Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Gretos Gužauskaitės
V kurso, Tarptautinės ir Europos Sąjungos
Studijų šakos studentės

Magistro darbas

Europos Sąjungos valstybių narių įgaliojimų apimtis užtikrinant asmens duomenų tvarkymą ir privataus gyvenimo apsaugą elektroninių ryšių sektoriuje

The scope of the powers of European Union member states to ensure the protection of personal data and privacy in the electronic communications sector

Vadovė: doc. dr. Deimilė Prapiestytė

Recenzentė: asist. dr. Laura Paškevičienė

Vilnius
2025

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame magistro darbe sistemiškai analizuojami privatumo ir asmens duomenų apsaugos aspektai elektroninių ryšių sektoriuje, ypatingą dėmesį skiriant fundamentalių teisių ribojimo teisiniams pagrindams bei šioms riboms taikomiems proporcingumo ir teisėtumo principams. Darbo tikslas – identifikuoti teisėkūros ir praktikos aspektus, lemiančius, kokiomis sąlygomis ir kokia apimtimi valstybės gali teisėtai riboti teisę į privatų gyvenimą elektroninių ryšių srityje. Siekiama nustatyti, kaip užtikrinamas teisinis balansas tarp asmens teisių apsaugos ir teisėtų viešojo intereso tikslų, tokių kaip nacionalinis saugumas ar nusikalstamumo prevencija. Analizėje vertinami skirtingų ES valstybių narių teisiniai sprendimai, atskleidžiant tiek jų suderinamumo, tiek fragmentacijos tendencijas bei grėsmes vidaus rinkos integralumui. Ypatingas dėmesys skiriamas teisinių išimčių taikymo sąlygų aiškumui, riboms ir priežiūros mechanizmams, taip siekiant užtikrinti, kad valstybės veiksmai nepažeistų pamatinių žmogaus teisių.

Pagrindiniai žodžiai: privatumas, asmens duomenys, elektroniniai ryšiai, teisės ribojimai, Europos Sąjungos teisė, BDAR, e. privatumo direktyva.

This Master's thesis provides a systematic analysis of privacy and personal data protection issues in the electronic communications sector, with a particular focus on the legal foundations and limits of restricting fundamental rights. The main aim of the thesis is to examine under which legal conditions and to what extent the right to privacy may be lawfully restricted by member states while preserving a necessary balance between individual rights and legitimate public interest goals, such as national security or crime prevention. The study evaluates the current legislative and judicial practices across EU member states, highlighting both harmonization and fragmentation trends, as well as the implications these have for the integrity of the internal market. Special emphasis is placed on assessing the clarity and proportionality of exceptions, the conditions under which they may be applied, and the role of independent oversight mechanisms in ensuring full compliance with fundamental rights.

Keywords: privacy, personal data, electronic communications, legal restrictions, European Union law, GDPR, e. privacy directive.

Turinys

Įžanga

Šiandien skaitmeninė erdvė skatina permąstyti tradicinius privatumo ir konfidencialumo principus, nes kiekvienas žmogaus žingsnis joje palieka neišdildomą pėdsaką. Technologinė pažanga, kuri ne tik palengvina kasdienį bendravimą bei suteikia plačias galimybes informacijos sklaidai ir komunikacijai, kartu kelia rimtų iššūkių asmens duomenų apsaugai. Šiame kontekste vis dažniau kyla klausimas – kiek šiandien dar egzistuoja asmens privatumo ribos, ir kur prasideda viešoji erdvė, kurioje individų gyvenimai tampa stebimi, analizuojami ir kontroliuojami. Šioje skaitmenizuotoje kasdienybėje informacija tampa jautriu ir vertingu ištekliumi, kuris lengvai gali būti panaudotas tiek individo naudai, tiek ir prieš jį patį. Kartu šios aplinkybės skatina teisines sistemas ieškoti naujų balansų tarp žmogaus teisės į privatumą ir visuomenės saugumo interesų. Iš esmės tai reiškia poreikį iš naujo įvertinti, kaip užtikrinti, jog svarbūs valstybės saugumo ir nusikalstamumo prevencijos tikslai nebūtų realizuojami neproporcingai aukojant teisę į privatų gyvenimą ir asmens duomenų apsaugą. Tai ne tik filosofinė ar teorinė problema, bet ir praktinė būtinybė, nes pernelyg plačios ar neaiškios privatumo ribojimo sąlygos gali pažeisti asmens teisės principus ir mažinti piliečių pasitikėjimą valstybės institucijomis ir teisine sistema apskritai. Todėl tampa aktualu išanalizuoti, kaip subtiliai ir tiksliai suformuoti teisinius mechanizmus ir išimtis, kurios leistų valstybės institucijoms veikti efektyviai, bet kartu išliktų aiškios, skaidrios ir nuoseklios. Šis magistro darbas atveria intriguojančią mokslinės ir praktinės diskusijos erdvę, kur teisiniai principai, technologinės galimybės bei visuomeniniai poreikiai susipina, iškeldami esminius klausimus apie privatumo ir konfidencialumo sampratos pokyčius šiuolaikinėje skaitmeninėje visuomenėje. Darbe analizuojami privatumo apsaugos pagrindai ir iššūkiai, kylantys derinant asmens teises su visuomenės interesais, kartu skatinant aktualias diskusijas teisinėje ir socialinėje skaitmeninio amžiaus aplinkoje.

Temos aktualumas. Asmens duomenų apsauga elektroninių ryšių sektoriuje – aktuali tema šiuolaikinėje skaitmeninėje visuomenėje, kurioje informacinės technologijos ne tik palengvina komunikaciją, bet ir kelia rimtų iššūkių asmenų privatumui. Didėjantis asmens duomenų rinkimo ir tvarkymo mastas reikalauja veiksmingo teisinio reguliavimo, užtikrinančio tinkamą duomenų apsaugą bei pusiausvyrą tarp asmens teisės į privatumą ir viešųjų interesų, tokių kaip nacionalinis saugumas ar teisėsaugos poreikiai. Europos Sąjungoje (toliau – **ES**) šią sritį reglamentuoja 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (toliau – **BDAR**) ir 2002 m. liepos 12 d.

Europos Parlamento ir Tarybos Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (toliau – **e. privatumo direktyva** arba **Direktyva 2002/58/EB**), tačiau jų taikymo ribos bei sąveika kelia daug teisinių klausimų. Magistro darbe ypač daug dėmesio skiriama e. privatumo direktyvos 15 straipsnio 1 dalies įgyvendinimui, kuris leidžia valstybėms narėms tam tikromis aplinkybėmis riboti privatumo apsaugą, tačiau šios išimtys turi būti taikomos laikantis būtinumo ir proporcingumo principų. Atsižvelgiant į jurisprudenciją ir valstybių narių praktikas, kyla svarbūs klausimai dėl teisinio reguliavimo aiškumo ir jo taikymo ribų. Darbo temos aktualumas atsiskleidžia būtent per šių klausimų analizę – kaip suderinamas nacionalinis ir ES teisės reguliavimas? Kokie iššūkiai kyla užtikrinant asmens duomenų apsaugą skirtingose valstybėse narėse? Kaip praktikoje taikomi šie teisės aktai?

Darbo tikslas. Išsamiai įvertinti, kaip ES valstybės narės įgyvendina e. privatumo direktyvos 15 straipsnio 1 dalį elektroninių ryšių sektoriuje. Norima išryškinti, kokios konkrečios teisės normos riboja privatumo ir konfidencialumo teises, kaip jos dera su ES pagrindiniais teisiniais principais ir kokie praktiniai iššūkiai kyla asmens duomenų apsaugos kontekste.

Darbo uždaviniai:

1. Išanalizuoti asmens duomenų apsaugos teisinį reguliavimą elektroninių ryšių sektoriuje, ypatingai dėmesį skiriant e. privatumo direktyvos ir BDAR sąveikai;
2. Nustatyti e. privatumo direktyvos 15 straipsnio 1 dalies taikymo ribas bei esminius teisėtumo kriterijus;
3. Išnagrinėti Europos Sąjungos Teisingumo Teismas (toliau – **ESTT**, **ES Teisingumo Teismas**) ir Europos Žmogaus Teisių Teismas (toliau – **EŽTT**, **Teismas**) jurisprudenciją, kuri atskleidžia, kaip praktikoje ribojamos privatumo ir konfidencialumo teisės;
4. Įvertinti skirtingų ES valstybės narės praktiką, identifikuojant pagrindinius reguliavimo iššūkius ir jų pasekmes.

Tyrimo objektas. Direktyvos 2002/58/EB 15 straipsnio 1 dalies įgyvendinimas ir taikymo praktika, susijusi su privatumo ir konfidencialumo ribojimu elektroninių ryšių sektoriuje ES ir Lietuvos teisinėje sistemoje.

Tyrimo metodai. Siekiant įgyvendinti darbo tikslą ir uždavinius, buvo taikyti šie tyrimo metodai: **teisės aktų analizės metodas** – taikytas siekiant detaliai išnagrinėti teisės normų turinį bei nustatyti jų reguliavimo apimtį ir ribas elektroninių ryšių sektoriuje; **sisteminės analizės metodas** – padėjo identifikuoti teisės aktų tarpusavio ryšius ir atskleisti jų veikimą kaip vientisos norminės struktūros dalį, vertinant BDAR, Europos Parlamento ir Tarybos

2018 m. gruodžio 11 d. direktyvos (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodekso (toliau – **Elektroninių ryšių kodeksas**, **Kodeksas**) ir e. privatumo direktyvos sąveiką; **lyginamosios (komparatyvinės) analizės metodas** – naudotas siekiant palyginti skirtingus teisinio reguliavimo aspektus ES lygiu bei valstybių narių lygmenyje, atskleidžiant nacionalinių įgyvendinimo modelių įvairovę ir jų galimą poveikį vidaus rinkos vientisumui; **jurisprudencijos analizės metodas** – taikytas tiriant ESTT praktiką, siekiant identifikuoti pagrindinius teisminės interpretacijos kriterijus bei aiškinimo tendencijas, susijusias su privatumo ribojimu; **teleologinis teisės aiškinimo metodas** – taikytas vertinant teisės normų tikslus ir paskirtį, analizuojant, kokiomis sąlygomis gali būti ribojamos privatumo teisės elektroninių ryšių kontekste pagal Direktyvą 2002/58/EB; **analizės ir sintezės metodas** – padėjo ne tik detalizuoti atskiras teisės normas ar bylas, bet ir integruoti jų turinį į bendrą probleminį kontekstą, siekiant pagrįstų darbo išvadų; **kritinė literatūros analizė** – leido apibendrinti mokslinėje doktrinoje pateikiamas nuostatas, nustatyti jų stipriąsias ir silpnąsias puses bei pateikti objektyvų teorinių pozicijų įvertinimą; **istorinis metodas** – taikytas analizuojant e. privatumo reglamento formavimosi aplinkybes ir institucinių sprendimų raidą ES teisėkūros procese.

Darbo originalumas. Šio magistro darbo originalumas atsiskleidžia per kryptingą e. privatumo direktyvos 15 straipsnio 1 dalies analizę, kurioje neapsiribojama bendro pobūdžio teorinėmis įžvalgomis, o kritiškai vertinami konkretūs ES ir nacionaliniai teisėkūros bei jurisprudencijos sprendimai dėl privatumo ribojimo sąlygų. Darbe išskirtinis dėmesys skiriamas e. privatumo ir BDAR normų sąveikai, proporcingumo principo taikymui, taip pat valstybėms narėms suteiktos diskrecijos apimčiai, kas iki šiol Lietuvos teisės moksle buvo nagrinėta fragmentiškai. Be to, lyginamoji analizė su kitų valstybių (pvz., Prancūzijos, Vokietijos) praktika ir institucine prieiga prie e. privatumo direktyvos 15 straipsnio įgyvendinimo leidžia ne tik išryškinti nacionalinio reguliavimo ypatumus, bet ir įvertinti jų poveikį ES vidaus rinkos integralumui. Tokiu būdu darbe atskleidžiamos naujos analitinės perspektyvos skaitmeninių teisių reguliavimo kontekste, grindžiamos ne tik teoriniu pagrindu, bet ir aktualių teisinių sprendimų praktiniu vertinimu.

Svarbiausi šaltiniai. Šio magistro darbo pagrindą sudaro ES ir nacionaliniai teisės aktai, reglamentuojantys asmens duomenų apsaugą ir elektroninių ryšių sektorių. Pagrindiniai nagrinėjami dokumentai apima BDAR, e. privatumo direktyvą, Elektroninių ryšių kodeksą, taip pat Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą ir Elektroninių ryšių įstatymą. Šių teisės aktų analizė glaudžiai siejama su ESTT ir EŽTT jurisprudencija, kuri padeda analizuoti privatumo ribojimo pagrįstumą ir proporcingumą. Darbas taip pat remiasi

doktrinine literatūra, įskaitant klasikinius darbus (S. Warren ir L. Brandeis *„The Right to Privacy“*, A. Westin *„Privacy and Freedom“*, W. Prosser, J. De Cew) bei naujesnius tyrimus (I. Walden *„Telecommunications Law and Regulation“*, moksliniai straipsniai *„Computer Law & Security Review”*). Svarbų indėlį sudaro ir oficialūs dokumentai – Europos duomenų apsaugos valdybos gairės**,** ENISA ataskaitos, Europos Komisijos ir Europos Audito Rūmų vertinimai, taip pat nacionalinių institucijų pateikiami duomenys. Visuma šių šaltinių leidžia kompleksiškai vertinti ne tik teisinį reguliavimą, bet ir faktinę teisės normų įgyvendinimo praktiką, analizuojant tiek centralizuotą ES požiūrį, tiek skirtingas valstybių narių praktikas bei jų poveikį teisės į privatų gyvenimą užtikrinimui elektroninių ryšių srityje.

1. Asmens duomenų apsauga ir privatumas

Šioje darbo dalyje bus nagrinėjama asmens duomenų teisinės apsaugos samprata ir jos reikšmė elektroninių ryšių sektoriuje, atsižvelgiant į ES teisinį reguliavimą bei elektroninių ryšių sektoriaus specifiką. Analizė apims asmens duomenų apibrėžties aiškinimą pagal BDAR ir Direktyvą 2002/58/EB, išskiriant duomenų kategorijas, patenkančias į šių teisės aktų taikymo sritį, bei jų reikšmę privatumo apsaugai. Taip pat bus vertinami teisės į privatų gyvenimą apsaugos aspektai elektroninių ryšių kontekste, išryškinant pagrindinius reguliavimo iššūkius, kuriuos lemia technologinė pažanga, duomenų *„suduomeninimo“* (angl. *datification*) procesas ir valstybių narių taikomos priemonės. Atskirai nagrinėjama Direktyvos 2002/58/EB 15 straipsnio 1 dalyje numatytų privatumo apsaugos ribojimų taikymo sąlygos, proporcingumo principo įgyvendinimas. Galiausiai apžvelgiama ESTT praktika, kuri formuoja teisinius standartus šių ribojimų vertinimui, kartu pabrėžiant asmens duomenų apsaugos reikšmę skaitmeninės visuomenės kontekste.

1.1. Asmens duomenų teisinės apsaugos samprata ir reikšmė elektroninių ryšių sektoriuje

Elektroninių ryšių sektoriuje asmens duomenų teisinė apsauga įgauna ypatingą aktualumą, kadangi sparčiai skaitmenizuojantis pasauliui tampa būtina užtikrinti tiek asmens privatumą, tiek visuomenės saugumą. Atitinkamai, ES teisės aktai, pavyzdžiui, Direktyva 2002/58/EB, nustato griežtus standartus, siekiant apsaugoti teisę į privatumą ir užtikrinti sąžiningą bei patikimą duomenų tvarkymo praktiką. Nepakankamai reglamentuoti duomenys gali sukelti rimtų pasekmių – diskriminaciją, reputacijos žalą ar finansinius nuostolius –, tuo tarpu patikima teisinė sistema stiprina vartotojų pasitikėjimą paslaugų teikėjais. Kadangi e. privatumo direktyva ne tik įtvirtina šiuos apsaugos standartus, bet ir numato galimybę riboti teises tam tikromis sąlygomis, esminė yra išsami analizė, kurios metu būtų aiškiai nustatytos sąlygos, leidžiančios taikyti tokias ribojimo priemones – o tai priklauso nuo tikslaus asmens duomenų apibrėžimo.

Visų pirma, pagal **BDAR 4 straipsnio 1 dalį**, asmens duomenimis laikoma bet kokia informacija, tiesiogiai ar netiesiogiai susijusi su fiziniu asmeniu, neatsižvelgiant į jos pateikimo formą ar išraiškos būdą. Tai reiškia, kad asmens duomenų sąvoką apima tiek tradiciniai identifikaciniai duomenys – vardas, pavardė, adresas, telefono numeris – tiek ir mažiau akivaizdūs duomenys, pavyzdžiui, IP adresai ar vietos nustatymo informacija. Be to, svarbu

pabrėžti, kad asmens duomenys nebūtinai turi būti materialiai užfiksuoti – jie gali būti perduodami žodžiu arba kitaip išreikšti, jei suteikia galimybę identifikuoti asmenį. Atsižvelgiant į tai, kad BDAR apibrėžia asmens duomenis plačiai, akademinėje literatūroje kyla diskusijų dėl šio apibrėžimo ribų. Pavyzdžiui, prof. dr. N. Purtova savo daktaro disertacijoje nagrinėja reiškinį, vadinamą *„suduomeninimu“*, kurio metu įvairūs gyvenimo aspektai – nuo vartotojų elgesio ir finansinių duomenų iki sveikatos rodiklių – tampa skaitmenine informacija, tinkama analizei ir panaudojimui įvairiais tikslais. Pasak Purtovos, tokia transformacija keičia suvokimą apie asmens duomenų apimtį ir jų reguliavimą, nes praktiškai bet kokia informacija gali būti laikoma asmens duomenimis, priklausomai nuo jos panaudojimo konteksto (2018, p. 41). Šiame kontekste nuolat kyla naujų iššūkių teisiniam reguliavimui, ypač kai vis plačiau taikomos duomenų analitikos ir dirbtinio intelekto technologijos, keliančios naujas grėsmes asmens privatumui. Toks situacijos dinamikos supratimas yra itin svarbus, nes jis leidžia ne tik įvertinti esamą duomenų apsaugos sistemą, bet ir identifikuoti būtinybę nuolat tobulinti teisinius standartus, kad jie atitiktų sparčiai kintančią skaitmeninę aplinką.

Atsižvelgdama į šiuos pokyčius, Europos duomenų apsaugos valdyba (toliau – **EDAV**), perėmusi buvusios 29 straipsnio darbo grupės funkcijas po BDAR įsigaliojimo, pabrėžė, kad sąmoningai buvo pasirinktas platus asmens duomenų apibrėžimas, siekiant efektyviai apsaugoti prigimtines žmogaus teises, ypač teisę į privatumą, skaitmeninės visuomenės kontekste (ES 29 str. darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007). Vis dėlto EDAV akcentuoja – asmens duomenų apsaugos taisyklių taikymo sritis neturėtų būti pernelyg plačiai išplečiama, nes tai gali sukelti perteklinio reguliavimo problemų. Griežti reikalavimai neproporcingai padidintų administracinę naštą duomenų valdytojams, apsunkintų teisinio reguliavimo aiškumą bei paskatintų teisinių spragų išnaudojimą ar net reguliacinės aplinkos fragmentaciją tarp valstybių narių. Tai ypač aktualu elektroninių ryšių sektoriui, kur operatyvus ir efektyvus duomenų tvarkymas yra būtinas ne tik mobiliojo ryšio, interneto ar kitų viešųjų ryšių paslaugų teikėjams, bet ir teisėsaugos institucijoms, siekiančioms užtikrinti nusikalstamų veikų prevenciją ir tyrimą (EDAV gairės 2/2019 dėl asmens duomenų tvarkymo, 2019). Taigi, platus asmens duomenų apibrėžimas suteikia galimybę užtikrinti įvairių informacijos rūšių apsaugą, tačiau kartu būtina aiškiai nustatyti ribas, kad būtų išvengta neproporcingų ar net perteklinių reguliavimo priemonių, kurios gali trukdyti teisėtam duomenų naudojimui.

