. eA-1740-525/2024.
63. Lietuvos vyriausiojo administracinio teismo 2025 m. kovo 26 d. nutartis administracinėje byloje Nr. eA-483-821/2025.
64. *Standard Verlagsgesellschaft MBH prieš Austriją (Nr. 3)* [EŽTT], Nr. 39378/15 [2021-12-07]. ECLI:CE:ECHR:2021:1207JUD003937815.
65. *Taganrog LRO ir kiti prieš Rusiją* [EŽTT], Nr. 32401/10 [2022-09-07]. ECLI:CE:ECHR:2022:0607JUD003240110.
66. *Tele2 Sverige AB prieš Post- och telestyrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.* [ESTT], Nr. C-203/15, [2016-12-21]. ECLI:EU:C:2016:970.

67. *Volker und Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen* [ESTT], Nr. C-92/09 ir C-93/09, [2010-11-09]. ECLI:EU:C:2010:662.
68. *Amann prieš Šveicariją* [EŽTT], Nr. 27798/95, [2000-02-16]. ECLI:CE:ECHR:2000:0216JUD002779895.
69. *Rotaru prieš Rumuniją* [EŽTT], Nr. 28341/95, [2000-05-04]. ECLI:CE:ECHR:2000:0504JUD002834195.
70. *Ahmet Yildirim prieš Turkiją* [EŽTT], Nr. 3111/10, [2012-12-18]. ECLI:CE:ECHR:2012:1218JUD000311110.
71. *Delfi AS prieš Estiją* [EŽTT], Nr. 64569/09, [2015-06-16]. ECLI:CE:ECHR:2015:0616JUD006456909.
72. *Benedik prieš Slovėniją* [EŽTT], Nr. 62357/14, [2018-04-24]. ECLI:CE:ECHR:2018:0424JUD006235714.
73. *OQ prieš Land Hessen* [ESTT], Nr. C-634/21, [2023-12-07]. ECLI:EU:C:2023:957.
74. *YETTEL BULGARIA EAD prieš FB* [ESTT], Nr. C-806/24, [2025-02-07]. Application (OJ).

Internetiniai šaltiniai:

75. Article19 (2024-09-03). *EU: Civil society demands action against spyware threats* [interaktyvus]. <https://www.article19.org/resources/eu-civil-society-demands-action-against-spyware-threats/>.
76. Bundesministerium für Digitales und Staatsmodernisierung (2025-11-17). *Summit for More Digital Sovereignty Starts in Berlin* [interaktyvus]. <https://bmfs.bund.de/aktuelles/pressemitteilungen/detail/summit-for-more-digital-sovereignty-starts-in-berlin>.
77. China Media Project (2015-09-30). *Internet Sovereignty* [interaktyvus]. <https://chinamediaproject.org/2015/09/30/internet-sovereignty/>.
78. China.org.cn (2010-06-08). *The Internet in China* [interaktyvus]. http://www.china.org.cn/government/whitepaper/node_7093508.htm.
79. Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (2023-05-22). *Report A9-0189/2023 of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI))* [interaktyvus]. https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

80. Council of Europe (2007-11-07). *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet (Adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies)* [interaktyvus]. <https://search.coe.int/cm?i=09000016805d4a39>.
81. Council of Europe (2014-04-16). *Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users* [interaktyvus]. [https://search.coe.int/cm#{%22CoEIdentifier%22:\[%2209125948801c50a5%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209125948801c50a5%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}).
82. Council of Europe (2022-04-06). *Recommendation of the Committee of Ministers to member States CM/Rec(2022)11 on principles for media and communication governance* [interaktyvus]. <https://search.coe.int/cm?i=09125948802680f5>.
83. Council of the European Union (2025-06-19). *Commission staff working dokument: Monitoring of the European Declaration on Digital Rights and Principles Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future (10407/25 ADD 32)* [interaktyvus]. <https://data.consilium.europa.eu/doc/document/ST-10407-2025-ADD-32/en/pdf>.
84. Council of the European Union (2025-11-27). *Declaration for European Digital Sovereignty, ST 15781/25* [interaktyvus]. <https://data.consilium.europa.eu/doc/document/ST-15781-2025-INIT/en/pdf>.
85. CZERNIAWSKI, Michal (2025-12-03). *EU's Digital Sovereignty and the Rights-Based Imperative* [interaktyvus]. <https://verfassungsblog.de/digital-sovereignty-and-the-rights/>.
86. Electronic Frontier Fondation (n.d.). *A declaration of the Independence of Cyberspace* [interaktyvus]. <https://www EFF.org/cyberspace-independence>.
87. Elysee (2017-09-26). *President Macron gives speech on new initiative for Europe* [interaktyvus]. <https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe>.
88. European Commision (2024-07-02) *Communication from the Commision to the European Parlament, the Council, the European Economic and Social Committee and the Committee of the Regions – State of the Digital Decade 2024; Com (2024) 260*