Antra, elektroninių ryšių sektoriuje yra tvarkomi itin jautrūs asmens duomenys, kurie apima tiek tarpusavio komunikacijos turinį (pvz., siunčiamų žinučių ar pokalbių informaciją), tiek techninius duomenis – tokius kaip ryšio pradžios ir pabaigos laikas, trukmė, geografinė

vieta, iš kurios ryšys buvo užmegztas, maršrutų informacija bei kiti srauto ir lokalizacijos duomenys. Šių duomenų pobūdis leidžia daryti detalias išvadas apie individo elgseną, socialinius ryšius, judėjimą ar net asmenines pažiūras, todėl jų apsauga turi esminę reikšmę privataus gyvenimo neliečiamumui. Atsižvelgiant į šių duomenų specifiką, ES suformuotas mišrus teisinio reguliavimo modelis: viena vertus, taikomi bendrieji BDAR principai, kita vertus, elektroninių ryšių sektoriuje taikoma ir e. privatumo direktyva kaip *lex specialis* (EDAV Nuomonė 5/2019 dėl e. privatumo direktyvos ir BDAR sąveikos, 2019). Šių aktų sąveika užtikrina, kad asmens duomenų apsaugos lygis šioje srityje atitiktų tiek technologinį kontekstą, tiek privatumo poreikius. Siekiant aiškiau suprasti, kokie duomenys tvarkomi elektroninių ryšių sektoriuje ir kokią reikšmę jie turi privatumo apsaugai, būtina išnagrinėti jų rūšis ir ypatumus, įtvirtintus Direktyvoje 2002/58/EB ir BDAR. Taigi, Direktyvos 2002/58/EB 2 straipsnis išskiria tris pagrindines duomenų kategorijas – srauto duomenis, lokalizacijos duomenis ir komunikacijos turinį, o BDAR papildomai detalizuoja asmens identifikavimo aspektus ir subjekto teisių įgyvendinimą:

a) **Elektroninių ryšių turinio duomenys** arba **komunikacijos turinys** (angl. *content data of electronic communications*) – bet kokia informacija, perduodama elektroninėmis ryšio priemonėmis, pavyzdžiui, elektroniniai laiškai, tekstiniai pranešimai ar kita tiesioginė komunikacija (e. privatumo direktyvos 2 straipsnio b punktas);
b) **Srauto duomenys** (*angl. traffic data*) – techninė informacija, susijusi su elektroninių ryšių eiga, įskaitant IP adresus, ryšio laiko žymas (datą, laiką), maršrutizavimo duomenis (nurodo, kaip ir kokiu keliu buvo perduota informacija tarp siuntėjo ir gavėjo) (e. privatumo direktyvos 2 straipsnio c punktas);
c) **Lokalizacijos duomenys** arba **vietos nustatymo duomenys** (angl. *location data*) – duomenys, leidžiantys nustatyti elektroninio įrenginio geografinę buvimo vietą ir atsekti asmens judėjimo trajektorijas (e. privatumo direktyvos 2 straipsnio d punktas);
d) **Identifikavimo duomenys** (angl. *identification data*) – telefono numeriai, abonento identifikatoriai ir kiti individualūs identifikatoriai, leidžiantys tiesiogiai ar netiesiogiai nustatyti asmens tapatybę (BDAR 4 straipsnio 1 dalis). Nors identifikavimo duomenys yra atskira duomenų kategorija, praktikoje jie dažnai naudojami kartu su srauto duomenimis siekiant nustatyti asmens veiksmus elektroninių ryšių kontekste. Pavyzdžiui, srauto duomenys gali parodyti, kada ir su kuo buvo užmegztas ryšys, o identifikavimo duomenys leidžia susieti šią informaciją su konkrečiu asmeniu.

Atsižvelgiant į elektroninių ryšių sektoriuje tvarkomų duomenų pobūdį – apimančius tiek komunikacijos turinį, tiek srauto, lokalizacijos ir identifikavimo duomenis – tampa akivaizdu, jog jų tvarkymui būtinas griežtas ir subalansuotas reguliavimas. Šių duomenų apimtis ir techninė specifika lemia didelį jų jautrumą privatumo požiūriu, todėl taikomi reguliaciniai mechanizmai turi ne tik užtikrinti tinkamą asmens duomenų apsaugą, bet ir suderinti ją su teisėsaugos bei nacionalinio saugumo interesais (Valstybinė duomenų apsaugos inspekcija, 2019). Tiek BDAR, tiek e. privatumo direktyva aiškiai įtvirtina, kad tokių duomenų rinkimas ir naudojimas turi būti grindžiamas apibrėžtais principais – visų pirma, duomenys turi būti tvarkomi tik konkrečiais, aiškiai apibrėžtais ir teisėtais tikslais, tokiais kaip paslaugų teikimas, viešojo saugumo užtikrinimas ar teisėsaugos poreikių tenkinimas. Tačiau praktikoje viena iš sudėtingiausių teisinių dilemų kyla dėl e. privatumo direktyvos 15 straipsnio taikymo – ši nuostata suteikia valstybėms narėms teisę numatyti papildomas duomenų saugojimo priemones ir tam tikrais atvejais riboti privatumo teises, o toks reguliavimas neišvengiamai kelia iššūkių bandant suderinti teisėtus nacionalinio saugumo ir baudžiamosios politikos tikslus su pagrindinėmis asmens teisėmis į privatumą ir duomenų apsaugą, kurios yra įtvirtintos tiek BDAR, tiek Europos Sąjungos pagrindinių teisių chartijoje (toliau – **Chartija**).

ESTT savo jurisprudencijoje yra aiškiai apibrėžęs šių ribų svarbą – bendro pobūdžio ir nediferencijuotas elektroninių ryšių duomenų saugojimas pažeidžia Chartijos 7 ir 8 straipsniuose įtvirtintas teises, nes neatitinka proporcingumo principo ir nėra pagrįstas objektyviu būtinybės kriterijumi (ESTT, *Digital Rights Ireland*, C-293/12, C-594/12, p. 65; ESTT, *Bezirkshauptmannschaft Landeck*, C-548/21). Todėl asmens duomenų apsaugos reikšmė elektroninių ryšių sektoriuje neapsiriboja vien individualių teisių gynimu – ji tampa esmine demokratinės visuomenės funkcionavimo sąlyga, susijusia su skaidrumu, pasitikėjimu institucijomis ir žmogaus orumo apsauga (Petraitytė, 2013, p. 144). ES teisinėje sistemoje ši apsauga įtvirtinta kaip savarankiška teisė pagal Chartijos 8 straipsnį ir detaliai reglamentuojama BDAR, kuris užtikrina vieningą duomenų apsaugos standartą visoje Sąjungoje. Šiuo požiūriu asmens duomenų apsauga tampa integralia elektroninių ryšių sektoriaus dalimi, kurioje būtina užtikrinti pusiausvyrą tarp efektyvaus paslaugų teikimo ir aukštų privatumo apsaugos standartų. Galiausiai, kaip pastebi teisės mokslų daktaras M. Vasiliauskas, duomenų apsaugos reguliavimą galima vertinti kaip prevencinę sistemą, kurios tikslas – ne tik saugoti individų privatumą, bet ir valdyti rizikas, kylančias tvarkant jautrius elektroninių ryšių duomenis, taip prisidedant prie visuomenės saugumo ir teisės viršenybės principo įgyvendinimo (Vasiliauskas, 2020).

1.2. Teisės į privataus gyvenimo apsaugą turinys

Elektroninių ryšių sektoriuje asmens duomenų apsauga ir teisė į privataus gyvenimo neliečiamumą yra glaudžiai persipynusios. Technologijų pažanga ir sparčiai besivystanti skaitmeninė aplinka paskatino didžiulį duomenų tvarkymo mastą bei iškėlė naujus privatumo apsaugos iššūkius. Šiuolaikinėje visuomenėje privatumas ir asmens duomenų apsauga tapo kertiniais principais, siekiant apsaugoti individą nuo perteklinės valstybės ar privačių subjektų intervencijos (ES Tarybos patvirtintos ES gairės dėl saviraiškos laisvės internete ir realiame gyvenime, 2014). Teisė į privataus gyvenimo apsaugą – tai ne tik pamatinė žmogaus teisė, bet ir vienas pagrindinių elementų, įtvirtinančių pasitikėjimą informacinėmis technologijomis ir elektroninių ryšių paslaugomis. Ji grindžiama tiek tarptautiniais žmogaus teisių dokumentais, tiek ES ir nacionalinės teisės aktais, kurie skirti užtikrinti, kad asmens duomenų tvarkymas vyktų teisėtai ir proporcingai. Šios darbo dalies tikslas – atskleisti teisės į privataus gyvenimo apsaugą turinį, išnagrinėti, kaip ši teisė yra interpretuojama teisės doktrinoje, tarptautiniuose dokumentuose ir teismų praktikoje, ir kokią reikšmę ji įgauna elektroninių ryšių sektoriuje. Taip pat bus aptariama teisės į privatumą raida ir samprata mokslinėje literatūroje, o vėliau analizuojama, kaip ši teisė įtvirtinama Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje, pasirašytoje 1950 m. lapkričio 4 d. Romoje, įsigaliojusioje 1953 m. rugsėjo 3 d. (toliau – **EŽTK**, **Konvencija**), ES teisėje ir Lietuvos konstitucinėje jurisprudencijoje.

Pirmiausia – teisė į privataus gyvenimo apsaugą yra prigimtinė žmogaus teisė. S. Warren ir L. D. Brandeis buvo vieni pirmųjų, kurie išskyrė šią teisę ir gilinosi į jos turinį. Savo straipsnyje *„Teisė į privatumą“* jie apibrėžė ją kaip *„teisę būti paliktam vienam“* (Warren ir Brandeis, 1890). Teisės į privatumą samprata toliau buvo aktyviai plėtojama Jungtinių Amerikos Valstijų teisės mokslininkų – W. Prosser šią teisę susiejo su asmens apsauga nuo trikdančios informacijos ir iškreiptų faktų apie asmenį paviešinimo (Prosser, 1960, p. 392). A. Westin privatumą apibūdino kaip asmens galimybę nuspręsti, kada, kokiu būdu ir kokios apimties informacija apie jį gali būti pateikiama kitiems (Westin, 1967, p. 7). W. Parent privatumą apibūdino kaip būseną, kai kiti neturi ar nežino informacijos apie asmenį, kurios nėra viešuose įrašuose (Parent, 1983, p. 346). J. De Cew privatumą apibrėžė kaip sudėtinę sampratą, apimančią informacijos apie save patį ir fizinio bei psichinio neliečiamumo kontrolę, taip pat galimybę priimti svarbius sprendimus šeimos ir gyvenimo būdo klausimais (DeCew, 1997, p. 62).

Asmens teisė į privatumą, sulaukusi mokslinio pripažinimo, buvo įtvirtinta tarptautiniuose teisės aktuose. Vienas pirmųjų šią teisę reglamentuojančių dokumentų yra

Visuotinė žmogaus teisių deklaracija, kurios 12 straipsnyje nustatyta – asmens privatumas, šeimos gyvenimas, buitis ir susirašinėjimas negali būti savavališkai pažeidžiami ar ribojami, o nepagrįstas kišimasis į asmens garbę ir reputaciją yra draudžiamas, kartu užtikrinant teisę į įstatymo apsaugą nuo tokių veiksmų (ES Tarybos patvirtintos ES gairės dėl saviraiškos laisvės internete ir realiame gyvenime, 2014). Kitas aktualus tarptautinis dokumentas, reglamentuojantis teisę į privataus gyvenimo apsaugą ir darantis tiesioginę įtaką asmens duomenų tvarkymo praktikai elektroninių ryšių sektoriuje, yra EŽTK, kurios 8 straipsnyje aiškiai įtvirtinama, kad kiekvienas asmuo turi teisę į privataus ir šeimos gyvenimo, būsto neliečiamumo bei susirašinėjimo slaptumo apsaugą, tačiau ši teisė gali būti ribojama tik įstatymų nustatytais pagrindais – kai tai būtina demokratinėje visuomenėje siekiant apsaugoti valstybės saugumą, viešąją tvarką, ekonominę gerovę ar kitų asmenų teises ir laisves. Šios nuostatos įgyja ypatingą reikšmę elektroninių ryšių sektoriuje, kur didelės apimties asmens duomenų tvarkymas tiesiogiai veikia privataus gyvenimo neliečiamumą.

Kadangi pagrindinis šio darbo tyrimo objektas yra ES teisė, EŽTT jurisprudencijos įtraukimas yra pagrįstas keliomis svarbiomis priežastimis. Pirma, tiek BDAR, tiek e. privatumo direktyva turi būti aiškinami atsižvelgiant į pagrindines teises, įtvirtintas Chartijoje, kurios 7 ir 8 straipsniai atitinka EŽTK 8 straipsnio turinį. Be to, ES Teisingumo Teismas savo sprendimuose dažnai remiasi EŽTT praktika, kurią interpretuoja kaip orientacinę bei papildomą nuorodą žmogaus teisių kontekste. Galiausiai, daugelyje ES valstybių narių teismai ir priežiūros institucijos vertina tiek ES teisę, tiek EŽTT formuojamą standartą siekdamos užtikrinti kuo aukštesnį pagrindinių teisių apsaugos lygį. Atsižvelgiant į tai, darbe EŽTT jurisprudencija naudojama kaip papildomas šaltinis, padedantis atskleisti teisės į privatų gyvenimą turinį elektroninių ryšių sektoriuje bei įvertinti, ar teisėtų šios teisės ribojimų priemonių proporcingumas yra tinkamai įgyvendintas. Taigi, EŽTT ne kartą yra pabrėžęs, jog teisės į privataus gyvenimo apsaugą sąvoka apima ne tik asmenybės raidą tarpasmeniniuose santykiuose (EŽTT, 1992, *Niemietz* prieš Vokietiją), asmens fizinį ir psichologinį vientisumą (EŽTT, 1985, *X* ir *Y* prieš Nyderlandus), seksualinę orientaciją (EŽTT, 1983, *Dudgeon* prieš JK), lytinį gyvenimą ar informaciją apie asmenį, bet ir asmens komunikacijos slaptumą bei ryšių konfidencialumą, kurie yra ypač svarbūs skaitmeninėje erdvėje (EŽTT, 2000, *Rotaru* prieš Rumuniją). Būtent todėl EŽTT praktika tampa reikšmingu atskaitos tašku vertinant, kaip valstybės narės įgyvendina savo įgaliojimus asmens duomenų apsaugos ir privataus gyvenimo srityse, įskaitant elektroninių ryšių sektorių. Tolimesnėse šio darbo dalyse bus detaliau analizuojama EŽTT jurisprudencija, atskleidžiant, kaip Teismas formuoja pusiausvyrą tarp valstybės teisėtų interesų ir asmens teisės į privatumą skaitmenizuotoje aplinkoje.

Tuo pačiu svarbu pabrėžti, jog atskleisdamas Lietuvos Respublikos Konstitucijos 22 straipsnio turinį, Lietuvos Respublikos Konstitucinis Teismas (toliau – **LRKT**) konstatavęs – privataus gyvenimo sąvoka apima asmens teisėtus lūkesčius privatumo srityje ir yra siejama su situacijomis, kai asmuo gali pagrįstai tikėtis privatumo apsaugos (LRKT 2000 m. gegužės 8 d. nutarimas). LRKT, tolygiai vartodamas teisės į privatų gyvenimą ir teisės į privatumą (LRKT 2004 m. gruodžio 29 d. nutarimas) sąvokas, pabrėžia, jog ši teisė apima asmens ir šeimos gyvenimą, namų neliečiamumą, fizinę ir psichinę neliečiamybę, asmens garbę ir reputaciją, konfidencialių asmens duomenų apsaugą bei draudimą nepagrįstai skelbti ar rinkti privačią informaciją. Tarptautiniuose ir nacionaliniuose teisės aktuose bei teismų praktikoje formuojama nuostata, jog asmens duomenų apsauga yra sudedamoji teisės į privatų gyvenimą apsaugos dalis. Informacija apie asmenį – vardas, pavardė, gyvenamoji vieta, išsilavinimas ar kiti asmens tapatybę nustatantys duomenys – paprastai laikoma asmens duomenimis. Todėl bet koks šių duomenų rinkimas, saugojimas ar naudojimas tiesiogiai veikia individo privatumą ir reikalauja visapusiškos apsaugos (Štitilis, Krikščiūnas ir Petrauskas, 2005, p. 22).

Teisės į privataus gyvenimo apsaugą įgyvendinimas elektroninių ryšių sektoriuje yra ne tik teisinės, bet ir praktinės svarbos klausimas, nes šioje aplinkoje asmens duomenys gali būti tvarkomi tiek aktyviai (asmenų iniciatyva), tiek pasyviai (valdytojų veiksmais ar sisteminiais procesais) (Computer Law & Security Review, 2020). **Aktyvūs veiksmai** – tai tokie, kurie priklauso nuo pačių asmenų pasirinkimų. Pavyzdžiui, teisė laisvai rinktis komunikacijos priemones ar savarankiškai konfigūruoti privatumo nustatymus yra įgyvendinama individualiais veiksmais. Kita vertus, **pasyviąją privatumo apsaugos dalį** lemia trečiųjų šalių elgesys, visų pirma elektroninių ryšių paslaugų teikėjų ir kitų duomenų valdytojų atsakomybė susilaikyti nuo neteisėtų veiksmų, galinčių pažeisti asmens privatumą, tokių kaip neteisėtas duomenų rinkimas, saugojimas ar naudojimas. Elektroninių ryšių sektoriuje privatumo ribas lemia įvairūs veiksniai. **Aktyvioji pusė** apima paties asmens sprendimus, tokius kaip viešas asmeninės informacijos skelbimas socialiniuose tinkluose ar nesaugių ryšio priemonių naudojimas. **Pasyvioji pusė** apima situacijas, kai technologiniai sprendimai ar valdytojų veiksmai tiesiogiai nulemia duomenų apsaugos lygį – kaip antai, kai automatizuotai kaupiami metaduomenys, atliekamas profiliavimas ar vykdoma duomenų analizė. Skaitmeninėje erdvėje informacija gali būti atkurta ar panaudota net ir po ilgo laiko, todėl privatumo apsauga reikalauja abiejų priemonių – tiek pasyvaus duomenų valdytojų susilaikymo nuo perteklinio kišimosi, tiek aktyvių apsaugos mechanizmų diegimo. Pastarieji apima šifravimą, duomenų minimizavimą, anonimizavimą bei kitų technologinių sprendimų

taikymą, leidžiančių užtikrinti aukštą privatumo apsaugos lygį (Computer Law & Security Review, 2020).

Be kita ko, asmens duomenų apsauga atlieka esminį vaidmenį įgyvendinant teisę į privatų gyvenimą, nes ši apsauga nustato standartus, kurių turi laikytis elektroninių ryšių paslaugų teikėjai ir kiti duomenų valdytojai, kad jų veikla būtų laikoma atitinkančia teisės į privatų gyvenimą principus. Elektroninių ryšių sektoriuje tai svarbu, nes čia tvarkomi ne tik komunikacijos turinio duomenys, bet ir jautrūs srauto, lokalizacijos ar identifikavimo duomenys, leidžiantys atskleisti asmenų veiklos modelius ir judėjimo trajektorijas, tačiau svarbu nepamiršti, jog duomenų apsaugos mechanizmai šioje srityje nėra savitiksliai. Jie kyla iš pačios teisės į privatų gyvenimą esmės – asmens duomenų apsauga yra praktinis šios teisės įgyvendinimo mechanizmas informacinėje visuomenėje. Asmenys turi teisę spręsti, kokiu mastu ir kokiomis priemonėmis naudotis privatumo apsauga, tačiau jų galimybės efektyviai kontroliuoti savo duomenis priklauso ir nuo tinkamo sektoriaus reguliavimo bei paslaugų teikėjų elgesio (ES Tarybos patvirtintos ES gairės dėl saviraiškos laisvės internete ir realiame gyvenime, 2014). Elektroninių ryšių sektoriuje išaugęs duomenų srautų apdorojimas, automatizuoti sprendimų priėmimo procesai bei stebėsenos technologijos paskatino plėtoti specifinį sektoriaus reguliavimą. Asmens duomenų apsaugos tikslas nėra stabdyti inovacijas ar technologinę pažangą, bet užtikrinti, kad naudojamos priemonės nepažeistų pamatinių žmogaus teisių ir teisėtų interesų. Šiame kontekste reikšmingą vaidmenį atlieka e. privatumo direktyva, kuri detalizuoja asmens duomenų apsaugos reikalavimus elektroninių ryšių paslaugų teikėjams, nustatydama griežtesnius standartus dėl duomenų saugojimo, stebėjimo priemonių naudojimo ir reklaminio sekimo.

EŽTT jurisprudencija, be kita ko, išplėtė teisės į privatų gyvenimą turinį, ne kartą konstatavus, jog vien duomenų rinkimas ir saugojimas elektroninių ryšių sektoriuje gali būti laikomas kišimusi į privatų gyvenimą, net jei tie duomenys vėliau nėra aktyviai naudojami (EŽTT, 2000, *Amann* prieš Šveicariją, 2000, p. 69). Todėl valstybės, reguliuodamos šį sektorių, privalo užtikrinti, kad jų priimamos priemonės atitiktų griežtus ES teisėje įtvirtintus privatumo ir proporcingumo standartus. Kaip jau buvo minėta, EŽTK taikymo kontekste ypatingą reikšmę turi EŽTT praktika, kuri formuoja privatumo ribojimo standartus ne tik Konvencijos taikymo ribose, bet ir daro poveikį Europos Sąjungos teisės raidai. EŽTT savo sprendimuose sistemingai vertina, ar valstybių ribojimai privatumo srityje yra būtini ir proporcingi. Nagrinėdamas bylas, Teismas analizuoja šiuos aspektus:

a) ar buvo **aiškiai apibrėžtas** duomenų rinkimo ir naudojimo teisinis pagrindas;
b) kokių **apsaugos mechanizmų** buvo imtasi;

c) kokio pobūdžio duomenys buvo **kaupiami** ir kaip jie buvo **naudojami**;
d) kokias **pasekmes** tai sukėlė asmens teisėms.

Sprendimuose *Malone* prieš JK (EŽTT, 1984, Nr. 8691/79), *Copland* prieš JK (EŽTT, 2007 m. sausio 3 d., Nr. 62617/00) ir *Tanrıkulu* prieš Turkiją (EŽTT, 1999 m. liepos 8 d., Nr. 23763/94) buvo suformuluoti esminiai reikalavimai, pagal kuriuos privatumo ribojimai, įskaitant elektroninių ryšių stebėjimą be aiškaus teisinio pagrindo, laikytini prieštaraujančiais EŽTK 8 straipsniui. Vėlesniuose sprendimuose, tokiuose kaip *Zakharov* prieš Rusiją (EŽTT, 2015, Nr. 47143/06) bei *Szabó* ir *Vissy* prieš Vengriją (EŽTT, 2016, Nr. 37138/14), buvo analizuoti plataus masto slaptos telekomunikacijų stebėsenos atvejai. *Zakharov* byloje Teismas konstatavo, kad Rusijos teisinis reguliavimas nesuteikė pakankamų garantijų nuo piktnaudžiavimo slaptu sekimu, o *Szabó* ir *Vissy* byloje nuspręsta, jog Vengrijos vykdomas sekimas, grindžiamas nacionalinio saugumo argumentu, nebuvo pakankamai apribotas įstatymu ir stokojo nepriklausomos kontrolės. Atitinkamai, ES Teisingumo Teismas savo sprendimuose taip pat rėmėsi panašiais principais, ir EŽTT praktika darė aiškią įtaką ES teisės aiškinimui. Pavyzdžiui, byloje *Digital Rights Ireland Ltd* prieš Airiją (ESTT, 2014, sujungtos bylos C-293/12 ir C-594/12) buvo vertinamas 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvos 2006/24/EB dėl tam tikrų duomenų, gaunamų ar tvarkomų teikiant viešąsias elektroninių ryšių paslaugas ar viešuosius ryšių tinklus, saugojimo ir ja iš dalies keičiama Direktyva 2002/58/EB (toliau – **Direktyva 2006/24/EB**, **duomenų saugojimo direktyva**) atitikimas pagrindinių teisių apsaugos standartams. ESTT konstatavo, kad Direktyva 2006/24/EB nesuteikė tinkamų apsaugos mechanizmų nuo perteklinio kišimosi į privatų gyvenimą, todėl ją pripažino negaliojančia. Taigi, tiek EŽTT, tiek ESTT savo jurisprudencijoje nuosekliai pabrėžia, kad privatumo apsauga elektroninių ryšių srityje apima ne tik valstybės institucijų pareigą susilaikyti nuo perteklinio kišimosi, bet ir pozityvią pareigą užtikrinti, kad tiek viešieji, tiek privatūs subjektai laikytųsi aukštų privatumo bei asmens duomenų apsaugos standartų.

Apibendrinant šios darbo dalies analizę, galima išskirti kelias esmines išvadas. Pirma, elektroninių ryšių sektoriuje asmens duomenų apsauga įgauna ypatingą reikšmę dėl specifinių duomenų tipų – srauto, lokalizacijos, komunikacijos turinio ir identifikavimo duomenų – tvarkymo. Šie duomenys yra itin jautrūs, nes leidžia atskleisti ne tik asmenų tapatybę, bet ir jų elgesio modelius, ryšius ir judėjimo trajektorijas, todėl jų apsaugai taikomi griežti BDAR ir e. privatumo direktyvos reikalavimai. Antra, asmens duomenų apsauga negali būti atskirta nuo plačiosios teisės į privatų gyvenimą sampratos, kuri apima asmens fizinį ir psichinį

neliečiamumą, šeimos gyvenimą, garbę ir reputaciją bei informacijos apie asmenį apsaugą. Trečia, EŽTT ir ESTT jurisprudencija patvirtina – teisė į privatų gyvenimą, įtvirtinta EŽTK ir Chartijoje, formuoja pagrindą, kuriuo remiantis vertinami asmens duomenų tvarkymo aspektai elektroninių ryšių sektoriuje. Todėl šioje srityje būtina užtikrinti ne tik efektyvų duomenų apsaugos taisyklių taikymą, bet ir pusiausvyrą tarp privatumo apsaugos ir kitų teisėtų interesų, tokių kaip viešasis saugumas ar nusikalstamumo prevencija.

2. Elektroninių ryšių sektorius

Pirmosios darbo dalies analizė parodė, kad asmens duomenų apsauga ir teisė į privataus gyvenimo neliečiamumą yra glaudžiai susijusios, o jų įgyvendinimas grindžiamas tarptautiniais ir ES teisės aktais, taip pat teismų praktika. Vis dėlto siekiant išsamiai suprasti šių principų taikymą praktikoje, būtina detaliau pažvelgti į specifinį sektorių, kuriame šios teisės ir apsaugos mechanizmai įgauna konkretų vaidmenį. Atsižvelgiant į tai, šioje dalyje detaliau nagrinėjama elektroninių ryšių sektoriaus specifika ir jos reikšmė asmens duomenų apsaugai. Pirmiausia bus analizuojama, kaip sparčiai besikeičianti sektoriaus veikla ir technologinė pažanga lemia naujus reguliavimo iššūkius, ypatingai koncentruojantis į e. privatumo direktyvos 15 straipsnio 1 dalies taikymą. Toliau išskiriama elektroninių ryšių paslaugų teikėjų – operatorių – atsakomybė užtikrinant asmens duomenų apsaugą bei jų vaidmuo teisinio reguliavimo kontekste. Galiausiai vertinami specifiniai sektoriaus ypatumai, susiję su valstybių narių institucijų prieiga prie duomenų ir privatumo teisių ribojimo galimybėmis, vadovaujantis ES teisės principais.

2.1. Elektroninių ryšių sektoriaus veiklos specifika

Elektroninių ryšių sektorius yra viena sparčiausiai besivystančių ekonomikos sričių ir itin kompleksiška infrastruktūrinė sistema, daranti reikšmingą įtaką šiuolaikinės visuomenės funkcionavimui. Dėl šios priežasties nuolat kyla poreikis iš naujo įvertinti tiek technologinius sprendimus, tiek taikomus reguliavimo modelius. Be to, elektroninių ryšių sektoriaus reikšmė susideda iš jo integruotumo į skaitmeninę ekonomiką – jis ne tik palaiko tradicines telekomunikacijų paslaugas (telefoniją ir interneto prieigą), bet ir yra esminis modernių duomenų perdavimo, virtualizacijos bei debesijos sprendimų (angl. *cloud computing solutions*) įgyvendinimo variklis. Kitaip tariant, elektroninių ryšių infrastruktūra yra tarsi pagrindas, ant kurio pastatytos visos kitos skaitmeninės paslaugos. Jei ši infrastruktūra nėra tinkamai reguliuojama – t. y. nėra užtikrinamas jos saugumas, patikimumas ir veiklos efektyvumas per aiškias teisinio reguliavimo gaires – tuomet tokios paslaugos kaip internetinės platformos, debesijos sprendimai ar kibernetinio saugumo technologijos lieka labiau konceptualiu sumanymu nei realiai veikiančiu ir patikimu įrankiu. Tai reiškia, kad net ir kuriant inovatyvias technologijas, jos negali veikti efektyviai be tvirtos, reguliaciniais principais pagrįstos

infrastruktūros, kuri leistų joms sklandžiai funkcionuoti tiek techniniu, tiek teisiniu požiūriu (Walden, Steinbrecher and Marinkovic, 2021, p. 1717).

Naujausios Elektroninių ryšių kodekso nuostatos pakeitė ne tik 2002 m. kovo 7 d. priimtą Europos Parlamento ir Tarybos direktyvą 2002/21/EB, kuria buvo nustatyti bendrieji elektroninių ryšių tinklų ir paslaugų reguliavimo principai (vadinamąją Pagrindų direktyvą), bet ir kitas su ja susijusias direktyvas. Tokiu būdu aiškiai išryškinant reguliavimo mechanizmų atnaujinimo būtinybę ir pripažįstant, kad modernios technologijos iš esmės keičia reguliavimo aplinką ir kelia naujus iššūkius. Šis pokytis nėra vien formalus – jis atspindi Europos Sąjungos siekį sistemingai prisitaikyti prie dinamiškai besikeičiančių rinkos poreikių bei užtikrinti aukšto lygio asmens duomenų apsaugą, kas rodo, jog tradiciniai reguliavimo metodai nebeatitinka sparčiai besivystančių technologijų realijų ir yra būtinas griežtas, argumentuotas, adaptyvus sprendimų priėmimo procesas (Walden, Steinbrecher and Marinkovic, 2021, p. 1717).

Elektroninių ryšių infrastruktūra yra kertinis skaitmeninės rinkos elementas, be kurio būtų neįmanoma įgyvendinti ES pagrindinių laisvių – prekių, paslaugų, kapitalo ir asmenų judėjimo, taip pat kurti vieningą skaitmeninę erdvę, skatinančią inovacijas ir konkurencingumą (Elektroninių ryšių kodekso 1, 3 ir 4 straipsniai). Tačiau, analizuojant šį sektorių, pastebima, kad reguliavimo iššūkiai kyla ne tik dėl technologinio progreso, bet ir dėl neatsiejamų duomenų srautų kontrolės bei privatumo klausimų. Reguliavimo sistema, numatyta Elektroninių ryšių kodekse, aiškiai pabrėžia valstybių narių įsipareigojimus – plėtoti ir užtikrinti infrastruktūros saugumą bei kurti skaidrią konkurencinę aplinką (ENISA, 2021). Tai nėra tik *„popierinė"* procedūra, valstybės turi remtis griežtais stebėjimo mechanizmais, nuolat vertinant tiek paslaugų kokybės, tiek technologinio saugumo aspektus. Šiame kontekste ypač svarbu kritiškai vertinti, kaip naujos technologijos, tokios kaip debesijos paslaugos (angl. *internet of things(IoT)*), IP telefonija, tinklų virtualizavimas bei realaus laiko duomenų srautų stebėjimas, iš esmės transformuoja tradicinių telekomunikacijų paslaugų pobūdį. Debesų kompiuterija ir virtualizuota infrastruktūra suteikia paslaugų teikėjams galimybę didinti veiklos efektyvumą, tačiau kartu atsiranda sudėtingų duomenų tvarkymo grandinių, kuriose vartotojų duomenys gali būti tvarkomi tiek pačių paslaugų teikėjų, tiek jų vardu veikiančių trečiųjų šalių, dažnai veikiančių skirtingose jurisdikcijose, taip sukuriant papildomų duomenų apsaugos ir kontrolės iššūkių (Computer Law & Security Review, 2020).

Valstybių narių lygmeniu Elektroninių ryšių kodekso nuostatos perkeliamos į nacionalinius teisės aktus, pavyzdžiui, į Lietuvos Respublikos elektroninių ryšių įstatymą (toliau – **ERĮ**), kuriame detalizuojami sektoriaus reguliavimo mechanizmai. Šioje reguliacinėje

aplinkoje itin svarbi tampa jautrių asmens duomenų – tokių kaip srauto, lokalizacijos ir komunikacijos turinio – apsauga, nes jų netinkamas ar perteklinis tvarkymas gali sukelti tiek privatumo pažeidimų, tiek grėsmių nacionaliniam saugumui. Tokie pavojai ypač aktualūs, kai duomenys tvarkomi tarpvalstybiniu mastu, įtraukiant trečiąsias šalis ar pasitelkiant debesijos infrastruktūrą, veikiančią už ES ribų, nes iškyla rizika, jog taikomi duomenų apsaugos standartai nebus vienodi, o prieiga prie informacijos gali būti suteikta institucijoms, veikiančioms be pakankamų teisinės kontrolės mechanizmų (Krašto apsaugos ministerija, 2024). Todėl tiek nacionaliniu, tiek ES lygmeniu būtina užtikrinti, kad duomenų tvarkymas būtų grindžiamas aiškiais, proporcingais ir būtinais pagrindais. Direktyvos 2002/58/EB 15 straipsnio 1 dalies ribojimai, kaip aiškiai nurodo ESTT, reikalauja, kad bet kokie nustatyti išimčių mechanizmai griežtai atitiktų proporcingumo principą bei būtinumo kriterijų, numatytus Chartijos 7 ir 8 straipsniuose bei BDAR nuostatose (ESTT, Digital Rights Ireland, C-293/12, C-594/12, p. 65).

Iš esmės, elektroninių ryšių sektoriaus specifika yra susijusi su nuolatiniu technologiniu pokyčių ir inovacijų ciklu, kuris verčia reguliavimo institucijas kurti lanksčias, bet tuo pačiu ir griežtas kontrolės sistemas. Nors technologinė pažanga sudaro sąlygas efektyvesniam informacijos perdavimui ir naujų paslaugų modelių kūrimui, ji kartu kelia esminių klausimų – kaip užtikrinti asmens duomenų apsaugą, tinklų vientisumą nepažeidžiant inovacijų skatinimo principų? Atsakymas į šį klausimą yra kompleksinis, reikalaujantis nuolatinės analizės ir adaptacijos, kas parodo, jog tradicinės reguliavimo sistemos nebeatitinka šiuolaikinių technologijų realijų (Europos Audito Rūmai, 2022). Galiausiai, elektroninių ryšių sektorius yra neatskiriama ES skaitmeninės politikos dalis, kurią reikia vertinti ne tik kaip infrastruktūrinį elementą, bet ir kaip dinamišką inovacijų bei rizikų sąveikos erdvę. Nuolatinės technologinės naujovės reikalauja, kad reguliavimo mechanizmai būtų nuolat peržiūrimi ir koreguojami, atsižvelgiant į sparčiai kintančią aplinką bei kylančius privatumo ir duomenų apsaugos iššūkius (Lietuvos Respublikos Ryšių reguliavimo tarnybos ataskaita, 2021).

Toliau bus nagrinėjama, kaip proporcingumo principas ir e. privatumo direktyvoje įtvirtinti ribojimai taikomi praktikoje, ypatingą dėmesį skiriant elektroninių ryšių operatorių atsakomybei duomenų tvarkymo grandinėje. Kadangi jie dažnai veikia kaip duomenų valdytojai ar tvarkytojai, jų sprendimai tiesiogiai lemia, ar taikomi apribojimai atitinka proporcingumo ir būtinybės principus.

2.2. Operatoriai ir jų vaidmuo asmens duomenų apsaugos srityje

Nors elektroninių ryšių operatorių vaidmuo iš pirmo žvilgsnio gali pasirodyti ganėtinai techninis – teikiant paslaugas, užtikrinant ryšių tinklų veikimą bei duomenų perdavimą – iš tikrųjų jų funkcijos yra daugiasluoksnės ir susijusios su kompleksiška asmens duomenų apsaugos problematika. Šie subjektai (kaip apibrėžta Elektroninių ryšių kodekso 2 straipsnio 7 ir 8 punktuose bei ERĮ 3 straipsnyje) teikia ne tik tradicines paslaugas, tokias kaip balso skambučiai, trumpųjų žinučių perdavimas, interneto prieiga bei duomenų perdavimo sprendimai, bet ir modernias technologijas – nuo IP telefonijos ir debesijos sprendimų iki IP pagrįstos televizijos (angl. *internet protocol television, IPTV*) bei daiktų interneto infrastruktūros. Tokia įvairovė kelia papildomų iššūkių asmens duomenų apsaugos kontekste, nes operatoriai tampa techniniais paslaugų teikėjais bei aktyviais duomenų valdytojais.

Pagrindinė problema kyla iš operatorių vaidmens kaip tarpininkų tarp galutinių naudotojų ir informacinių tinklų, t. y. operatoriai, veikdami kaip tarpininkai tarp galutinių naudotojų ir informacinių tinklų, turi tiesioginę prieigą prie įvairių techninių duomenų. Kaip antai, savo veikloje jie nuolat tvarko įvairius duomenis, įskaitant itin jautrią informaciją (pvz., buvimo vietos, komunikacijos turinį bei metaduomenis), kurios apdorojimas tampa neatsiejama asmens privatumo apsaugos dalimi. Esminis klausimas – kaip užtikrinti, kad duomenų tvarkymo apimtis būtų griežtai apribota tik tiek, kiek būtina elektroninių ryšių paslaugų teikimui bei su tuo susijusiam abonento apmokestinimui ir mokėjimų administravimui, kaip tai numatyta e. privatumo direktyvos 6 straipsnyje. T. y. srauto duomenų tvarkymas šiuo pagrindu laikytinas teisėtu tik tuo atveju, jei jis yra būtinas konkrečiam tikslui – pavyzdžiui, abonento sąskaitos išrašymui ar atsiskaitymams už tinklų sujungimo paslaugas. Pažymėtina, kad toks duomenų tvarkymas gali būti vykdomas tik tol, kol nepasibaigęs laikotarpis, per kurį atitinkama sąskaita gali būti teisėtai ginčijama arba pradėtas mokėjimo išieškojimo procesas. Bet koks papildomas duomenų naudojimas turi būti grindžiamas aiškiu naudotojo sutikimu arba griežtai reglamentuojamomis teisės normomis (be to, e. privatumo direktyvos 9 straipsnis riboja net ir vietos nustatymo duomenų tvarkymą be naudotojo sutikimo).

Be techninės veiklos, operatoriams tenka ir su viešuoju interesu susijusi atsakomybė – jų infrastruktūra bei veiklos procesai tampa pagrindiniu kanalu, per kurį valstybės siekia užtikrinti ne tik veiksmingą elektroninių ryšių paslaugų teikimą, bet ir suderinti asmens duomenų apsaugos reikalavimus su nacionalinio saugumo politika. Šiame kontekste kyla norminis konfliktas tarp ES duomenų apsaugos reikalavimų ir nacionalinių saugumo bei teisės

taikymo institucijų interesų: operatoriai privalo laikytis Europos Sąjungos teisėje įtvirtintų duomenų tvarkymo teisėtumo, proporcingumo principų, užtikrinti komunikacijos konfidencialumą, duomenų subjektų informavimą bei sutikimo reikalavimų laikymąsi (pvz., e. privatumo direktyvos 5 ir 6 straipsnių nuostatų), tuo pačiu spręsdami klausimus, susijusius su nacionalinio reguliavimo, leidžiančio taikyti teisės aktų pagrindu pagrįstas prieigos prie duomenų išimtis, protokolais. Operatorių veikla, kuri apima tiek techninius sprendimus, tiek su valstybės institucijų prieigos prie duomenų užtikrinimu susijusius procesus, tampa kritiniu veiksniu siekiant užtikrinti, kad įgyvendinant tokius reikalavimus nebūtų pažeidžiamos asmens teisių apsaugos nuostatos. ESTT jurisprudencija, be kita ko, aiškiai nurodo, kad operatoriai negali būti priversti masiškai kaupti visų naudotojų duomenų be konkretizuoto teisėsaugos institucijų poreikio ir nepriklausomo teisminio sprendimo (ESTT, *La Quadrature du Net*, C-511/18; Prokuratuur, C-746/18; *Privacy International*, C-793/19 ir C-794/19). Tokiu būdu, operacinio lygio sprendimai tampa tiesioginiu reguliavimo ir proporcingumo principų įgyvendinimo veiksniu. Ši teisinė praktika ne tik apibrėžia operatorių kasdienės veiklos ribas, bet ir kelia klausimų dėl duomenų tvarkymo racionalumo bei galimų piktnaudžiavimo scenarijų, kai operatoriai priverstinai susiduria su nacionalinio ir ES reguliavimo konfliktu.

Analizuojant operatorių vaidmenį būtina atsižvelgti į platesnį teisinį ir politinį kontekstą – jie veikia ne tik tarp technologinių sprendimų ir galutinių naudotojų, bet ir tarp duomenų apsaugos principų bei valstybės saugumo interesų (Valstybinė duomenų apsaugos inspekcija, 2023). Todėl duomenų apsaugos sistemos formavimas turi apimti aiškų operatorių atsakomybės ribų apibrėžimą, siekiant užtikrinti pusiausvyrą tarp inovacijų plėtros ir pagrindinių teisių apsaugos. Operatoriai neapsiriboja techninėmis funkcijomis – jų veikla turi tiesioginį poveikį asmens duomenų apsaugos užtikrinimui, nes jie veikia kaip operaciniai duomenų kontrolės taškai, per kuriuos valstybės realizuoja tiek privatumo apsaugos, tiek teisėtos prieigos prie duomenų mechanizmus (EDPS, 2014).

2.3. Specifinės nuostatos asmens duomenų apsaugai elektroninių ryšių sektoriuje

Asmens duomenų apsauga elektroninių ryšių sektoriuje – aktuali tema šiuolaikinėje skaitmeninėje visuomenėje, kurioje komunikacijos technologijos palengvina informacijos mainus, bet ir kelia privatumo iššūkius. Milžiniški duomenų srautai elektroninių ryšių sektoriuje ir technologinė pažanga reikalauja veiksmingų teisinių priemonių tinkamam asmens duomenų tvarkymui ir apsaugai (Europos Komisija, 2023). Elektroninių ryšių sektoriuje taikomos papildomos taisyklės, kurios padeda suderinti asmenų privatumo apsaugą su verslo

interesais ir kompetentingų institucijų teisėtos prieigos prie duomenų poreikiais (Europos duomenų apsaugos valdyba, 2021).

Kaip pažymėta pirmiau, elektroninių ryšių sektoriuje duomenų apsauga grindžiama ne tik bendraisiais BDAR principais, bet ir specifinėmis nuostatomis, taikomomis šiai sričiai pagal e. privatumo direktyvą. Svarbiausias aspektas yra užtikrinti griežtą elektroninių ryšių konfidencialumo apsaugą – tai apima reikalavimus, taikomus tiek ryšių turinio, tiek srauto ir lokalizacijos duomenų rinkimui, saugojimui bei prieigai (ENISA, 2023). Šiame kontekste dažnai tenka derinti asmenų teisę į privatumą su viešuoju interesu, o tokie kompromisai atskleidžia esminius reguliavimo iššūkius (Tarptautinė telekomunikacijų sąjunga, 2024). Atsižvelgiant į šiuos aspektus, tolesnėse šio darbo dalyse analizuojamos specifinės taisyklės bei jų praktinis taikymas, kartu nagrinėjant pagrindinius e. privatumo direktyvos ir BDAR sąveikos aspektus, kurie atsispindi teismų praktikose, ypač susijusiose su valdžios institucijų prieiga prie elektroninių ryšių duomenų.