- final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2024:260:FIN>.
89. European Commission (2024-10-09). *Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, COM(2024) 451 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0451>.
 90. European Commission (2020-02-19). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future. COM(2020) 67 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067>.
 91. European Commission (n.d.). Political Guidelines. *Ursula von der Leyen. Candidate for the European Commission President* [interaktyvus]. https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf.
 92. European Council (2026-02-24). *Council signs off simplification of sustainability reporting and due diligence requirements to boost EU competitiveness* [interaktyvus]. <https://www.consilium.europa.eu/en/press/press-releases/2026/02/24/council-signs-off-simplification-of-sustainability-reporting-and-due-diligence-requirements-to-boost-eu-competitiveness/>.
 93. European Data Protection Board (2025-01-16). *2024 Coordinated Enforcement Action; Implementation of the right of access by controllers* [interaktyvus]. https://www.edpb.europa.eu/system/files/2025-01/edpb_cef-report-2024_20250116_rightofaccess_en.pdf.
 94. European Digital Rights (EDRi) (2025-01-08). *CSA Regulation Document Pool* [interaktyvus]. <https://edri.org/our-work/csa-regulation-document-pool/>.
 95. European Digital Rights (EDRi) (2025-04-03). *CJEU saved the HADOPI: what implications for the future of data retention in the EU?* [interaktyvus]. <https://edri.org/our-work/cjeu-saved-the-hadopi-what-implications-for-the-future-of-data-retention-in-the-eu/>.
 96. European Digital Rights (EDRi) (2025-11-13). *Forthcoming Digital Omnibus would mark point of no return* [interaktyvus]. <https://edri.org/our-work/forthcoming-digital-omnibus-would-mark-point-of-no>

return/#:~:text=reform%20of%20the%20EU's%20digital,other%20core%20digital%20rights%20protections".

97. European Digital Rights (EDRi) (2025-11-19). *Why the Digital Omnibus puts GDPR and ePrivacy at risk* [interaktyvus]. https://edri.org/wp-content/uploads/2025/11/202511-Eexplaining-GDPR_eprivacy-Digital-Omnibus.pdf.
98. European Parliament (2024-01-23). *European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)) (C/2024/494)* [interaktyvus]. <https://eur-lex.europa.eu/eli/C/2024/494/oj/eng/pdf>.
99. European Repository of Cyber Incidents (EuRepoC) (n.d.). *Cyber Incident Dashboard* [interaktyvus]. <https://eurepoc.eu/dashboard/>.
100. European Commission (2025-06-18). *Lithuania 2025 Digital Decade Country Report* [interaktyvus]. <https://digital-strategy.ec.europa.eu/en/factpages/lithuania-2025-digital-decade-country-report>.
101. Europos duomenų apsaugos valdyba (2022-07-28). *EDAV-EDAPP Bendra nuomonė 4/2022 dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės* [interaktyvus]. https://www.edpb.europa.eu/system/files/2023-02/edpb_edps_jointopinion_202204_csam_lt.pdf.
102. Europos Komisija (2020-02-19). *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Europos duomenų strategija*, COM(2020) 66 final [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52020DC0066>.
103. Europos Komisija (2021-03-09). *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: 2030 m. skaitmeninės politikos kelrodis: Europos skaitmeninio dešimtmečio kelias*, COM(2021) 118 final [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52021DC0118>.
104. Europos Komisija (2021-12-10). *Komisijos ataskaita Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Pagrindinių teisių apsauga skaitmeniniame amžiuje, 2021 m. metinė ES pagrindinių teisių chartijos taikymo ataskaita*, COM(2021) 819 final [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52021DC0819>.