Visų pirma, **e. privatumo direktyvos 5 straipsnio 1 dalis** įtvirtina elektroninių ryšių slaptumo principą, pagal kurį tiek turinio, tiek metaduomenų (pvz., ryšio trukmės, laiko, IP adreso, siuntėjo ir gavėjo tapatybės) tvarkymas galimas tik gavus naudotojo sutikimą. Bet koks tokių duomenų perėmimas, stebėjimas ar saugojimas be aiškaus teisinio pagrindo laikytinas neteisėtu. Ši nuostata formuoja ne tik technologinio konfidencialumo standartą, bet ir kelia esminį teisinį klausimą dėl pusiausvyros tarp privataus gyvenimo apsaugos ir viešojo intereso užtikrinimo. Griežtai taikant šį principą, tiek viešojo, tiek privataus sektoriaus subjektai – įskaitant valstybės institucijas – negali įgyti prieigos prie asmens duomenų be konkretaus teisinio pagrindo, numatyto teisės aktuose. Išimtys gali būti taikomos tik tuomet, kai jos atitinka būtinumo ir proporcingumo kriterijus, pavyzdžiui, nacionalinio saugumo ar sunkių nusikaltimų prevencijos kontekste. Vis dėlto tokie apribojimai kelia praktinių iššūkių: siekiant užtikrinti konstitucinę asmens teisių apsaugą, gali būti apsunkinamos galimybės institucijoms operatyviai gauti duomenis, būtinus tyrimams. ESTT nuosekliai laikosi pozicijos, kad masinis ir neselektyvus duomenų rinkimas prieštarauja Chartijos 7 ir 8 straipsniams, garantuojantiems teisę į privatų gyvenimą ir asmens duomenų apsaugą (ESTT, *La Quadrature du Net,* C-511/18; *Prokuratuur*, C-746/18; *Privacy International*, C-793/19 ir C-794/19). Tai verčia susimąstyti, ar esama teisinė sistema tinkamai atspindi sparčiai kintančios skaitmeninės erdvės poreikius, ir ar ji sugeba dinamiškai subalansuoti saugumo reikalavimus su asmens teisių apsauga. Tokiu būdu, šis nuostatos taikymo ribojimas skatina nuolatinį teismų ir teisėsaugos institucijų dialogą, siekiant užtikrinti, kad valstybės veiksmai būtų ne tik teisėti, bet ir proporcingi bei būtini. Diskusijos apie šiuos apribojimus rodo, kad teisinės normos turi būti nuolat peržiūrimos

ir adaptuojamos, jog atitiktų tiek technologinius iššūkius, tiek saugumo imperatyvus, nepažeidžiant fundamentalių žmogaus teisių.

Antra, **Direktyvos 2002/58/EB 6 straipsnyje** nustatomos konkrečios sąlygos, kuriomis elektroninių ryšių paslaugų teikėjai gali teisėtai tvarkyti srauto duomenis. Duomenys, apimantys skambučių trukmę, IP adresus, naudojamą tinklą, prisijungimo laiką ir buvimo vietą – apibrėžti kaip būtini paslaugų teikimui, atsiskaitymui su abonentais ar tinklo valdymo funkcijoms vykdyti. Ši nuostata ne tik griežtai riboja duomenų tvarkymo mastą, bet ir pabrėžia būtinumo kriterijaus svarbą: tvarkyti galima tik tiek, kiek iš esmės reikalinga paslaugų funkcionavimui. Duomenys privalo būti saugomi tik ribotą laikotarpį, po kurio jie turi būti ištrinti arba anonimizuoti, kai nebereikia pirminiam tikslui. Toks apribojimas siekia sumažinti galimą asmens duomenų kaupimo riziką, kurios pasekmės gali paveikti privatumo apsaugą (ESTT informacijos suvestinė, 2018). Be to, bet koks tolesnis srauto duomenų tvarkymas, pavyzdžiui, jų panaudojimas rinkodaros ar analitiniais tikslais, yra griežtai ribojamas ir leidžiamas tik gavus aiškų naudotojo sutikimą. Šis reikalavimas ne tik stiprina duomenų tvarkymo skaidrumą ir vartotojo kontrolę, bet ir iškelia platesnį klausimą dėl etinių ribų – kaip technologinės naujovės gali būti suderintos su asmens privatumo apsaugos principais. Tokiu būdu e. privatumo direktyva apima ne vien techninius duomenų tvarkymo aspektus, bet ir įtvirtina proporcingumo, duomenų kiekio mažinimo bei teisėto tikslo principus, kurie tampa ypač svarbūs siekiant išvengti nepagrįsto kišimosi į privatų gyvenimą net ir komerciniais ar analitiniais tikslais.

Trečia, **Direktyvos 2002/58/EB 8 straipsnyje** reglamentuojamos skambinančiojo ir skambučio gavėjo numerio identifikavimo funkcijos, siekiant užtikrinti asmenų teisę į privatumą elektroninių ryšių srityje – naudotojams suteikiama galimybė kontroliuoti savo telefono numerio atskleidimą bei gauti informaciją apie gaunamus skambučius, kartu nustatant apribojimus, skirtus apsaugoti kitų asmenų teises. Pagal šio straipsnio nuostatas, paslaugų teikėjai turi pasiūlyti skambinantiems naudotojams galimybę paprastomis priemonėmis ir nemokamai neleisti nustatyti ryšio linijos, iš kurios skambinama. Tokia pati teisė suteikiama ir abonentams, kuriems skambinama – jie gali pasirinkti neleisti nustatyti ryšio linijos, iš kurios skambinama, atsižvelgiant į pagrįstą funkcijos naudojimą. Be to, jei skambinimo linija nustatoma prieš skambučiui įvykstant, abonentas, kuriam skambinama, turi teisę atsisakyti gaunamo skambučio, jei skambinantysis pasinaudojo funkcija, leidžiančia paslėpti savo numerį. Taip pat nustatyta, kad abonentas, kuriam skambinama, turi galimybę neleisti skambinančiajam nustatyti ryšio linijos, į kurią skambinama. Šie apribojimai užtikrina, kad elektroninių ryšių paslaugų naudotojai turėtų galimybę apsisaugoti nuo nepageidaujamų ar

anonimiškų skambučių bei kontroliuoti savo privatumo lygį. Iš esmės, e. privatumo direktyvos 8 straipsnis sudaro papildomą privatumo apsaugos mechanizmą, suteikiant naudotojams daugiau kontrolės priemonių savo asmeninės informacijos atskleidimui elektroninių ryšių kontekste, taip užtikrinant galimybę laisvai naudotis elektroninėmis ryšio priemonėmis nepatiriant perteklinio kišimosi į privatumą (Valstybinė duomenų apsaugos inspekcija, 2019).

Ketvirta, **e. privatumo direktyvos 9 straipsnis** reguliuoja vietos nustatymo duomenų, nesudarančių srauto duomenų, tvarkymą. Šie duomenys gali būti renkami naudojant įvairias technologijas, pavyzdžiui, GPS, Wi-Fi tinklus ar mobiliojo ryšio bokštus, ir gali būti tvarkomi tik dviem atvejais: jei jie yra anonimizuoti arba jei naudotojas aiškiai sutiko su jų tvarkymu. Sutikimas turi būti duotas laisva valia, aiškiai suprantamas, konkretus ir atšaukiamas bet kuriuo metu. E. privatumo direktyva numato, kad prieš gaudamas sutikimą, paslaugų teikėjas privalo aiškiai informuoti naudotojus apie tai, kokie duomenys bus renkami, kokiais tikslais jie bus naudojami, kiek laiko bus saugomi bei ar jie bus perduoti trečiosioms šalims, teikiančioms paslaugas, grindžiamas papildomu duomenų panaudojimu – vadinamąsias pridėtinės vertės paslaugas (angl. *value-added services*). Be to, naudotojai turi turėti galimybę bet kuriuo metu nemokamai ir paprastomis priemonėmis laikinai sustabdyti savo vietos nustatymo duomenų tvarkymą kiekvieno prisijungimo prie tinklo arba kiekvieno pranešimo perdavimo atveju. Direktyvos 2002/58/EB 9 straipsnis taip pat numato, kad vietos nustatymo duomenis, nesudarančius srauto duomenų, gali tvarkyti tik įgalioti subjektai – viešųjų ryšių tinklų teikėjai, elektroninių ryšių paslaugų teikėjai ar trečiosios šalys, teikiančios pridėtinės vertės paslaugas, ir tik tiek, kiek būtina šioms paslaugoms teikti. Tokiu būdu siekiama užtikrinti, kad naudotojų vietos nustatymo duomenys nebūtų tvarkomi pertekliniu būdu ar be aiškaus teisinio pagrindo (ESTT informacijos suvestinė, 2018).

Šių e. privatumo direktyvos straipsnių taikymas taip pat yra glaudžiai susijęs su BDAR, kuris nustato bendruosius asmens duomenų apsaugos principus visoje ES. Nors BDAR įtvirtina pagrindinį teisinį pagrindą visoms duomenų tvarkymo veikloms, e. privatumo direktyva pateikia taisykles, taikomas specifinėje elektroninių ryšių srityje, kurios kai kuriais atvejais gali numatyti griežtesnius reikalavimus (European Data Protection Board, 2020, p. 9).

Nepaisant šių apsaugos mechanizmų, **e. privatumo direktyvos 15 straipsnio 1 dalis** numato valstybėms narėms galimybę tam tikrais atvejais riboti elektroninių ryšių konfidencialumo principą. Ši išimtis leidžia apriboti privatumo apsaugą nacionalinio saugumo, gynybos, viešosios tvarkos ar nusikalstamumo prevencijos tikslais, tačiau toks ribojimas privalo atitikti teisėtumo ir proporcingumo principus, kaip jie suprantami demokratinėje visuomenėje. ESTT jurisprudencijoje yra išaiškinęs šių nuostatų taikymo ribas. Pavyzdžiui,

byloje *Tele2 Sverige* ir *Watson* konstatuota, kad visiems vartotojams taikomas bendras, neribojamas (nediferencijuotas) duomenų saugojimas, neatsižvelgiant į konkrečius pavojus ar grėsmes, yra nesuderinamas su Chartijos 7 ir 8 straipsniuose įtvirtintomis teisėmis (ESTT, *Tele2 Sverige* ir *Watson*, C-203/15 ir C-698/15, p. 99–101). Kitaip tariant, duomenų negalima saugoti apie visus asmenis *„iš anksto“* ir *„be priežasties“*, tik tam atvejui, jei jų prireiktų ateityje – tokia praktika pažeidžia asmenų teisę į privatų gyvenimą ir asmens duomenų apsaugą. Be kita ko, byloje *Ministerio Fiscal* ESTT nurodė, kad ribotos prieigos prie tam tikrų duomenų, skirtų nustatyti pavogtų mobiliųjų įrenginių naudotojus, galima, tačiau toks ribojimas turi būti proporcingas ir pateisinamas atsižvelgiant į nusikalstamumo prevencijos poreikį (ESTT, *Ministerio Fiscal*, C-207/16, p. 53-57). Byloje nurodyta, kad prieiga prie tokių duomenų nebūtinai turi būti ribojama tik sunkių nusikaltimų tyrimu, jei kitaip užtikrinami Chartijos reikalavimai. Panaši pozicija išsakyta, jau minėtose bylose – *La Quadrature du Net* ir *Privacy International* – kuriose ESTT aiškiai uždraudė valstybes nares įpareigoti paslaugų teikėjus masiškai ir be diferencijavimo saugoti visų naudotojų srauto ir vietos nustatymo duomenis, nebent tai pagrįsta realia ir akivaizdžia grėsme nacionaliniam saugumui (ESTT, *La Quadrature du Net*, C-511/18, p. 134-139; *Privacy International*, C-793/19 ir C-794/19). Dar vienas svarbus aspektas išryškėjo byloje *Prokuratuur*, kurioje nurodyta, jog prokuratūra, kaip proceso šalis, negali būti laikoma nepriklausoma institucija, kuri galėtų priimti sprendimą dėl prieigos prie elektroninių ryšių duomenų. Prieiga prie tokių duomenų turi būti suteikiama tik gavus nepriklausomos teisminės institucijos leidimą (ESTT, *Prokuratuur*, C-746/18, p. 58-61).

Šios ESTT praktikos kontekste svarbu įvertinti nacionalinį reguliavimą Lietuvoje, kurioje elektroninių ryšių sektoriaus duomenų apsaugą reglamentuoja ERĮ, į nacionalinę teisę perkeliantis e. privatumo direktyvos reikalavimus. Kadangi elektroninių ryšių paslaugų teikėjai tvarko asmens duomenis, jų veiklai taikomi ne tik ERĮ, bet ir BDAR nustatyti bendrieji duomenų apsaugos principai, kaip tai numatyta BDAR 2 straipsnio 2 dalies c punkte. Šis teisinis reguliavimas apima tiek duomenų konfidencialumo apsaugą, tiek valstybės institucijų prieigos prie duomenų reglamentavimą. Tam tikrais aspektais Lietuva taiko griežtesnius reikalavimus nei kai kurios kitos ES valstybės narės, nes pagal ERĮ 77 straipsnio 2 dalį, 80 straipsnio 5 dalį ir 96 straipsnio 1 dalį elektroninių ryšių paslaugų teikėjai privalo sistemingai saugoti ir nedelsiant teikti plačiai apibrėžtus duomenis kompetentingoms institucijoms, įskaitant žvalgybos ir ikiteisminio tyrimo subjektus. Toks reguliavimas neatitinka ES teisėje įtvirtintų proporcingumo ir selektyvumo principų bei būtinybės kriterijaus, nes duomenų saugojimas taikomas visiems naudotojams be individualizuotos rizikos analizės ar konkrečios grėsmės pagrindimo, duomenų prieiga vykdoma be išankstinio

nepriklausomos institucijos leidimo, o duomenų teikimo tikslai formuluojami pernelyg plačiai, apimant neapibrėžtas grėsmes valstybės interesams ar ekonominei galiai. Toks modelis prieštarauja ESTT jurisprudencijoje suformuluotai pozicijai, kad masinis ir neselektyvus duomenų rinkimas pažeidžia Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsnius, įtvirtinančius teisę į privatų gyvenimą ir asmens duomenų apsaugą. Lietuva, kaip ir kitos ES valstybės narės, buvo priversta peržiūrėti savo teisinę sistemą po ESTT sprendimų bylose *Tele2 Sverige* ir *Watson*, kuriose teismas aiškiai konstatavo, kad bendra ir nediferencijuota elektroninių ryšių duomenų saugojimo prievolė pažeidžia pagrindines teises į privatų gyvenimą ir asmens duomenų apsaugą (ESTT, *Tele2 Sverige* ir *Watson,* C-203/15 ir C-698/15). Nors šie sprendimai įtvirtino aiškius proporcingumo ir selektyvumo standartus, Lietuvos teisės aktai iki šiol išlaiko sisteminę pareigą paslaugų teikėjams saugoti duomenis, kurie gali būti teikiami institucijoms gana plačiai suformuluotais pagrindais.

Galiausiai, vertinant elektroninių ryšių duomenų saugojimo reguliavimą Europos Sąjungoje, pažymėtina, kad valstybės narės laikosi skirtingų modelių, o šie skirtumai atskleidžia platesnes įgyvendinimo problemas ir harmonizacijos iššūkius, kurie bus detaliau nagrinėjami tolesnėje darbo dalyje. Vokietijos Federalinio Konstitucinio Teismo sprendimas 2010 m. byloje (BVerfG, 1 BvR 256/08), kuriuo buvo panaikinta nacionalinė prievolė saugoti ryšių duomenis dėl konstitucinių teisių pažeidimo, parodė, kad tam tikrose jurisdikcijose nacionalinės konstitucinės normos gali tapti barjeru ES direktyvų įgyvendinimui. Tokia pozicija sustiprino proporcingumo reikalavimų taikymą duomenų apsaugos srityje ir tapo precedentu kitų šalių konstituciniam vertinimui. Prancūzijoje, nepaisant ESTT jurisprudencijos, išliko tendencija išlaikyti bendro pobūdžio duomenų saugojimo reikalavimus (ESTT, *La Quadrature du Net*, C-511/18; ESTT, *Privacy International,* C-623/17). Tačiau ši praktika buvo transformuota papildomais garantijų mechanizmais – pavyzdžiui, sugriežtinta priežiūros sistema ir ribotas duomenų naudojimo mastas (Prancūzijos duomenų apsaugos įstatymas). Tuo tarpu Suomijos ir Estijos pavyzdžiai demonstruoja nuoseklų BDAR ir e. privatumo direktyvos nuostatų taikymą, orientuojantis į griežtesnę teisinę priežiūrą. Šiose šalyse teisėsaugos institucijų prieiga prie saugomų duomenų leidžiama tik esant aiškiai apibrėžtiems, individualizuotiems pagrindams ir nepriklausomos teismų kontrolės sąlygoms (BEREC Report on data retention practices, 2023). Tai atitinka ESTT suformuotą praktiką, pagal kurią tik tikslingas ir selektyvus duomenų rinkimas gali būti laikomas suderinamu su ES pagrindinių teisių apsauga. Apibendrinant, šių nacionalinių modelių skirtumai rodo, jog e. privatumo direktyvos siekis suvienodinti asmens duomenų apsaugos standartus elektroninių ryšių sektoriuje nėra iki galo įgyvendintas. Skirtingi konstituciniai prioritetai, nacionalinių

teismų praktika ir teisėsaugos institucijų prieigos ribojimai lemia, kad kai kuriose šalyse duomenų subjektai gali turėti ženkliai skirtingas apsaugos garantijas, o tai kelia grėsmę bendrai ES vidaus rinkos vientisumui ir teisinio aiškumo principui.

Apibendrinant šios dalies analizę, darytina išvada, kad elektroninių ryšių sektorius išsiskiria duomenų apsaugos reguliavimo intensyvumu dėl nuolat tvarkomų didelio masto asmens duomenų srautų ir sektoriaus technologinių ypatumų. Dėl to čia taikomos ne tik bendrosios BDAR nuostatos, bet ir e. privatumo direktyvoje įtvirtintos taisyklės (ESTT informacijos suverstinė, 2021). Direktyvos 2002/58/EB 5–9 straipsniai numato aiškius reikalavimus dėl ryšių konfidencialumo ir duomenų tvarkymo ribojimų, kurie įpareigoja paslaugų teikėjus užtikrinti griežtą jautrių duomenų apsaugą, tuo tarpu 15 straipsnio 1 dalyje įtvirtinta galimybė valstybėms narėms taikyti teisėkūros pagrįstas išimtis, kurios gali būti pateisinamos tik tuo atveju, jei atitinka proporcingumo principą ir būtinybės kriterijų. Analizė taip pat atskleidė, kad operatoriai šioje srityje neapsiriboja techniniais duomenų valdytojo vaidmenimis – jie tampa tarpininkais tarp duomenų subjektų ir valstybės institucijų, vykdydami ES ir nacionalinės teisės aktuose nustatytus reikalavimus. Galiausiai, ESTT jurisprudencija išlieka esminiu elementu, kuris riboja valstybių narių diskreciją ir užtikrina, kad valstybės nustatomos prieigos prie elektroninių ryšių duomenų priemonės būtų suderintos su pagrindinių teisių apsaugos standartais

3. Direktyvos 2002/58/EB 15 straipsnio įgyvendinimas ir susiję pokyčiai

Skaitmeninės visuomenės plėtra ir technologijų pažanga išryškina asmens duomenų apsaugos svarbą elektroninių ryšių sektoriuje, kur dėl didelių duomenų srautų ir realaus laiko informacijos perdavimo iškyla papildomi privatumo iššūkiai. Atsižvelgiant į šias aplinkybes, Europos Sąjungoje be BDAR taikomi ir papildomi teisės aktai, iš kurių pagrindinis elektroninių ryšių srityje yra e. privatumo direktyva. Šis dokumentas reglamentuoja ne tik elektroninių ryšių slaptumo užtikrinimą, bet ir su komunikacijos duomenų saugumu, nepageidaujama komercine informacija bei kibernetiniu saugumu susijusius klausimus (e. privatumo direktyvos 4, 5, 13 straipsniai). Vienas labiausiai diskutuotinų Direktyvos 2002/58/EB aspektų yra jos 15 straipsnio 1 dalis, suteikianti valstybėms narėms diskreciją priimti teisės aktus, leidžiančius riboti privatumo ir konfidencialumo teises, kai tai būtina viešajam interesui – nacionalinio saugumo, gynybos ar nusikalstamumo prevencijos tikslams. Reaguodama į spartų technologinį vystymąsi ir vis dažniau pasitaikančią praktiką riboti privatumo apsaugą, 2017 m. Europos Komisija pateikė naujo e. privatumo reglamento projektą – Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, COM/2017/010, 2017/0003(COD)) (toliau – **e. privatumo reglamentas**). Vienas pagrindinių e. privatumo reglamento tikslų – suvienodinti elektroninių ryšių reguliavimą, užtikrinti aiškesnį ir vieningesnį privatumo teisių ribojimo sąlygų taikymą visoje ES. Vis dėlto, šis e. privatumo reglamentas iki šiol nepriimtas, o tai kelia praktinių klausimų dėl privatumo apsaugos užtikrinimo nuoseklumo. Šios darbo dalies tikslas – išanalizuoti Direktyvos 2002/58/EB 15 straipsnio 1 dalies taikymo aspektus, ypatingą dėmesį skiriant valstybių narių diskrecijai riboti privatumo ir konfidencialumo teises.

3.1. Direktyvos 2002/58/EB reikšmė ir būtinybė šiuolaikiniame teisiniame kontekste

Prieš analizuojant e. privatumo reglamentą, būtina įvertinti, ar atskiras teisinis reguliavimas, skirtas elektroninių ryšių privatumo apsaugai, vis dar yra aktualus ir ar šią funkciją gali atlikti BDAR bei Direktyva 2002/58/EB. Svarbu suvokti, jog e. privatumo direktyva buvo priimta kaip specialus teisės aktas, papildantis bendrą asmens duomenų apsaugos reguliavimą, nes ES teisės aktų leidėjai jau nuo 1990-ųjų pripažino – elektroninių ryšių konfidencialumas reikalauja atskiro reguliavimo (Council of the European Union, 2021). Nors BDAR, įsigaliojęs 2018 m., siekia užtikrinti visapusišką asmens duomenų apsaugą, pažymėtina, kad jis yra bendras teisės aktas, orientuotas į fizinių asmenų duomenų tvarkymą įvairiose srityse. Tuo tarpu Direktyva

2002/58/EB reglamentuoja platesnį ryšių konfidencialumo spektrą, apimant ne tik fizinių asmenų privatumo apsaugą, bet ir juridinių asmenų susižinojimą, slapukų naudojimą, tinklo saugumą, tiesioginę rinkodarą bei kitas su elektroniniais ryšiais susijusias sritis (EDAV, 2019). Esminis skirtumas tarp BDAR ir e. privatumo direktyvos išryškėja nagrinėjant 15 straipsnio 1 dalį, kuri numato galimybę valstybėms narėms riboti ryšių privatumo apsaugą tam tikrais pagrindais. Ši nuostata leidžia nustatyti išimtis iš privatumo apsaugos principų nacionalinio saugumo, teisėsaugos ir kitais viešojo intereso tikslais (EDAV, 2019). Dėl tokios išimties valstybės narės gali įpareigoti elektroninių ryšių paslaugų teikėjus saugoti metaduomenis, stebėti ryšius ir netgi riboti ryšių konfidencialumą remiantis teisėsaugos ar nacionalinio saugumo argumentais.

BDAR nereglamentuoja valstybių įgaliojimų riboti privatumo teises elektroninių ryšių sektoriuje, nes jo tikslas yra reguliuoti asmens duomenų tvarkymą privačiame ir viešajame sektoriuose. Tuo tarpu **Direktyvos 2002/58/EB 15 straipsnio 1 dalis** suteikia valstybėms narėms galimybę nustatyti tam tikrus privatumo apribojimus, kaip antai, įpareigoti elektroninių ryšių paslaugų teikėjus saugoti metaduomenis tam tikrą laikotarpį. Tokia nuostata parodo, kad BDAR negali visiškai pakeisti e. privatumo direktyvos, kuri apima ne tik duomenų tvarkymą, bet ir specifinius elektroninių ryšių konfidencialumo ribojimo pagrindus (EDAV, 2019). Būtent šiuo aspektu aktuali tampa ESTT praktika, kurioje pažymima, kad valstybės narės, taikydamos Direktyvos 2002/58/EB 15 straipsnio 1 dalyje numatytas išimtis, privalo užtikrinti, jog bet koks privatumo ribojimas atitiktų ES teisėje įtvirtintus pagrindinių teisių apsaugos principus. Pavyzdžiui, ESTT pateikė aiškią poziciją – nacionalinės taisyklės, numatančios plačios apimties ir be diferencijavimo elektroninių ryšių duomenų saugojimą, neatitinka Europos Sąjungos teisės reikalavimų, nes pažeidžia Chartijos nuostatas (ESTT, *Tele2 Sverige* ir *Watson*, C-203/15 ir C-698/15, p. 117–118 punktai). Kitoje aktualioje byloje ES Teisingumo Teismas išaiškino, kad nacionalinio saugumo sumetimais riboti elektroninių ryšių konfidencialumą galima tik esant aiškiai apibrėžtiems teisiniams kriterijams ir laikantis proporcingumo principo (ESTT, *La Quadrature du Net* C-511/18, p. 120 ir 126). Šie sprendimai rodo, kad teisės į privatumą ribojimo išimtys turi būti taikomos griežtai ir negali būti interpretuojamos per plačiai, todėl būtina aiškiai apibrėžti jų taikymo ribas ir sąlygas.

Atsižvelgiant į tai, kad BDAR nėra orientuotas į elektroninių ryšių konfidencialumo apsaugą, o e. privatumo direktyvoje nustatytos specialios privatumo ribojimo taisyklės, galima teigti, jog atskiro e. privatumo reglamentavimo poreikis vis dar išlieka aktualus. BDAR užtikrina asmens duomenų apsaugą, tačiau nepakankamai reguliuoja nacionalinių institucijų galimybes riboti privatumo teises. Todėl Europos Komisija 2017 m. pasiūlė e. privatumo

reglamentą, siekdama užtikrinti aiškesnį teisinį reguliavimą ir suvienodinti privatumo apsaugą elektroninių ryšių srityje visose valstybėse narėse (Europos Komisijos pasiūlymas, COM/2017/010, 2017/0003(COD)). Viena iš pagrindinių naujovių – aiškesnės taisyklės dėl elektroninių ryšių konfidencialumo ribojimo, įskaitant privatumo išimtis pagal Direktyvos 2002/58/EB 15 straipsnio 1 dalį. Taigi, kadangi valstybių narių praktika skiriasi, o BDAR nesuteikia pakankamai aiškumo dėl teisėsaugos ir nacionalinio saugumo išimčių, e. privatumo direktyvos funkcijos išlieka būtinos, o būsimas e. privatumo reglamentas turėtų jas dar labiau konkretizuoti ir suvienodinti reguliavimą ES mastu.

3.2. E. privatumo reglamento naujovės ir jo įtaka e. privatumo direktyvos 15 straipsnio 1 dalies taikymui

Atsižvelgiant į ankstesnėje darbo dalyje nustatytą būtinybę turėti specialų elektroninių ryšių privatumo apsaugos reguliavimą, šioje dalyje analizuojamos e. privatumo reglamento naujovės ir jų galimas poveikis Direktyvos 2002/58/EB 15 straipsnio 1 dalies taikymui. Pagrindinis tikslas – nustatyti, ar e. privatumo reglamento nuostatose yra pašalinami esami teisinio reguliavimo trūkumai, ypač tie, kurie susiję su valstybių narių diskrecija riboti ryšių konfidencialumą.

E. privatumo reglamento analizę tikslinga pradėti nuo teritorinio taikymo srities – e. privatumo reglamentas būtų taikomas visiems elektroninių ryšių duomenims, kurie yra tvarkomi paslaugų teikėjų, nepriklausomai nuo jų įsisteigimo vietos, jeigu paslaugos yra teikiamos galutiniams vartotojams, esantiems ES teritorijoje (Europos Komisijos pasiūlymas, COM/2017/010, 2017/0003(COD), 3 straipsnis, preambulės 15 p.). E. privatumo reglamentas įpareigoja paslaugų teikėjus, neturinčius atstovybės ES, paskirti įgaliotą atstovą valstybėje narėje, kurioje yra galutinis vartotojas. Tokiu būdu reglamento taikymas, kaip ir BDAR atveju, peržengia ES ribas, siekiant užtikrinti aukštesnį privatumo apsaugos lygį.

Pagal savo taikymo sritį e. privatumo reglamentas numato išplėstinę elektroninių ryšių paslaugų sąvoką, kuri apima ne tik tradicines telekomunikacijų paslaugas (pvz., telefono skambučius ar SMS), bet ir skaitmenines platformas, *OTT* (angl. *over-the-top (OTT)*) paslaugas, tiesioginės žinutės paslaugas bei kitus interneto pagrindu veikiančius sprendimus (žr. Elektroninių ryšių kodekso 2 straipsnio 4 d. ir Reglamento (ES) 2015/2120 dėl atviros interneto prieigos ir tarptinklinio ryšio 2 straipsnio 2 d.). Taip siekiama išvengti situacijos, kai inovatyvūs paslaugų teikėjai patenka už reguliavimo ribų, bei užtikrinti vienodas sąlygas rinkoje.

Taip pat ypatingai svarbus aspektas – e. privatumo direktyvos 15 straipsnio 1 dalies išimtis, leidžianti valstybėms narėms nustatyti privatumo ribojimus nacionalinio saugumo ar teisėsaugos tikslais. Nors e. privatumo reglamente išlaikoma galimybė taikyti išimtis, kaip ir e. privatumo direktyvoje, Europos Komisijos pasiūlymo (COM/2017/010, 2017/0003(COD), 11 straipsnis) nuostatose numatyti papildomi saugikliai, kurie riboja tokių išimčių taikymo apimtį ir nustato griežtesnius teisėtumo bei proporcingumo reikalavimus. Siekiant aiškumo, e. privatumo reglamentas detaliau apibrėžia, kokiomis sąlygomis valstybės narės gali remtis išimtimi. Atsižvelgiant į tai, kad tiek e. privatumo direktyvoje, tiek e. privatumo reglamente numatytos galimybės taikyti išimtis, tačiau jų taikymui keliami vis griežtesni reikalavimai, grindžiami ES teisės principais ir ESTT jurisprudencija, šiame darbe toliau apibrėžiami pagrindiniai kriterijai, kurie, autorės vertinimu, turi būti laikomi būtinais siekiant užtikrinti proporcingą ir teisėtą asmens duomenų tvarkymą elektroninių ryšių srityje:

a) **Proporcingumo ir teisėtumo principai** – nacionalinės priemonės turi būti pagrįstos aiškiais ir konkrečiais teisiniais kriterijais, o bet kokie duomenų saugojimo ar prieigos ribojimai turi būti taikomi griežtai ribotais atvejais, remiantis įrodymais apie realią grėsmę nacionaliniam saugumui ar rimtus viešojo intereso tikslus (ESTT, *Tele2 Sverige* ir *Watson,* C-203/15, C-698/15).
b) **Išimties taikymo konkretumas** – e. privatumo reglamente numatyta, kad valstybės narės turi tiksliai apibrėžti, kokiose situacijose ir kokiems duomenims gali būti taikomi ribojimai, užtikrinant, kad jie būtų būtini ir proporcingi. Toks reikalavimas taip pat apima poreikį tiksliai apibrėžti sąvokas, tokias kaip *„nacionalinio saugumo“* ir *„nusikalstamumo prevencijos“*, siekiant išvengti perteklinių ar neproporcingų ribojimų (Europos Komisijos pasiūlymas, COM/2017/010, 11 straipsnis).
c) **Suderinamumas su ES teismų praktika** – e. privatumo reglamente nurodoma, kad visos nacionalinės nuostatos turi atitikti Chartijos 7 ir 8 straipsnius bei ESTT jurisprudencijoje įtvirtintas ribas. ESTT pabrėžė, kad prieiga prie ryšių duomenų teisėsaugai turi būti leidžiama tik gavus nepriklausomo teismo leidimą (ESTT, *Prokuratuur,* C-746/18).

Remiantis ankstesnėmis įžvalgomis, e. privatumo reglamente siūlomos naujovės turėtų išspręsti praktines problemas, susijusias su e. privatumo direktyvos 15 straipsnio 1 dalies taikymu. Vienas svarbiausių pokyčių – aiškesnis ir griežčiau apibrėžtas nacionalinių valdžios institucijų įgaliojimų ribojimas, užtikrinant, kad duomenų saugojimo išimtys būtų taikomos tik esant objektyviai pagrįstoms ir griežtai proporcingoms sąlygoms, atsižvelgiant į ESTT praktiką. Taip pat e. privatumo reglamente išplečiama tiek teritorinė, tiek materialinė taikymo

sritis, suteikiant vienodą apsaugą ne tik ES rezidentams, bet ir užsienio subjektams, jei jų veikla susijusi su ES rinka. Šis pokytis yra esminis siekiant suvienodinti taisykles, kurios iki šiol buvo interpretuojamos nevienodai skirtingose valstybėse narėse. Be kita ko, e. privatumo reglamento nuostatos griežčiau apibrėžia sutikimo dėl duomenų tvarkymo reikalavimus, užtikrinant, kad naudotojai išreikštų aiškų, aktyvų sutikimą, o ne būtų pasyviai priversti jį duoti per numatytuosius nustatymus ar blanketinės formos pranešimus. Tokiu būdu siekiama pašalinti dabartinės e. privatumo direktyvos trūkumus, kai privatumo apsauga dažnai buvo užtikrinama tik formaliai, o ne realiai garantuojant naudotojų kontrolę savo duomenų atžvilgiu (ESTT, *Commission prieš Bavarian Lager*, C-28/08 P, p. 77). Tokiu būdu e. privatumo reglamentas, išplėtęs privatumo ir konfidencialumo apsaugos nuostatas, turėtų padėti ne tik pagerinti asmenų teisių apsaugą, bet ir suvienodinti teisės įgyvendinimą visoje ES, kas yra esminė Bendrosios skaitmeninės rinkos strategijos dalis (Europos Komisija, 2017, COM(2017) 10 final).

Apibendrinus tai, kas išdėstyta apie e. privatumo direktyvos svarbą ir e. privatumo reglamento poveikį, matyti, kad teisinis reguliavimas elektroninių ryšių sektoriuje yra esminis elementas užtikrinant asmenų privatumo apsaugą šiuolaikinėje informacinėje visuomenėje. BDAR, nors ir svarbus asmens duomenų apsaugos dokumentas, yra orientuotas tik į fizinius asmenis ir neapima visų specifinių elektroninių ryšių sektoriaus aspektų, todėl e. privatumo direktyvos ir e. privatumo reglamento reikšmė bei būtinybė išlieka aktualios. E. privatumo reglamentas, plėsdamas Direktyvos 2002/58/EB taikymo sritį ir įtraukdamas naujas technologijas bei jų teikėjus, siekia užtikrinti, kad privatumo apsaugos principai būtų taikomi vienodai visose valstybėse narėse. Tai ypač svarbu atsižvelgiant į globalizaciją ir technologinius pokyčius, kurie leidžia paslaugų teikėjams veikti tarptautiniu mastu, tačiau e. privatumo reglamentas susilaukia kritikos dėl galimų privatumo apsaugos spragų, ypač susijusių su nepakankamai aiškiai apibrėžtais sutikimo formavimo principais ir galimu vartotojų sekimu be jų aiškaus sutikimo. Ši darbo dalis iš dalies atskleidžia, kad nors yra žengiami žingsniai siekiant išplėsti ir patobulinti teisinį reguliavimą, vis dar būtina tobulinti teisės aktus, užtikrinant, kad jos atitiktų aukščiausius privatumo apsaugos standartus, laikytųsi proporcingumo, aiškumo ir teisėsaugos principų.

3.3. E. privatumo direktyvos ir BDAR sąveika

Nors tam tikrais atvejais Direktyva 2002/58/EB ir BDAR apima tas pačias sritis, tai nereiškia, kad šios nuostatos visada susikerta. Tai galima suprasti iš to, kad e. privatumo direktyvos 1 straipsnio 2 dalyje aiškiai nurodoma, jog ji yra skirta patikslinti ir papildyti ankstesnę

Direktyvą 95/46/EB, kuri reglamentavo asmens duomenų apsaugą ir jų laisvą judėjimą. Norint tiksliai suprasti, kaip Direktyva 2002/58/EB ir BDAR tarpusavyje veikia, pirmiausia reikia paaiškinti e. privatumo direktyvos 1 straipsnio 2 dalies reikšmę, o tada pereiti prie BDAR 95 straipsnio.

Pagal teisės principą *lex specialis derogat legi generali*, specialiosios teisės normos turi viršenybę prieš bendrąsias, jei jos reglamentuoja tą patį klausimą išsamiau (žr. pagal analogiją ESTT, T-60/06 RENV II ir T-62/06 RENV II, p. 81). Atsižvelgiant į tai, kai kurios Direktyvos 2002/58/EB nuostatos detalizuoja ir paaiškina BDAR reikalavimus asmens duomenų tvarkymo elektroninių ryšių srityje kontekste, todėl šios nuostatos taikomos prioritetine tvarka. Taigi kai e. privatumo direktyva detaliau paaiškina BDAR reikalavimus, šios nuostatos turi pranašumą prieš BDAR. Vis dėlto, jeigu Direktyva 2002/58/EB neapima tam tikrų duomenų tvarkymo aspektų, tada taikomos BDAR nuostatos. Vienas iš pavyzdžių, kai Direktyva 2002/58/EB detaliau paaiškina BDAR nuostatas, yra Direktyvos 2002/58/EB 6 straipsnis, susijęs srauto duomenimis. Asmens duomenų tvarkymas gali būti teisėtas pagal kelis BDAR 6 straipsnyje numatytus pagrindus. Tačiau elektroninių ryšių paslaugų teikėjas negali taikyti visų BDAR 6 straipsnyje nurodytų teisėtų pagrindų, kai kalbama apie srauto duomenis, nes e. privatumo direktyvos 6 straipsnyje yra aiškiai nurodytos sąlygos, kada srauto duomenys gali būti tvarkomi, įskaitant asmens duomenis, todėl e. privatumo direktyvos nuostatos turi pranašumą prieš bendresnes BDAR nuostatas. Tačiau kitos BDAR nuostatos, pavyzdžiui, susijusios su duomenų subjekto teisėmis, taip pat taikomos be apribojimų. Be kita ko, Direktyvos 2002/58/EB 6 straipsnyje nėra paneigiamas reikalavimas, kad asmens duomenų tvarkymas turi būti teisėtas ir sąžiningas (BDAR 5 straipsnio 1 dalies a punktas). Panaši situacija yra ir su e. privatumo direktyvos 5 straipsnio 3 dalimi, kai kalbama apie informaciją, saugomą galutiniuose naudotojo įrenginiuose. Pagal šią nuostatą, išankstinis naudotojo sutikimas paprastai yra reikalingas, kad būtų galima saugoti arba pasiekti informaciją, jau saugomą įrenginyje. Jeigu ši informacija yra asmens duomenys, e. privatumo direktyvos 5 straipsnio 3 dalis turi pirmenybę prieš BDAR 6 straipsnį, kai kalbama apie šios informacijos saugojimą ar prieigą prie jos. Direktyva 2002/58/EB taip pat papildo BDAR nuostatas, susijusias su asmens duomenų tvarkymu elektroninių ryšių sektoriuje. Pavyzdžiui, Direktyva 2002/58/EB siekiama apsaugoti tiek fizinių asmenų, tiek juridinių asmenų teises ir interesus – taip ne tik stiprinama fizinių asmenų teisę į privatumą, bet ir pripažįstama juridinių asmenų teisę į duomenų apsaugą, papildant BDAR (e. privatumo direktyvos 12 konstatuojamoji dalis).

BDAR 95 straipsnyje nurodyta, kad BDAR *„nepriklauso nustatyti papildomų reikalavimų fiziniams ar juridiniams asmenims, kurie tvarko duomenis, susijusius su viešaisiais elektroninių ryšių tinklais, jeigu tai jau reglamentuojama Direktyvoje 2002/58/EB ir siekiama tų pačių tikslų“*. Iš esmės tai reiškia, kad BDAR 95 straipsnio tikslas yra užkirsti kelią papildomai administracinei naštai, nes kitaip duomenų valdytojams gali tekti laikytis dviejų beveik identiškų reikalavimų. Pavyzdžiui, tiek e. privatumo direktyva (4 straipsnis), tiek BDAR (32–34 straipsniai) numato, kad duomenų saugumo pažeidimas turi būti pranešamas kompetentingoms institucijoms. Tokie pranešimai turi būti pateikiami pagal abu teisės aktus, priklausomai nuo to, kurios nuostatos yra taikomos, tačiau tai gali sukelti papildomą naštą, nes pranešimai turi būti teikiami pagal tiek BDAR, tiek nacionalines e. privatumo teisės nuostatas, tačiau šis dvigubas pranešimas ne visuomet duoda aiškios naudos. Pagal BDAR 95 straipsnį, jei elektroninių ryšių paslaugų teikėjas pranešė apie pažeidimą pagal nacionalinius teisės aktus, jis nebeturi privalomai pranešti duomenų apsaugos institucijai pagal BDAR 33 straipsnį. Kaip jau buvo minėta anksčiau, kai yra specialiosios nuostatos, kurios reguliuoja konkrečius duomenų tvarkymo veiksmus, turi būti taikomos šios specialiosios nuostatos (*lex specialis*), o jeigu tokių nuostatų nėra, taikoma bendroji norma (*lex generalis*). Tai patvirtinama BDAR 173 konstatuojamojoje dalyje, t. y. preambulės 15 p., kuriame teigiama, kad, jeigu e. privatumo direktyva netaiko specialių įpareigojimų, galioja BDAR. Taip pat BDAR 173 konstatuojamojoje dalyje pakartojama e. privatumo direktyvos 10 konstatuojamoji dalis, kurioje numatyta, kad *„elektroninių ryšių sektoriuje Reglamentas (ES) 2016/679 taikomas visiems klausimams, susijusiems su pagrindinių teisių ir laisvių apsauga, išskyrus tuos, kurie jau reglamentuojami šios direktyvos nuostatomis“*. Pavyzdžiui, elektroninių ryšių paslaugų teikėjas, kuris teikia paslaugas per viešus ryšių tinklus, turi laikytis nacionalinių teisės aktų, įgyvendinančių e. privatumo direktyvos 6 straipsnio 2 dalį, kuri reglamentuoja srauto duomenų tvarkymą, kai šie duomenys būtini abonentų sąskaitoms pateikti ir sumokėti už tinklų sujungimus. Kadangi nėra specialiųjų e. privatumo direktyvos nuostatų, pavyzdžiui, dėl teisės susipažinti, taikomos BDAR nuostatos. Galiausiai, Direktyvos 2002/58/EB 32 konstatuojamojoje dalyje numatyta, kad jeigu elektroninių ryšių paslaugų teikėjai naudoja subrangovus asmens duomenims tvarkyti, sutarčių su subrangovais sudarymas ir duomenų tvarkymas turi visiškai atitikti BDAR reikalavimus, kuriuos privalo laikytis tiek duomenų valdytojai, tiek tvarkytojai. Taip pat svarbu įvertinti, kaip praktikoje užtikrinamas šių dviejų teisės aktų tarpusavio suderinamumas, ypač kalbant apie kompetencijų paskirstymą tarp nacionalinių institucijų. Kai valstybės narės priima teisės aktus skirtus įgyvendinti Direktyvą 2002/58/EB, jos turi atsižvelgti ir į BDAR reikalavimus, ypač kai tai susiję su teisių gynimo

priemonėmis, atsakomybe ar sankcijomis (Direktyvos 2002/58/EB 15 straipsnio 2 dalis ir BDAR 94 straipsnis). Kadangi e. privatumo direktyva nesuteikia tiesioginių įgaliojimų konkrečiai institucijai, šią funkciją gali vykdyti skirtingos institucijos, priklausomai nuo nacionalinės teisinės sistemos – tai gali būti tiek duomenų apsaugos priežiūros institucijos, tiek telekomunikacijų ar vartotojų apsaugos reguliuotojai. Toks situacijos lankstumas leidžia valstybėms narėms pritaikyti reguliavimą pagal nacionalinius poreikius, tačiau kartu sukelia ir rizikų dėl nevienodo Direktyvos 2002/58/EB įgyvendinimo visoje ES.