105. Europos Komisija (2022-02-23). *Duomenų aktas. Komisija siūlo teisingos ir novatoriškos duomenų ekonomikos priemonės* [interaktyvus]. https://ec.europa.eu/commission/presscorner/detail/lt/ip_22_1113.
106. Europos Komisija (2022-05-11). *Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės, COM/2022/209 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM%3A2022%3A209%3AFIN>.
107. Europos Komisija (2025-11-12). *Kova su internetine dezinformacija* [interaktyvus]. <https://digital-strategy.ec.europa.eu/lt/policies/online-disinformation>.
108. Europos Komisija (2025-11-19). *Elgesio kodeksai pagal Skaitmeninių paslaugų aktą* [interaktyvus]. <https://digital-strategy.ec.europa.eu/lt/policies/dsa-codes-conduct>.
109. Europos Komisija (2025-11-19). *Europos duomenų strategija* [interaktyvus]. <https://digital-strategy.ec.europa.eu/lt/policies/strategy-data>.
110. Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys), COM/2025/837 final* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0837>.
111. Europos Komisija (2025-11-19). *Pasiūlymas: Europos Parlamento ir Tarybos reglamentas kuriuo dėl suderintų dirbtinio intelekto taisyklių įgyvendinimo supaprastinimo iš dalies keičiami Reglamentai (ES) 2024/1689 ir (ES) 2018/1139, (Bendrasis skaitmeninės srities dokumentų rinkinys dėl dirbtinio intelekto)* [interaktyvus]. <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52025PC0836>.
112. Gaia-X (n.d.). *About Gaia-X* [interaktyvus]. <https://gaia-x.eu/about/>.
113. Gartner (2025-08-06). *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5% in 2024* [interaktyvus]. <https://www.gartner.com/en/newsroom/press-releases/2025-08-06-gartner-says-worldwide-iaas-public-cloud-services-market-grew-22-point-5-percent-in-2024>.
114. IN'T VELD, Sophie (2025-01-31). *An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?* [interaktyvus]. <https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/>.

115. LEDWON, Benjamin ir DAVID, Torben (2019-11-15). *A sovereign cloud and data infrastructure for Germany and Europe* [interaktyvus]. https://www.bitkom.org/sites/default/files/2019-11/20191115_key-points-for-a-sovereign-cloud-infrastructure-in-germany-and-_.pdf.
116. Privacy International (PI) (2024-03-01). *Privacy International's submission for the UNSR on racism's thematic report on artificial intelligence (AI) and racial discrimination* [interaktyvus]. https://privacyinternational.org/sites/default/files/2024-05/PI%20submission%20on%20AI%20and%20racial%20discrimination%20to%20UNSR%20on%20racism%20on%20AI_March%202024.pdf.
117. RENGERVE, Helene (2025-10-13). *Changes to EU Law Will Undermine Corporate Accountability. Reduced Scope, Obstacles to Civil Liability Hollow Out Law's Effectiveness* [interaktyvus]. <https://www.hrw.org/news/2025/10/13/changes-to-eu-law-will-undermine-corporate-accountability>.
118. ROUSSI, Antoaneta (2023-11-25). *How Europe became the Wild West of spyware* [interaktyvus]. <https://www.politico.eu/article/how-europe-became-wild-west-spyware/>.
119. Steering Committee on Media and Information Society (CDMSI) (2025-12-05). *Resisting Disinformation: ten building blocks to strengthen information integrity* [interaktyvus]. <https://rm.coe.int/cdmsi-2025-17rev-e-clean-resisting-disinformation-10-building-blocks-f/488029df7d>.
120. U.S. Department of State. (2024-05-06). *Building Digital Solidarity: The United States International Cyberspace & Digital Policy Strategy* [interaktyvus]. <https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/>.
121. United Nations (2011-05-16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)* [interaktyvus]. <https://docs.un.org/en/A/HRC/17/27>.
122. United Nations (2015-02-10). *Resolution adopted by the General Assembly on 18 December 2014. 69/166. The right to privacy in the digital age* [interaktyvus]. <https://docs.un.org/en/A/RES/80/215>.
123. United Nations (2025-12-22). *Resolution adopted by the General Assembly on 18 December 2025. 80/215. Promotion and protection of human rights in the context of digital technologies* [interaktyvus]. <https://docs.un.org/en/A/RES/80/215>.

Enciklopediniai, informaciniai ir statistiniai šaltiniai:

124. Valstybinė duomenų apsaugos inspekcija (2026-03-05). 2025 m. veiklos ataskaita [interaktyvus].
https://vdai.lrv.lt/public/canonical/1772605397/1298/2025m_VDAI_veiklos_ataskaita_galutinis.pdf.
125. Valstybinė duomenų apsaugos inspekcija (2025-08-08). *2024 m. asmens duomenų apsaugos priežiūros Lietuvoje apžvalga* [interaktyvus].
https://vdai.lrv.lt/public/canonical/1754559815/1040/Ataskaita_EDAV_2024.pdf.
126. World Economic Forum (2026-01-14). *Global Risks Report 2026* [interaktyvus].
https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf.