3.4. Elektroninių ryšių kodekso poveikis elektroninių ryšių sektoriui ir privatumo apsaugai

Atsižvelgiant į darbo temą, kurioje analizuojama valstybių narių įgaliojimų apimtis užtikrinant asmens duomenų tvarkymą ir privataus gyvenimo apsaugą elektroninių ryšių sektoriuje, tikslinga detaliau išnagrinėti Elektroninių ryšių kodekso reikšmę šioje srityje. Kodeksas – vienas iš pagrindinių ES teisės aktų, kuriuo siekiama suvienodinti elektroninių ryšių sektoriaus reguliavimą visoje Europos Sąjungoje, skatinti inovacijas ir konkurenciją bei užtikrinti aukštą galutinių vartotojų teisių apsaugos lygį (Kodekso 1 straipsnis). Kodekso 1 straipsnio 3 dalies b) ir c) punktuose papildomai nurodoma, kad vienas iš jo tikslų yra prisidėti prie aukšto galutinio naudotojų duomenų apsaugos lygio užtikrinimo ir stiprinti vartotojų teises, įskaitant teisę į privatumą. Elektroninių ryšių kodeksas glaudžiai sąveikauja su e. privatumo direktyva ir BDAR – kartu šie teisės aktai sudaro teisinį pagrindą, reguliuojantį asmens duomenų tvarkymą elektroninių ryšių sektoriuje. Kodekse nustatytos nuostatos gali tiesiogiai veikti, kaip valstybės narės taiko e. privatumo direktyvos 15 straipsnio 1 dalies išimtis, susijusias su privatumo ir konfidencialumo ribojimu viešojo intereso pagrindu. Todėl šioje darbo dalyje bus nagrinėjama, kaip Kodeksas įtvirtina bendrą reguliacinę aplinką, kurioje valstybės narės turi derinti elektroninių ryšių paslaugų teikėjų pareigas užtikrinant asmens duomenų apsaugą bei galimus iš šios srities kylančius privatumo ribojimus.

Kodeksas pirmiausia orientuotas į elektroninių ryšių paslaugų reguliavimą, užtikrinant bendrąją rinką ir skatinant aukšto lygio ryšio infrastruktūros plėtrą, tačiau kodeksas taip pat įtraukia svarbias nuostatas, susijusias su vartotojų apsauga, įskaitant privatumo aspektus. Taigi, kalbant apie poveikį elektroninių ryšių sektoriui – Kodeksas įveda platesnį elektroninių ryšių paslaugų apibrėžimą, kuris apima ne tik tradicinius telekomunikacijų operatorius, bet ir naujus rinkos dalyvius, tokius kaip *„over-the-top”* paslaugų teikėjai (pvz., *„WhatsApp“*, *„Skype“*).

Tai reiškia, kad didelė dalis duomenų tvarkymo procesų, kurie anksčiau buvo reguliuojami tik BDAR, dabar patenka ir į Elektroninių ryšių kodekso reguliavimo sritį.

Magistro darbo autorės vertinimu, šis reguliavimo pokytis yra reikšmingas dėl kelių priežasčių. Pirma, tai užtikrina vienodesnį reguliavimą visiems elektroninių ryšių paslaugų teikėjams, nepriklausomai nuo technologinės platformos, per kurią jie veikia. Tradiciniai telekomunikacijų operatoriai ilgą laiką buvo griežtai reguliuojami, o tokios paslaugos kaip *„WhatsApp“* ar *„Skype“* iki šiol veikė santykinai mažiau reglamentuotoje aplinkoje. Dabar Elektroninių ryšių kodeksas įpareigoja šiuos paslaugų teikėjus laikytis panašių duomenų apsaugos ir privatumo standartų, kaip ir tradicinius operatorius. Antra, šie pokyčiai turi įtakos duomenų tvarkymo skaidrumui ir teisiniam aiškumui, kadangi *OTT* paslaugų teikėjai tvarko didžiulius asmens duomenų kiekius (pvz., susirašinėjimo istorijas, skambučių duomenis, buvimo vietos informaciją), jų įtraukimas į Elektroninių ryšių kodekso reguliavimo lauką užtikrina, kad vartotojų duomenys bus tvarkomi pagal aiškesnes ir vieningesnes taisykles. Trečia, tai daro įtaką teisėsaugos institucijų prieigai prie duomenų. Kadangi *OTT* paslaugos dabar oficialiai laikomos elektroninių ryšių paslaugomis, joms gali būti taikomi tie patys duomenų išsaugojimo ir prieigos reikalavimai, kurie taikomi tradiciniams operatoriams. Tai kelia svarbius privatumo apsaugos klausimus, ypač susijusius su valstybinių institucijų galimybėmis gauti prieigą prie šių paslaugų naudotojų duomenų (Elektroninių ryšių kodeksas, 2, 6, 112, 113, 123 straipsniai).

Aktualu ir tai, kad vienas iš svarbiausių aspektų, susijusių su Elektroninių ryšių kodekso įtaka elektroninių ryšių sektoriui, yra jo sąveika su galiojančiomis duomenų apsaugos normomis, ypač e. privatumo direktyva. Kadangi e. privatumo direktyva reglamentuoja elektroninių ryšių paslaugų teikėjų pareigas užtikrinti asmens duomenų ir ryšių konfidencialumą, būtina įvertinti, kaip Kodeksas papildo ar įtakoja šias nuostatas. Nors pats Kodeksas nedetalizuoja privatumo apsaugos taisyklių taip išsamiai kaip Direktyva 2002/58/EB, jis tiesiogiai veikia elektroninių ryšių sektoriuje vykdomą asmens duomenų tvarkymą. Svarbu pažymėti, kad Elektroninių ryšių kodekso 1 straipsnio 3 dalies b) ir c) punktuose aiškiai nurodoma, jog Kodeksas nepažeidžia nei ES, nei nacionalinių teisės aktų, reglamentuojančių asmens duomenų ir privatumo apsaugą ar viešąją tvarką bei nacionalinį saugumą. Kitaip tariant, privatumo apsaugos klausimai paliekami reguliuoti specialiesiems teisės aktams, tokiems kaip BDAR ir Direktyva 2002/58/EB. Šiuo požiūriu Kodeksas veikia kaip bendroji telekomunikacijų sektoriaus reguliavimo sistema, tačiau neeliminuoja specialiųjų duomenų apsaugos standartų. BDAR, kaip visose ES valstybėse narėse tiesiogiai taikomas teisės aktas, nustato bendruosius duomenų tvarkymo principus ir duomenų subjektų teises, o

Direktyva 2002/58/EB užtikrina specifinius konfidencialumo reikalavimus elektroninių ryšių srityje, kurie taikomi tiek tradiciniams operatoriams, tiek naujos kartos skaitmeninėms paslaugoms.

Direktyvos 2002/58/EB 15 straipsnio 1 dalis suteikia valstybėms narėms teisę nustatyti išimtis, leidžiančias riboti privatumo ir konfidencialumo teises esant būtinybei, susijusiai su nacionaliniu saugumu, viešąja tvarka ar kitais svarbiais interesais, tačiau kaip ir buvo paminėta anksčiau tokie ribojimai turi būti pagrįsti proporcingumo principu ir atitikti Chartijoje įtvirtintas nuostatas. Kodeksas, įtraukdamas nuostatas, susijusias su nacionalinių reguliavimo institucijų (toliau – **NRI**) vaidmeniu elektroninių ryšių sektoriuje, taip pat gali turėti poveikį e. privatumo direktyvos 15 straipsnio taikymui. Autorės nuomone, pagrindiniai aspektai, į kuriuos būtina atsižvelgti, yra šie:

a) **Kodeksas suteikia NRI platesnius įgaliojimus** ne tik ryšių paslaugų reguliavime, bet ir konfidencialumo bei duomenų apsaugos užtikrinime, kas gali turėti įtakos e. privatumo direktyvos 15 straipsnio taikymui, ypač jei NRI aktyviai vykdo priežiūrą ir užtikrina, kad operatoriai laikytųsi privatumo ir duomenų apsaugos reikalavimų.
b) Kadangi **Kodeksas reglamentuoja elektroninių ryšių sektorių**, o BDAR nustato bendrąsias duomenų apsaugos taisykles, kyla klausimas, kaip pasiskirsto kompetencija tarp NRI ir duomenų apsaugos institucijų. Skirtingas šių institucijų vaidmens aiškinimas gali lemti nevienodą e. privatumo direktyvos 15 straipsnio taikymą skirtingose valstybėse narėse, taip didinant reguliavimo fragmentaciją ES lygmeniu.
c) **Kodeksu siekiama harmonizuoti elektroninių ryšių reguliavimą** ES, tačiau valstybės narės gali turėti skirtingas taisykles dėl teisėsaugos prieigos prie duomenų, o tai gali sukelti situacijas, kai Elektroninių ryšių kodekse įtvirtintos nuostatos prieštarauja nacionaliniams teisės aktams, reglamentuojantiems prieigos prie elektroninių ryšių duomenų sąlygas.
d) **Kodeksas taip pat nustato specifines pareigas elektroninių ryšių paslaugų teikėjams**, susijusias su tinklo ir paslaugų saugumu, duomenų apsauga bei incidentų valdymu. Kodekso 40 straipsnyje įtvirtinta, kad paslaugų teikėjai privalo taikyti atitinkamas technines ir organizacines priemones užtikrinti tinklų bei paslaugų saugumą, įskaitant reikalavimą pranešti apie saugumo incidentus, kaip tai nustatyta 40 ir 41 straipsniuose. Šie reikalavimai gali būti vertinami kaip papildomi įpareigojimai, egzistuojantys šalia e. privatumo direktyvos nuostatų.
e) Kadangi **Kodeksas leidžia valstybėms narėms lanksčiai organizuoti reguliavimo institucijų sistemą** (Kodekso 5 straipsnio 4 dalis), tai lemia nevienodą Direktyvos 2002/58/EB 15 straipsnio 1 dalies taikymą ES mastu. Valstybės narės gali nustatyti

skirtingas taisykles dėl teisėsaugos institucijų prieigos prie elektroninių ryšių duomenų, skirtingai reglamentuoti duomenų saugojimo terminus ar bendradarbiavimo su teisėsaugos institucijomis apimtį.

Taigi, Elektroninių ryšių kodeksas suteikia nacionalinėms reguliavimo institucijoms papildomus įgaliojimus ne tik ryšių sektoriaus reguliavimui, bet ir duomenų apsaugai bei konfidencialumo užtikrinimui, o tai gali tiesiogiai paveikti e. privatumo direktyvos 15 straipsnio taikymą. Kadangi BDAR ir Elektroninių ryšių kodeksas reguliuoja skirtingus, bet persidengiančius aspektus, jų sąveika priklauso nuo to, kaip valstybės narės paskirsto atsakomybę tarp duomenų apsaugos priežiūros institucijų ir telekomunikacijų reguliuotojų. Kodeksas leidžia valstybėms narėms nustatyti skirtingas taisykles dėl teisėsaugos prieigos prie elektroninių ryšių duomenų, o tai gali lemti prieštaravimus tarp ES mastu siekiamos harmonizacijos ir nacionalinių teisės aktų. Ryšių paslaugų teikėjams taikomi papildomi tinklo saugumo ir incidentų valdymo reikalavimai gali būti traktuojami kaip papildoma našta, o skirtingas šių taisyklių aiškinimas gali prisidėti prie nevienodo 15 straipsnio įgyvendinimo praktikoje (Walden, 2021, p. 1717).

Svarbu būtų paminėti ir tai, kad privatumo ribojimo išimtys elektroninių ryšių sektoriuje kelia teisinių ir praktinių iššūkių, ypač atsižvelgiant į skirtingą valstybių narių požiūrį į jų taikymą ir reguliavimą. Kodekso ir e. privatumo direktyvos sąveikoje egzistuoja tam tikros įtampos dėl privatumo ribojimo išimčių, kadangi valstybės narės gali taikyti skirtingas taisykles, kyla reguliavimo fragmentacijos problemų, kurios gali apsunkinti elektroninių ryšių paslaugų teikimą visoje ES ir sukelti reikšmingų iššūkių paslaugų teikėjams. Vienas ryškiausių pavyzdžių – skirtingi duomenų saugojimo reikalavimai, dėl kurių įmonės, veikiančios keliose šalyse, priverstos taikyti nevienodas atitikties strategijas. Kaip antai, jei Prancūzija ar Vokietija reikalauja ilgesnio duomenų saugojimo laikotarpio nei Nyderlandai ar Belgija, įmonės turi prisitaikyti prie skirtingų reguliavimo standartų, o tai didina veiklos kaštus ir administracinę naštą. Be to, teisėsaugos prieigos prie duomenų reglamentavimas taip pat nėra vienodas, nes kai kuriose valstybėse, tokiose kaip Lenkija ar Vengrija, teisėsaugos institucijos gali gauti prieigą prie elektroninių ryšių duomenų be teismo leidimo, o Skandinavijos šalyse tokia prieiga yra griežčiau kontroliuojama (Europos Parlamentas, 2024). Dėl šių skirtumų gali kilti teisiniai ginčai dėl duomenų apsaugos pažeidimų, ypač kai paslaugų teikėjai susiduria su prieštaringais reguliavimo reikalavimais. Fragmentacija taip pat pasireiškia nevienodu sankcijų taikymu – jei Italija numato griežtesnes baudas už privatumo pažeidimus nei Portugalija, verslo sąlygos tarp skirtingų valstybių tampa nevienodos, o griežtesnio reguliavimo šalys gali tapti mažiau

patrauklios investuotojams. Technologinių reikalavimų skirtumai dar labiau apsunkina situaciją – jei viena valstybė reikalauja specifinių duomenų šifravimo standartų, kaip tai daro Ispanija, o kita, pavyzdžiui, Airija, leidžia laisvesnį technologijų pasirinkimą, įmonės priverstos diegti kelias skirtingas saugumo sistemas, kas didina veiklos sudėtingumą. Galiausiai, privatumo ribojimo priemonių taikymas taip pat nėra vieningas net visoje Europos Sąjungoje, kaip antai, jei viena valstybė leidžia vyriausybinėms institucijoms stebėti tam tikras elektroninių ryšių paslaugas viešojo saugumo tikslais, o kita tai draudžia remdamasi pagrindinių teisių apsaugos principais, susidaro teisinio nenuoseklumo situacija (EDAV Nuomonė 5/2019, 2019 m. kovo 12 d.). Tai gali paskatinti teisinį *„forum shopping“*, kai paslaugų teikėjai registruoja savo veiklą valstybėse su palankesniu reguliavimu, taip silpnindami bendrą Europos Sąjungos privatumo apsaugos sistemą. Reguliavimo fragmentacija ne tik didina elektroninių ryšių paslaugų teikėjų veiklos kaštus, bet ir sukuria teisinį neapibrėžtumą, kuris gali trukdyti bendros skaitmeninės rinkos veikimui. Todėl būtina siekti didesnio reguliavimo suderinamumo, kad būtų išvengta prieštaravimų ir užtikrinta nuosekli privatumo apsauga visose valstybėse narėse (EDAV Nuomonė 5/2019, 2019 m. kovo 12 d.).

Apibendrinant šios dalies analizę, galima teigti, kad pastarojo dešimtmečio reguliavimo pokyčiai Europos Sąjungoje reikšmingai transformavo asmens duomenų apsaugos politiką ir elektroninių ryšių sektoriaus reguliavimą. Nors BDAR nustatė bendruosius duomenų apsaugos standartus, elektroninių ryšių sektorius išliko specifinė sritis, reikalaujanti papildomo reguliavimo. Šią funkciją atliko e. privatumo direktyva, kuri kartu su BDAR užtikrina konfidencialumo apsaugą, slapukų naudojimo reglamentavimą ir kitus ryšių privatumo aspektus. Tačiau Direktyvos 2002/58/EB suteikiama diskrecija valstybėms narėms riboti privatumo teises pagal 15 straipsnio 1 dalį lėmė reguliavimo fragmentaciją, skirtingas nacionalines interpretacijas ir teisinio aiškumo trūkumą. ESTT formuojamoje jurisprudencijoje pabrėžia, kad privatumo ribojimai turi būti proporcingi ir aiškiai apibrėžti, tačiau kai kurios valstybės narės vis dar taiko plačias duomenų saugojimo ir stebėjimo priemones, kurios gali neatitikti ES teisės reikalavimų. Todėl reikalingas aiškesnis šios nuostatos įgyvendinimas nacionaliniuose teisės aktuose ir didesnė taikymo praktikos harmonizacija visoje ES. Šiame kontekste esminę reikšmę įgyja būsimas e. privatumo reglamentas, kuris turėtų pakeisti galiojančią e. privatumo direktyvą ir užtikrinti vienodesnį teisinį reguliavimą visose valstybėse narėse. Jo tikslas – pašalinti direktyvos trūkumus, aiškiai apibrėžti teisėsaugos prieigos prie duomenų sąlygas ir sumažinti reguliavimo fragmentaciją. Be to, Kodeksas dar labiau keičia elektroninių ryšių reguliavimo sistemą, nes plečia NRI įgaliojimus ir gali sukelti papildomų

teisinių kolizijų su BDAR bei e. privatumo direktyva. Kadangi Elektroninių ryšių kodeksas įtraukia naujus rinkos dalyvius, tokius kaip *OTT*, kyla klausimų dėl skirtingų priežiūros institucijų kompetencijų persidengimo ir bendros reguliavimo politikos suderinamumo. Tai reiškia, kad BDAR, e. privatumo direktyva ir Kodeksas turi būti aiškiai suderinti, siekiant užtikrinti vienodą privatumo apsaugą ir sklandų reguliavimo mechanizmų veikimą visoje ES. Skirtingos nacionalinės taisyklės ir neaiškus būsimo e. privatumo reglamento statusas išlieka didžiausiais iššūkiais, trukdančiais užtikrinti nuoseklią privatumo apsaugą elektroninių ryšių sektoriuje. Siekiant sumažinti šiuos iššūkius, būtina stiprinti reguliavimo aiškumą, užtikrinti, kad privatumo ribojimo išimtys būtų taikomos proporcingai ir pagal aiškius kriterijus, bei sustiprinti nacionalinių ir ES institucijų bendradarbiavimą. Tik taip galima užtikrinti skaidrią ir vieningą privatumo apsaugos sistemą, atitinkančią tiek technologinius pokyčius, tiek pagrindinių teisių apsaugos principus (EDAV Nuomonė 5/2019, 2019 m. kovo 12 d.).

4. E. privatumo direktyvos 15 straipsnio 1 dalies analizė

Kaip jau darbe buvo užsiminta – Direktyva 2002/58/EB numato išimtį, leidžiančią valstybėms narėms priimti teisės aktus, kuriais ribojamas tam tikrų e. privatumo direktyvos nuostatų taikymas, kai tai būtina demokratinėje visuomenėje. Tokia išimtis leidžia valstybėms narėms taikyti šiuos ribojimus, pavyzdžiui, e. privatumo direktyvos 5 straipsnio nuostatoms, kurios įtvirtina pranešimų ir su jais susijusių srauto duomenų konfidencialumo principą. Konfidencialumo principas draudžia klausytis, įrašyti, kaupti ar kitaip perimti elektroninius pranešimus be naudotojo sutikimo, išskyrus įstatymuose numatytas išimtis. Ribojimai gali būti taikomi ir e. privatumo direktyvos 6 straipsnio nuostatoms, reglamentuojančioms srauto duomenų tvarkymą. Šios nuostatos nustato, kad srauto duomenys gali būti saugomi ar tvarkomi tik tiek, kiek būtina paslaugų teikimui ir sąskaitų išrašymui, nebent teisės aktai numato kitaip. Panašiai ribojimai gali būti susiję su Direktyvos 2002/58/EB 8 straipsnio nuostatomis dėl skambinančiosios ir skambinamosios ryšio linijos identifikavimo bei jo apribojimo, taip pat su Direktyvos 2002/58/EB 9 straipsnyje įtvirtintomis vietos nustatymo duomenų tvarkymo taisyklėmis, kurios leidžia tokių duomenų tvarkymą tik gavus naudotojo sutikimą arba anonimizavus duomenis.

2006 m. priimta Direktyva 2006/24/EB, numatė pareigą saugoti tam tikras kategorijas duomenų teisėsaugos tikslams, tačiau 2014 m. balandžio 8 d. ESTT sprendimu byloje *Digital Rights Ireland* ši direktyva buvo pripažinta negaliojančia kaip nesuderinama su Chartijos nuostatomis (ESTT, *Digital Rights Ireland*, C-293/12, C-594/12). Nepaisant šio sprendimo ir duomenų saugojimo direktyvos panaikinimo ES lygmeniu, kai kurios valstybės narės, remdamosi šia direktyva arba jos pagrindu priimtais nacionaliniais aktais, iki šiol taiko panašias duomenų saugojimo taisykles savo nacionalinėje teisėje. Šie klausimai išlieka aktualūs vertinant pusiausvyrą tarp viešojo saugumo poreikių ir pagrindinių teisių į privatumą apsaugos, todėl jie bus detaliau nagrinėjami tolesnėse darbo dalyse.

4.1. E. privatumo direktyvos 15 straipsnio 1 dalies nuostatų taikymas

Taigi, pereinant prie konkrečių Direktyvos 2002/58/EB nuostatų, pažymėtina, jog paprastai siekiant užtikrinti nacionalinį saugumą, gynybą, viešąją tvarką ar vykdyti nusikalstamų veikų prevenciją, tyrimą, atskleidimą bei baudžiamąjį persekiojimą, valstybės narės gali pasitelkti Direktyvos 2002/58/EB 15 straipsnio 1 dalies nuostatą kaip priemonę kovoti su rimtomis grėsmėmis, keliančiomis pavojų valstybės institucijų veiklos stabilumui ir visuomenės gerovei.

Tai apima galimybę riboti asmens duomenų apsaugą, siekiant sustabdyti organizuotą nusikalstamumą, kovoti su terorizmu ir užkirsti kelią nesankcionuotam duomenų srautų naudojimui.

Ši konkreti e. privatumo direktyvos nuostata – 15 straipsnis – taikoma 5 ir 6 straipsniuose, 8 straipsnio 1–4 dalyse bei 9 straipsnyje įtvirtintoms konfidencialumo ir duomenų apsaugos taisyklėms, kurios reglamentuoja elektroninių pranešimų ir su jais susijusių duomenų konfidencialumą bei srauto duomenų saugojimą. Nacionalinės valdžios institucijos, siekdamos apsaugoti nacionalinį saugumą, visuomenės saugumą, gynybą ar vykdyti nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą, gali nustatyti ribojimus, kurie apima – leidimą teisėsaugai prieiti prie elektroninių pranešimų turinio arba su juo susijusių duomenų (pvz., šaltinio ir gavėjo identifikavimo duomenų, ryšio trukmės, laikų, vietos nustatymo duomenų) be naudotojo sutikimo; metaduomenų, susijusių su elektroniniais ryšiais, saugojimo ir prieigos teisėsaugai nustatymą, kai tai būtina teisėsaugos tikslams; laikinas duomenų saugojimo pareigas, jei šie duomenys yra būtini vėlesniam nusikalstamų veikų tyrimui ar prevencijai. Svarbu tai, jog bet kokie ribojimai turi būti aiškiai apibrėžti nacionaliniuose teisės aktuose, nurodant, kokie duomenys bus naudojami ir kokiems tikslams, o valstybės narės turi teisę, tačiau ne pareigą, įtvirtinti išimtis, leidžiančias riboti tam tikras konfidencialumo teises elektroninių ryšių sektoriuje, be kita ko ribojimai turi atitikti proporcingumo principą bei būti suderinti su ES teisės reikalavimais ir tarptautiniais žmogaus teisių apsaugos standartais.

Kalbant apie praktinį e. privatumo direktyvos nuostatos taikymą, šalys narės gali nustatyti pareigas elektroninių ryšių paslaugų teikėjams saugoti metaduomenis, įskaitant duomenis apie ryšio faktą, jo aplinkybes, siuntėjo ir gavėjo identifikavimą, skambučio laiką, trukmę, IP adresus bei vietos nustatymo duomenis. Tokia praktika suteikia teisėsaugai galimybę gauti informaciją, kuri gali būti esminė tiriant nusikalstamas veikas, tokius kaip terorizmas, organizuotas nusikalstamumas, nelegalių veiksmų organizavimas ar kitų rimtų grėsmių nustatymas. Pavyzdžiui, teisėsaugoms institucijoms gali būti suteikta galimybė nustatyti įtariamuosius ir jų bendrininkus pagal ryšio duomenis, atsekti ryšių eigą ir netgi nustatyti asmenų buvimo vietą, remiantis vietos nustatymo duomenimis, kurie gali būti naudojami siekiant išaiškinti nusikaltimus ar užkirsti kelią grėsmėms valstybės saugumui. Vis dėlto, šiems ribojimams taikomi ES ir tarptautinės teisės nustatyti reikalavimai, kurie užtikrina, kad asmens duomenų apsauga būtų gerbiama ir nenukentėtų pagrindinės teisės. Pirmiausia, ribojimai turi būti aiškiai apibrėžti nacionaliniuose teisės aktuose, nustatant konkrečius duomenis, kuriuos reikia saugoti, ir tikslus, kuriems šie duomenys gali būti naudojami. Tai

leidžia užkirsti kelią piktnaudžiavimui, užtikrinant, kad duomenys būtų naudojami tik pagal teisėtus tikslus, pvz., kovą su nusikalstamumu. Be kita ko, pagal ES teisę, visos priemonės, kuriomis ribojamos asmens teisės, turi būti pagrįstos proporcingumo principu. Tai reiškia, kad duomenys turi būti saugomi tik tiek, kiek būtina, ir tik tokiais atvejais, kai tai yra reikalinga tam tikroje tyrimo stadijoje. Pavyzdžiui, jeigu duomenys yra reikalingi tik tam tikro laikotarpio tyrimui, jie turi būti saugomi ne ilgiau, nei būtina pagal konkrečią bylą. Nacionalinės institucijos privalo užtikrinti, kad šie ribojimai nepažeistų asmens teisių į privatumą ir kad būtų laikomasi teisės aktų reikalavimų dėl duomenų saugojimo ir prieigos. Papildomai pastebėtina, jog šie ribojimai turi būti suderinti su tarptautiniais žmogaus teisių apsaugos standartais, tokiais kaip EŽTK, Chartija bei Europos Sąjungos sutarties 6 straipsniu (LVAT, ESTT praktikos apžvalga, 2015). Tai užtikrina, kad bet kokie teisėsaugos veiksmai, susiję su metaduomenų saugojimu ir naudojimu, nepažeistų asmenų teisių į privatumą ir laisvę, užkertant kelią savavališkam ar pertekliniam valdžios kišimuisi.

ESTT jurisprudencijoje taip pat aiškinama, jog ribojimai, susiję su e. privatumo direktyvos 15 straipsnio 1 dalimi turi būti ne tik konkretūs, bet ir tiksliai apibrėžti teisės aktuose. Tokie ribojimai privalo būti taikomi tik aiškiai apibrėžtiems tikslams ir niekada negali viršyti būtinybės reikalavimų, kad būtų išvengta nepagrįsto arba pernelyg plataus asmens teisių apribojimo. Pavyzdžiui, ESTT nurodė, kad įgyvendindamos ES teisės aktus, valstybės narės turi užtikrinti teisingą pusiausvyrą tarp skirtingų pagrindinių teisių, įskaitant teisę į privatų gyvenimą ir intelektinės nuosavybės apsaugą. ES Teisingumo teismas priimtame sprendime pabrėžė, kad nacionalinės valdžios institucijos ir teismai, aiškindami savo teisės aktus, ne tik turi užtikrinti atitiktį ES teisės normoms, bet ir garantuoti, kad teisės aktai nepažeidžia pagrindinių teisių bei bendrųjų ES teisės principų, tokių kaip proporcingumo reikalavimas (LVAT, ESTT praktikos apžvalga, 2015). Šis – *Productores de Música de España* prieš *Telefónica de España SAU* – sprendimas išryškino esminę nuostatą: asmens duomenų apsauga nėra absoliuti ir gali būti ribojama tik tam tikromis aplinkybėmis, tačiau tokie ribojimai turi būti aiškiai apibrėžti teisės aktuose – atitinkančiuose įstatymo lygmenį, kaip to reikalauja tiek Chartijos 52 straipsnis, tiek Direktyvos 2002/58/EB 15 straipsnio 1 dalis, – ir privalo užtikrinti proporcingumą bei veiksmingą teisinę gynybą asmenims, kurių duomenys yra tvarkomi (ESTT, *Productores de Música de España* prieš *Telefónica de España* SAU C-275/06).

Kaip nurodoma Europos Tarybos parengtame teisės aktų aiškinamajame memorandume dėl duomenų saugojimo teisėtumo, vertinant duomenų tvarkymo teisėtumą pagal EŽTK 8 straipsnį, EŽTT taiko trijų dalių testą – pirmiausia nustatoma, ar buvo pažeistos EŽTK 8 straipsnyje įtvirtintos teisės, apimančios privataus gyvenimo gerbimą ir susirašinėjimo

slaptumą; tuomet analizuojama, ar duomenų tvarkymas yra pagrįstas įstatymu, kitaip tariant, ar egzistuoja aiškus teisinis pagrindas nacionalinėje teisėje, atitinkantis teisinės valstybės principą, kuris reikalauja, kad duomenų tvarkymas būtų aiškiai reglamentuotas ir nuspėjamas; galiausiai vertinama, ar šis duomenų tvarkymas yra būtinas demokratinėje visuomenėje, siekiant užtikrinti viešąjį interesą, pavyzdžiui, nacionalinį saugumą ar nusikaltimų prevenciją (Teisės aktų memorandumas dėl duomenų saugojimo teisėtumo, 2003). Tokie kriterijai padeda aiškiai įvertinti, ar duomenų tvarkymo praktika atitinka konstitucinius ir tarptautinius standartus ir ar ji gali būti teisėta pagal Europos žmogaus teisių teisę. EŽTT praktika pateikia konkrečių šių principų taikymo pavyzdžių, tad svarbu paminėti ir klasikinius precedentus, kurie formavo EŽTT 8 straipsnio aiškinimo kryptį ir tebėra aktualūs tiek akademinėje doktrinoje, tiek vėlesnėje jurisprudencijoje:

a) **Byloje *Rotaru* prieš Rumuniją** konstatuota, kad Rumunijos slaptosios tarnybos rinko ir saugojo duomenis apie asmenį be aiškaus teisinio pagrindo (EŽTT, 2000, *Rotaru* prieš Rumuniją).
b) **Byloje *Amann* prieš Šveicariją** nustatyta, jog valdžios institucijos, be aiškaus teisinio pagrindo rinkusios ir saugojusios duomenis apie privatų asmenį, pažeidė EŽTK 8 straipsnį. Teismas konstatavo, kad tokie veiksmai buvo neproporcingi ir nesuteikė pareiškėjui veiksmingos teisinės apsaugos nuo valdžios kišimosi į jo privatų gyvenimą (EŽTT, 2000, *Amann* prieš Šveicariją).
c) **Byloje *Klass* ir kiti prieš Vokietiją** EŽTT nagrinėjo valdžios vykdytą slaptą telefoninių pokalbių sekimą dėl nacionalinio saugumo. Konstatuota, jog tokia praktika gali būti teisėta tik tada, kai ji aiškiai apibrėžta įstatymuose ir kai užtikrinama veiksminga apsauga nuo savavališko valdžios kišimosi į privatų gyvenimą (EŽTT, 1978, *Klas*s prieš Vokietiją).
d) **Byloje *Big Brother Watch* prieš JK** Teismas analizavo valstybės vykdytas masinio sekimo programas, kurios leido rinkti ir analizuoti didelius elektroninių ryšių duomenų srautus. Šioje sujungtoje byloje pareiškėjai ginčijo tris JK žvalgybos taikytas sekimo sistemas: (1) masinį elektroninių ryšių srauto perėmimą, (2) žvalgybos duomenų pasidalijimą su užsienio vyriausybėmis ir (3) privačių ryšių paslaugų teikėjų renkamų duomenų gavimą valdžios institucijų. EŽTT pripažino, kad pats masinio perėmimo mechanizmas nėra savaime nesuderinamas su Konvencija, jei valstybė užtikrina griežtas apsaugos priemones, tačiau JK taikytame mechanizme buvo nustatytas EŽTK 8 straipsnio pažeidimas dėl nepakankamos kontrolės, t. y. nebuvo nepriklausomos institucijos, kuri dar prieš pradedant sekimą patvirtintų, ką konkrečiai galima stebėti, nebuvo aiškių taisyklių, kaip pasirenkami žmonės ar duomenys, kuriuos reikia perimti. Galiausiai, surinktų

duomenų analizė nebuvo pakankamai prižiūrima, todėl kilo rizika, kad jie gali būti naudojami netinkamai. Taip pat konstatuota, kad komunikacijos meta-duomenų (pvz., ryšio išklotinių, vietos duomenų) gavimo iš telekomunikacijų bendrovių tvarka neatitiko Konvencijos reikalavimų – nebuvo numatyta išankstinė nepriklausoma priežiūra, o duomenų rinkimas neapsiribojo tik sunkių nusikaltimų tyrimu ir nesuteikė pakankamos apsaugos žurnalistų konfidencialiai komunikacijai (EŽTT, 2021, *Big Brother Watch prieš JK*).

e) **Byloje *Centrum för Rättvisa* prieš Švediją** EŽTT vertino žvalgybos tarnybos vykdomą plačios apimties elektroninių ryšių perėmimą nacionalinio saugumo tikslais. Nors toks sekimas savaime neprieštarauja EŽTK 8 straipsniui, Teismas nustatė pažeidimą dėl nepakankamų apsaugos priemonių. Trūko aiškių taisyklių dėl duomenų saugojimo terminų, nebuvo pareigos įvertinti privatumo rizikas dalijantis duomenimis su užsienio partneriais, o priežiūra po sekimo buvo neefektyvi. EŽTT pabrėžė, kad net ir nacionalinio saugumo atveju būtinos pagrindinės garantijos: nepriklausomas leidimas sekimui, aiškus tikslas ir apimtis, bei veiksminga kontrolė. Švedijos sistema šių standartų neatitiko, todėl buvo pripažinta, kad ji nesuteikė pakankamos apsaugos nuo valdžios piktnaudžiavimo. Šis sprendimas dar kartą patvirtina, kad pagal e. privatumo direktyvos 15 straipsnio 1 dalį valstybės negali taikyti masinio sekimo be griežtos, nepriklausomos ir proporcingos kontrolės (EŽTT, 2021, *Centrum för Rättvisa* prieš Švediją).

f) **Byloje *Škoberne* prieš Slovėniją** EŽTT vertino buvusio teisėjo nuteisimą už korupciją, kuris rėmėsi ir jo ryšio metaduomenimis, gautais pagal tuo metu galiojusią Slovėnijos duomenų saugojimo tvarką. Įstatymai įpareigojo operatorius 14 mėnesių saugoti visų naudotojų ryšio ir vietos duomenis, nepriklausomai nuo jų veiksmų ar rizikos. Nors vėliau ši praktika buvo pripažinta prieštaraujančia tiek Slovėnijos Konstitucijai, tiek ES teisei, EŽTT nusprendė, kad tuo metu taikytas duomenų rinkimas buvo neteisėtas ir neproporcingas, todėl pažeidė EŽTK 8 straipsnį. Teismas pabrėžė, kad visuotinis, nediferencijuotas duomenų saugojimas nėra *„būtinas demokratinėje visuomenėje“* ir nesuteikia apsaugos nuo galimo valdžios piktnaudžiavimo (EŽTT, 2024, *Škoberne* prieš Slovėniją).

Taigi asmens duomenų apsauga nėra absoliuti – ji gali būti ribojama tam tikromis aplinkybėmis, tačiau tokie ribojimai privalo būti aiškiai nurodyti teisės aktuose, proporcingi ir užtikrinantys veiksmingą teisinę gynybą asmenims, kurių duomenys yra tvarkomi (Teisės aktų memorandumas dėl duomenų saugojimo teisėtumo, 2003). Vertinant e. privatumo direktyvos

15 straipsnio 1 dalies įtvirtintas ribojimų galimybes, būtina pažymėti, kad jos taikymo sąlygos glaudžiai dera su EŽTK 8 straipsnyje nustatytais standartais. EŽTK numato, kad teisė į privatų gyvenimą gali būti ribojama tik tuomet, kai tai būtina siekiant apsaugoti valstybės saugumą, viešąją tvarką, sveikatą, moralę ar kitas svarbias vertybes. EŽTT praktika iliustruoja šių principų *taikymą konkrečiose situacijose:*

g) *Byloje* ***Segerstedt-Wiberg*** **ir kiti prieš Švediją** pripažinta, kad atsisakymas suteikti asmeniui prieigą prie policijos registre esančios informacijos gali būti pateisinamas, jei toks ribojimas būtinas siekiant apsaugoti nacionalinį saugumą ir vykdyti kovą su terorizmu (EŽTT, 2006, *Segerstedt-Wiberg* ir kiti prieš Švediją).

h) **Byloje *Kruslin* prieš Prancūziją** EŽTT nustatė, kad telefoninių pokalbių kontrolė buvo įgyvendinta remiantis pernelyg neapibrėžtomis taisyklėmis, nesuteikusiomis tinkamų garantijų prieš savavališką kišimąsi į privatų gyvenimą (EŽTT, 1990, *Kruslin* prieš Prancūziją).

i) **Byloje *Foxley* prieš JK** Teismas konstatavo, kad valdžios institucijų sprendimas perimti asmeninę korespondenciją be pakankamų teisinių apsaugos priemonių ir veiksmingos kontrolės mechanizmų pažeidė EŽTK 8 straipsnį (EŽTT, 2000, *Foxley* prieš JK)[1].

Sprendimuose išnagrinėjus nurodytas bylas teigiama – kišimasis į asmens privatumą gali būti teisėtas tik tuomet, kai jis yra aiškiai reglamentuotas įstatyme, proporcingas ir būtinas demokratinėje visuomenėje. Toks požiūris aktualus ir po 2001 m. rugsėjo 11 d. įvykių, kai daugelis valstybių ėmėsi griežtesnių saugumo priemonių, sukeldamos diskusijas dėl jų suderinamumo su žmogaus teisių apsauga. Taigi, bet kokie privatumo ribojimai, įtvirtinti nacionaliniuose teisės aktuose remiantis e. privatumo direktyvos 15 straipsnio 1 dalimi, turi būti grindžiami aiškiais teisiniais pagrindais ir atitikti nustatytus standartus, siekiant užtikrinti pusiausvyrą tarp viešojo intereso apsaugos ir asmens teisių į privatumą.

4.2. Duomenų saugojimas sunkių nusikaltimų tyrimo, atskleidimo bei persekiojimo tikslais

Elektroninių ryšių sektoriuje generuojami duomenys – nuo srauto metaduomenų iki vietos nustatymo informacijos – šiandien tapo neatsiejama teisėsaugos arsenalą formuojančia

[1] Sprendimų analizei pasirinkti tiek klasikiniai precedentai, formavę EŽTT 8 straipsnio aiškinimą, tiek naujesni sprendimai, atspindintys dabartines technologines grėsmes. Teismo sprendimai atrinkti remiantis jurisprudencijos analize, akademiniais šaltiniais ir EŽTT sprendimų paieška (HUDOC sistema).

priemone. Tokių duomenų prieinamumas leidžia ne tik rekonstruoti nusikalstamą veiklą, bet ir operatyviai reaguoti į grėsmes visuomenės saugumui. Vis dėlto duomenų rinkimo ir saugojimo procesas atveria kertinį teisinių diskusijų lauką: kaip suderinti teisę į privatų gyvenimą ir duomenų apsaugą su visuomenės poreikiu užtikrinti efektyvų sunkių nusikaltimų tyrimą ir prevenciją? Pagrindinis ES reguliavimo instrumentas, leidžiantis nacionalinėms institucijoms įvesti privalomą elektroninių ryšių duomenų saugojimą – Direktyva 2002/58/EB. Nors šis teisės aktas suteikia valstybėms narėms diskreciją tam tikromis sąlygomis riboti asmens privatumo teises, jo nuostatų formuluotės neapibrėžtumas sudaro prielaidas labai plačioms interpretacijoms, kurios ne tik skatina teisės taikymo fragmentaciją tarp valstybių narių, bet ir kelia riziką, kad duomenų saugojimo praktikos taps plataus masto, nediferencijuotos bei neatitiks Chartijos 7 straipsnio (teisė į privatų gyvenimą) ir 8 straipsnio (teisė į asmens duomenų apsaugą) reikalavimų. Šią problemą ypač ryškiai iliustruoja Direktyvos 2006/24/EB (duomenų saugojimo direktyvos) panaikinimas. ESTT aiškiai konstatuoja – plataus masto, vienodai taikomas duomenų saugojimas neatitinka proporcingumo principo ir peržengia būtino saugumo poreikio ribas. Tačiau šių sprendimų palikta teisinė tuštuma – aiškios gairės, kokius konkrečius duomenis ir kokiomis sąlygomis valstybės narės gali saugoti remiantis e. privatumo direktyvos 15 straipsniu – iki šiol nėra išspręsta. Šioje dalyje sistemingai analizuojama e. privatumo direktyvos 15 straipsnyje numatyta valstybių narių teisinė diskrecija ir jos ribos, lyginant ES institucijų nuomones su ESTT praktika (29 str. darbo grupės nuomonės Nr. 10/2001 ir Nr. 3/2006). Taip pat nagrinėjama, kaip Vokietija, Prancūzija ir Lietuva interpretuoja *„sunkių nusikaltimų“* sąvoką bei kokius duomenis privalo saugoti, vertinant fundamentalių teisių balansą tyrimo bei prevencijos kontekste. Šios šalys pasirinktos dėl akivaizdžiai skirtingų nacionalinių požiūrių į Direktyvos 2002/58/EB 15 straipsnio 1 dalies įgyvendinimą ir taikymą: jos leidžia atskleisti, kaip teisinio reguliavimo neapibrėžtumas ES lygmeniu skatina fragmentuotas praktikas, kurios kelia riziką nevienodai užtikrinti asmens teises skirtingose valstybėse narėse. Galiausiai pateikiamos rekomendacijos siekiant sukurti vieningą, proporcingą ES reguliavimą, suderinant efektyvų tyrimą su asmens teisėmis.