SANTRAUKA

Skaitmeninio suvereniteto iššūkiai žmogaus teisių apsaugai pagal tarptautinę ir ES teisę

Greta Činčikaitė

Magistro darbe analizuojami skaitmeninio suvereniteto keliami iššūkiai žmogaus teisių apsaugai Europos Sąjungos ir tarptautinės teisės kontekste. Darbo tikslas – išnagrinėti skaitmeninio suvereniteto sampratą, įvertinti jo potencialą stiprinant žmogaus teises bei nustatyti jo keliamus pavojus. Darbe atlakama ES teisės aktų, tarptautinių žmogaus teisių standartų, teismų praktikos ir „minkštosios teisės“ dokumentų analize.

Pirmojoje darbo dalyje nagrinėjama skaitmeninio suvereniteto sąvoka ir jos raida, įskaitant perėjimą nuo klasikinio teritorinio suvereniteto supratimo prie šiuolaikinio skaitmeninės aplinkos reguliavimo. Trumpai analizuojami įvairių valstybių požiūriai į skaitmeninės erdvės reguliavimą, siekiant nustatyti ES modelio ypatumus.

Antrojoje dalyje nagrinėjamas skaitmeninio suvereniteto vaidmuo stiprinant žmogaus teisių apsaugą. Nustatyta, kad žmogaus teisės taikomos skaitmeninėje erdvėje, o jų tolesnis aiškinimas vyksta per teismų praktiką. ES reguliavimas užtikrina asmens duomenų kontrolę ir stiprina pasitikėjimą skaitmenine aplinka. Be to, ES nustatyti standartai daro įtaką už Sąjungos ribų.

Trečiojoje dalyje analizuojami skaitmeninio suvereniteto keliami pavojai žmogaus teisėms. Nustatoma, kad įgyvendinant skaitmeninį suverenitetą, gali išnykti riba tarp leistinų teisių apribojimų ir masinio stebėjimo praktikos, taip pat dėmesys gali būti nukreiptas technologijų vystymui, o ne asmens teisių apsaugai. Daroma išvada, kad pagrindinės grėsmės kyla ne dėl skaitmeninio suvereniteto siekio, o dėl jo įgyvendinimo būdų.

Apibendrinant nustatyta, kad skaitmeninis suverenitetas yra dvejopas reiškiny, kurio poveikis žmogaus teisėms priklauso nuo taikomų teisinių mechanizmų pobūdžio. Veiksminga žmogaus teisių apsauga įmanoma, jei sustiprinamos teisinės garantijos, laikomasi proporcingumo principo ir formuojamas reguliavimas, orientuotas į žmogaus teisių apsaugą.

SUMMARY

Digital Sovereignty Challenges for Human Rights Protection under International and EU Law

Greta Činčikaitė

This master's thesis analyses the challenges posed by digital sovereignty to the protection of human rights in the context of European Union and international law. The aim – is to examine the concept of digital sovereignty, assess its potential for strengthening human rights and identify the risks it poses. The thesis is based on an analysis of EU legislation, international human rights standards, case law, and “soft law” documents.

The first part examines the concept of digital sovereignty and its evolution from the classical territorial understanding of sovereignty to the contemporary regulation of the digital environment. The cases of various states on the regulation of the digital space are briefly analysed to identify the EU model.

The second part examines the role of digital sovereignty in strengthening the protection of human rights. It is established that human rights apply in the digital space, and their further interpretation takes place through judicial practice. EU regulation ensures control over personal data and strengthens trust in the digital environment. Furthermore, the EU standards have an impact beyond the Union's borders.

The third section analyses the threats to human rights posed by digital sovereignty. Noted, that implementing digital sovereignty, the line between permissible restrictions on rights and mass surveillance practices may blur, and the focus may shift toward technological development rather than the protection of individual rights. Concluded, that the main threats arise not from the pursuit of digital sovereignty itself, but from the methods used to implement it.

In summary, digital sovereignty is a dual phenomenon, the impact of which on human rights depends on the nature of the legal mechanisms applied. Effective protection of human rights is possible if legal safeguards are strengthened, the principle of proportionality is observed, and regulations focused on the protection of human rights are developed.