Visų pirma, duomenų saugojimas yra būtina priemonė efektyviam sunkių nusikaltimų tyrimui, atskleidimui ir baudžiamajam persekiojimui. ES teisės sistemoje pagrindinė nuostata, suteikianti valstybėms narėms galimybę įvesti privalomą elektroninių ryšių duomenų saugojimą, yra e. privatumo direktyvos 15 straipsnio 1 dalis. Ši nuostata leidžia nacionalinėms valdžioms apriboti elektroninių ryšių vartotojų konfidencialumą *„kai tai būtina nacionalinio saugumo, viešojo saugumo arba nusikalstamumo prevencijos tikslais“*, tačiau teisės aktų nuostatose neišdėstoma, kokie konkretūs duomenų tipai ir kokiomis sąlygomis gali būti

saugomi, kas sukuria plačias interpretacijos galimybes ir iš esmės palieka diskreciją valstybėms narėms nustatyti savo taisykles. 29 straipsnio duomenų apsaugos darbo grupės (dabar – EDAV) Nuomonė Nr. 10/2001 ir Nuomonė Nr. 3/2006 aiškiai pabrėžia, kad *„bet koks duomenų saugojimas turi būti proporcingas, teisėtas ir aiškiai reglamentuotas teisės aktuose, siekiant užtikrinti pusiausvyrą tarp viešojo saugumo interesų ir asmens teisės į privatumą“* (29 str. darbo grupės nuomonės Nr. 10/2001 ir Nr. 3/2006). Nuomonėse darbo grupė atkreipia dėmesį į riziką, kad plačios apimties duomenų rinkimas gali tapti pernelyg invazinis ir neatitikti Chartijos 7 ir 8 straipsnių nuostatų apie teisę į privatumą bei asmens duomenų apsaugą. Kaip jau buvo užsiminta šios darbo dalies pradžioje, svarbiausias precedentas šioje srityje – ESTT sprendimai bylose *Digital Rights Ireland* (sujungtos bylos C-293/12 ir C-594/12) bei *Tele2 Sverige AB ir Watson* (sujungtos bylos C-203/15 ir C-698/15), kuriuose buvo suformuluoti pagrindiniai privatumo ribojimų vertinimo principai. Abu sprendimai vienareikšmiškai nurodė, kad Direktyvos 2006/24/EB nuostatos dėl plataus masto ir vienodo visų vartotojų elektroninių ryšių duomenų saugojimo pažeidžia proporcingumo principą. ESTT konstatavo, kad duomenų saugojimo reikalavimas turi būti tiksliai nukreiptas**,** laikinai ir diferencijuotas, o jo apimtis – griežtai ribota pagal konkrečias nusikalstamos veikos kategorijas. Tokiu būdu ESTT įtvirtino, jog bet koks ES teisės aktas, leidžiantis rinkti ir saugoti elektroninių ryšių duomenis, turi atitikti ES pagrindinių teisių standartus ir proporcingumo principą. Tolesnėje praktikoje šie standartai buvo papildomai konkretizuoti Didžiosios kolegijos 2022 m. balandžio 5 d. sprendimu byloje *G. D. prieš Commissioner of An Garda Síochána ir kt.* (C-140/20). ESTT šioje byloje aiškiai nurodė, kad Direktyvos 2002/58/EB 15 straipsnio 1 dalis, aiškinama kartu su Chartijos 7, 8, 11 ir 52 straipsniais, draudžia bet kokias nacionalines teisėkūros priemones, kurios numato bendrą ir nediferencijuotą srauto bei vietos nustatymo duomenų saugojimą, net kai siekiama kovoti su sunkiais nusikaltimais ar užkirsti kelią didelėms grėsmėms visuomenės saugumui. Dar daugiau, ESTT pabrėžė, kad prieiga prie tokių duomenų turi būti griežtai reglamentuota ir leidžiama tik remiantis išankstine, nepriklausoma teisminės arba administracinės institucijos kontrole, o ne vien instituciniu formaliu tikrinimu. Vadovaujantis tuo buvo atmesta galimybė, kad prieigos sprendimus priiminėtų patys policijos pareigūnai ar jiems pavaldūs padaliniai, nes tokia praktika pažeidžia nepriklausomumo ir nešališkumo principus. Ši byla dar kartą primena, kad nacionalinės praktikos, kurios nesuteikia tinkamo išankstinio teisminio kontrolės mechanizmo ar leidžia diskrecinį, plačios apimties saugojimą, prieštarauja ES teisei, net jei jų tikslas – kova su sunkiais nusikaltimais. Tai taip pat patvirtina būtinybę aiškiai apibrėžti ir

riboti nacionalinių teisės aktų taikymo ribas, siekiant išvengti proporcingumo pažeidimų ir užtikrinti vienodą teisių apsaugą visoje ES.

Europos Komisijos komunikatai ir pasiūlymai bandė šią spragą užpildyti. 2005 m. pateiktame pasiūlyme dėl duomenų saugojimo direktyvos (žr. Europos Komisijos pasiūlymas, 2005, COM(2005) 438 final) EK nurodė, kad saugomi duomenys turėtų būti griežtai susiję su konkrečių nusikaltimų tyrimu ir saugojami tik minimalų laiką (Darbo grupė, 2005, Nuomonė 4/2005). Tačiau šis pasiūlymas, kuriuo buvo grindžiama vėliau priimta duomenų saugojimo direktyva, sulaukė netiesioginės kritikos, kai ESTT pripažino pačią direktyvą negaliojančia dėl jos neatitikimo pagrindinių teisių apsaugos standartams (ESTT, *Digital Rights Ireland*, C-293/12 ir C-594/12).Vėlesni Europos Komisijos komunikatai (pvz., 2022, 2023 m. komunikatai dėl duomenų saugojimo politikos ateities ir duomenų apsaugos reformos) akcentuoja, jog būtinas aiškus ES reguliavimo standartas, bet konkrečių teisės aktų pakeitimų iki šiol nėra priimta. Remiantis analize dabartinė padėtis rodo, kad ES lygmeniu egzistuoja trys esminės teisinių spragų kategorijos – **apibrėžties trūkumas**: nėra vieningo sutarimo, kas yra *„sunkaus nusikaltimo“* sąvoka, todėl valstybės gali įtraukti skirtingas nusikaltimų kategorijas; p**roporcingumo kriterijų nepakankamas įgyvendinimas**: nėra ES teisės akto, kuris detalizuotų, kaip užtikrinti duomenų rinkimo diferencijavimą, minimalią saugojimo trukmę ir prieigos kontrolę; **priežiūros mechanizmų nebuvimas**: ES direktyvos ir sprendimai numato principus, tačiau trūksta privalomų priežiūros, audito ar teisinės kontrolės priemonių, kurios garantuotų, kad nacionalinės taisyklės atitiktų ES standartus. Tokiu būdu galima konstatuoti, kad nors e. privatumo direktyvos 15 straipsnio 1 dalis išlieka teisiniu pagrindu duomenų saugojimui, Direktyva 2002/58/EB yra struktūriškai nepakankama ir nepakankamai sureguliuota ES lygmeniu. Ši situacija verčia valstybes nares pasirinkti tarp skirtingų teisinės aiškumo lygmenų ir leidžia jų nacionalinėms praktikoms plėstis už proporcingumo ribų. Kitoje darbo dalyje bus nagrinėjama, kaip šis ES teisinis neapibrėžtumas atsispindi konkrečiose nacionalinėse duomenų saugojimo praktikose ir kokius iššūkius tai kelia teisės vienybei bei asmens teisių apsaugai.

Antra, Vokietijos, Prancūzijos ir Lietuvos nacionalinės duomenų saugojimo praktikos yra akivaizdžiai fragmentuotos. Europos Sąjungos teisinio vakuumo fone valstybės narės ėmėsi skirtingų sprendimų, kaip interpretuoti e. privatumo direktyvos 15 straipsnį ir apibrėžti *„sunkių nusikaltimų“* sąvoką. Tokia situacija iš dalies kyla dėl to, kad baudžiamosios teisės sritis pagal Sutarties dėl Europos Sąjungos veikimo (SESV) 4 ir 83 straipsnius priklauso dalijamai kompetencijai, o valstybių narių prerogatyvos čia išlieka reikšmingos. ES gali tik nustatyti bendrus minimalius reikalavimus tam tikrose srityse, pavyzdžiui, terorizmo ar

organizuoto nusikalstamumo, tačiau neapibrėžia visų nusikaltimų kategorijų vienodai. Todėl nėra ir negali būti centralizuoto ES lygmens *„sunkaus nusikaltimo“* apibrėžimo, o valstybės šią sąvoką taiko remdamosi savo nacionaliniais baudžiamosios teisės principais. Tokia įvairovė sukuria sisteminę fragmentaciją, kuri ne tik kenkia teisės vienybei, bet ir kelia riziką, kad ES piliečių privatumo apsauga skirsis priklausomai nuo jų buvimo vietos (Jones Day, 2016).

Kaip antai, Vokietijos duomenų saugojimo režimas, nors ir apribotas – telefonijos metaduomenis saugoti 10 savaičių, o vietos nustatymo duomenis 4 savaites – laikomas bendro ir neselektyvaus pobūdžio**,** nes taikomas visiems vartotojams be išankstinio selektyvaus kriterijaus (Jones Day, 2016). ESTT patvirtino, kad net trumpesni saugojimo terminai neatšaukia grėsmės privatumui, nes masiškai renkami duomenys leidžia formuoti išsamias asmenų profilių schemas (ESTT, *Privacy Internationa*, C-793/19, C-794/19). Todėl Vokietijos nacionalinė tvarka, nors ir griežtesnė nei ankstesnės direktyvos reikalavimai, vis tiek prieštarauja Chartijos 7 ir 8 straipsniams dėl proporcingumo trūkumo (eucrim, 2022).

Kalbant apie Prancūzijos teisės aktus (Prancūzijos elektroninių ryšių ir pašto kodeksas, 1952), pažymėtina, jog jie įpareigoja saugoti metaduomenis **vienerius metus**, apimančius tiek telefonijos, tiek interneto ryšio duomenis. Teisėsauga argumentuoja, kad privalomas duomenų saugojimas yra būtinas kovai su sunkiu nusikalstamumu, tačiau Prancūzijos *le Conseil d'État* (Prancūzijos aukščiausiasis administracinis teismas) sprendimai rodo, jog tokia praktika gali pažeisti ES proporcingumo principą dėl per didelės apimties ir trukmės. Prancūzijos sistema leidžia plačią valstybės prieigą prie duomenų, bet neužtikrina aiškių ribų, kaip ir kokiomis sąlygomis galima kreiptis dėl informacijos (Jones Day, 2016).

Lietuvoje nustatytas ribotas duomenų saugojimo terminas, tačiau neaiškiai apibrėžta *„sunkaus nusikaltimo“* sąvoka palieka erdvės plačiai interpretacijai, kuri gali lemti perteklinį duomenų rinkimą. Nacionaliniuose teisės aktuose duomenų saugojimo trukmė nustatyta 6 mėnesiams (Elektroninių ryšių įstatymo 96 straipsnis), vis dėlto nėra aišku, kuri nusikalstamos veikos kategorija suteikia pagrindą taikyti tokią priemonę. Lietuvos Respublikos baudžiamojo kodekso 11 straipsnis klasifikuoja nusikaltimus pagal jų pavojingumo laipsnį, tačiau Direktyvos 2002/58/EB 15 straipsnio 1 dalyje nepateikiama, kokio sunkumo nusikaltimams duomenų saugojimas gali būti taikomas. Tai susiję su tuo, kad e. privatumo direktyva buvo priimta 2002 m., dar iki Lisabonos sutarties, kuri nuo 2009 m. suteikė Europos Sąjungai ribotą kompetenciją baudžiamosios teisės ir baudžiamojo proceso srityje (SESV 82–83 straipsniai). Todėl šių sąvokų suvienodinimas išliko valstybių narių prerogatyva, o tai lemia esminius skirtumus taikant duomenų saugojimą. Nacionalinės institucijos tokiomis aplinkybėmis gali taikyti e. privatumo direktyvą plačiau, nei numato jos tikslas, įtraukdamos

net vidutinio sunkumo ar mažesnio pavojingumo veikas. Šį Lietuvos teisinio reguliavimo trūkumą išryškino ESTT 2023 m. sprendime byloje *A. G. prieš Lietuvos Respublikos generalinę prokuratūrą* (C-162/22). Šioje byloje nagrinėta situacija, kai Lietuvos Generalinė prokuratūra, vykdydama tarnybinio nusižengimo tyrimą dėl galimo prokuroro piktnaudžiavimo, rėmėsi kriminalinės žvalgybos metu surinktais elektroninių ryšių srauto ir vietos nustatymo duomenimis. Šie duomenys, pasak ESTT, buvo surinkti kovos su sunkiais nusikaltimais tikslu ir todėl negali būti naudojami mažesnės svarbos tikslams, tokiems kaip tarnybinių ar drausminių nusižengimų tyrimas. ESTT akcentavo, kad pagal Direktyvos 2002/58/EB 15 straipsnio 1 dalį bet koks konfidencialumo ribojimas turi būti būtinas demokratinėje visuomenėje ir proporcingas siekiamam tikslui, o šių kriterijų neįmanoma užtikrinti, kai duomenys naudojami kitokiu – mažesnės svarbos – pagrindu nei jų pradinio rinkimo tikslas. Sprendimas ne tik pagrindžia būtinybę aiškiai apibrėžti *„sunkaus nusikaltimo“* ribas nacionaliniuose teisės aktuose, bet ir parodo, jog dabartinis toks reglamentavimas kuria praktikas, prieštaraujančias ES teisei bei proporcingumo principui.

Toliau, palyginamosios analizės būdu nustatyti esminiai Vokietijos, Prancūzijos ir Lietuvos duomenų saugojimo skirtumai pateikiami autorės parengtoje lentelėje. Kaip jau buvo užsiminta anksčiau, konkrečios šalys pasirinktos siekiant atskleisti skirtingus nacionalinius požiūrius į e. privatumo direktyvos įgyvendinimą bei pademonstruoti, kaip Europos Sąjungos teisės neapibrėžtumas baudžiamosios teisės sankirtoje su duomenų apsauga lemia nevienodą asmens teisių užtikrinimą priklausomai nuo buvimo valstybėje:

	Duomenų saugojimo laikotarpis	**Duomenų apimtis**	***„Sunkaus nusikaltimo“* apibrėžtis**	**Prieigos kontrolė**
DE	10 sav. (ryšio ir interneto metaduomenys), 4 sav. (vietos duomenys).[2]	Telefono skambučių, SMS, interneto prisijungimų duomenys. Turinys nesaugomas – nedraudžiama saugoti pokalbių, SMS teksto, el. laiškų turinio ar aplankytų puslapių URL.[3]	Apibrėžta įstatyme – duomenys gali būti naudojami tik tiriant ypač sunkius nusikaltimus, išvardytus baudž. proc. kodekse (terorizmas, nužudymai, pagrobimai), kitiems nusikaltimams duomenų naudoti neleidžiama.	Ribota, selektyvi prieiga: tik teisėsaugos institucijoms, tik su teismo orderiu ir tik sunkių nusikaltimų tyrimui. Kitiems tikslams naudoti draudžiama. Yra griežta teisminė ir techninė priežiūra.[4]

[2] Vokietijos Telekomunikacijų įstatymo (TKG) 176-180 straipsniai.
[3] Ten pat.
[4] Vokietijos Telekomunikacijų įstatymo (TKG) 113 straipsnis.

FR	12 mėn. visiems nustatytiems duomenims.[5]	Platus metaduomenų spektras: vartotojų identifikavimo duomenys; srauto duomenys – skambučių, SMS, el. komunikacijų datos, laikas, adresatai ir aplankytų interneto svetainių adresų sąrašai; vietos duomenys. Turinio duomenys nesaugomi.[6]	Nėra aiškiai apribota – saugojimas skirtas bendram kovos su nusikalstamumu ir terorizmu tikslui, o ne išimtinai sunkiems nusikaltimams. Teisės aktuose *„sunkaus nusikaltimo“* kriterijus tiesiogiai neapibrėžtas – duomenys prieinami tiriant bet kurią nusikalstamą veiką, nors praktiškai akcentuojami sunkesni nusikaltimai.[7]	Plati prieiga, su tam tikra priežiūra: duomenis gali gauti teisėsaugos institucijos vykdydamos tyrimą, taip pat žvalgybos ir kitos valdžios institucijos nacionalinio saugumo tikslais. Teisėsauga duomenis gauna per teisinį procesą, žvalgybos tarnybų prieiga administracinė Prieiga neselektyvi savo apimtimi – duomenys kaupiami apie visus gyventojus, tačiau jų naudojimas formaliai kontroliuojamas.[8]
LT	6 mėn. (daugumai ryšio ir vietos duomenų). Tam tikri mažiau reikšmingi duomenys, pvz., nepavykusių skambučių registro įrašai, saugomi trumpiau – ~2 mėn. [9]	Visi pagrindiniai ryšio metaduomenys – telefono ryšio duomenys, interneto prieigos duomenys, mobiliojo ryšio buvimo vietos duomenys. Turinys nesaugomas, tik suvestiniai duomenys.[10]	Įstatymai nenurodo, kad duomenys renkami tik dėl sunkių nusikaltimų. Prievolė suformuluota bendrai nusikalstamų veikų prevencijai, atskleidimui ir tyrimui, tad apima ir mažesnio sunkumo veikas. Intervencijos intensyvumas vėliau diferencijuojamas per BPK: pvz., turinio pasiklausymai galimi tik esant sunkiems/labai sunkiems nusikaltimams, tačiau metaduomenims tokia aiški riba nenumatyta. Tai reiškia, kad *„sunkaus nusikaltimo”* sąvoka duomenų saugojimo kontekste nėra teisės akte tiksliai atribota – bent formaliai duomenys gali būti naudojami ir tyrimuose dėl nesunkių nusikaltimų.[11]	Prieiga ribojama teisėsaugai, tačiau saugojimas – visuotinis. Praktikoje saugomus duomenis gali gauti teisėsaugos institucijos vykdydamos ikiteisminius tyrimus. Žvalgybos tarnybos taip pat gali gauti prieigą nacionalinio saugumo tyrimuose, vadovaudamosi žvalgybos įstatymu ir gavusios nustatytus leidimus. Prieigos pobūdis: selektyvus konkretaus tyrimo rėmuose (nėra taip, kad visų piliečių duomenys būtų nuolat tiesiogiai prieinami – jie pateikiami tik pateikus užklausą dėl konkretaus asmens ar įvykio).[12]

1 lentelė. Nacionalinių duomenų saugojimo sistemų palyginimas

šaltinis: autorės sudaryta

[5] Prancūzijos Pašto ir elektroninių komunikacijų kodekso 34-1 straipsnis.
[6] Prancūzijos Pašto ir elektroninių komunikacijų kodekso 34-1 straipsnis.
[7] Prancūzijos Pašto ir elektroninių komunikacijų kodekso 34-1 straipsnis.
[8] Prancūzijos Pašto ir elektroninių komunikacijų kodekso 34-1 straipsnis.
[9] Lietuvos Respublikos elektroninių ryšių įstatymo Nr. IX-2135 pakeitimo įstatymas, 78 straipsnis.
[10] Ten pat.
[11] Lietuvos Respublikos baudžiamojo proceso kodeksas Nr. VIII-1968 154 straipsnis.
[12] Valstybinės duomenų apsaugos inspekcijos gairės (2024).

Nors analizė apima tik kelias valstybes nares, jų atvejai rodo, kad ES lygmeniu vis dar nėra pakankamai aiškaus mechanizmo, kuris užtikrintų proporcingą, tikslingą ir teisiškai apsaugotą duomenų saugojimo praktiką visose valstybėse narėse. Tokia situacija ne tik sukuria teisinį neapibrėžtumą tarptautiniams elektroninių ryšių paslaugų teikėjams, bet ir sudaro galimybes valstybėms narėms piktnaudžiauti duomenų saugojimo reikalavimais platesniu mastu. Papildomai tai sustiprina riziką, jog privatūs tinklai (pvz., įmonių vidaus ryšių sistemos ar darbuotojų stebėjimo priemonės), patekę į reguliacinę spragą, suformuos vadinamąją *„pilkąją zoną“*, kurioje duomenų apsaugos standartai taikomi fragmentuotai ar nepakankamai nuosekliai.

Trečia, proporcingumo principas ir 29 straipsnio duomenų apsaugos darbo grupės nuomonės yra svarbūs kriterijai, apibrėžiantys duomenų saugojimo priemonių taikymo ribas. Taigi, proporcingumas reikalauja, kad bet kokios valstybės taikomos priemonės būtų tiksliai nukreiptos, būtinos ir nedaug išplečiamos už konkretaus tikslo ribų (Europos Sąjungos sutarties 5 straipsnio 4 dalis). Direktyvos 2002/58/EB 15 straipsnio 1 dalis suteikia teisę riboti konfidencialumą, tačiau be aiškių ribų proporcingumo principas praranda prasmę, o nacionalinės praktikos gali peržengti Chartijos garantijas. Nuomonė Nr. 10/2001 pabrėžia, kad duomenų saugojimas turi būti pagrįstas aiškiu teisėkūros aktu, apibrėžiančiu saugojamų duomenų apimtį, saugojimo terminą ir prieigos sąlygas (29 straipsnio duomenų apsaugos darbo grupė, 2001). Darbo grupė ragina vengti masinio ir nediferencijuoto rinkimo, atkreipdama dėmesį, kad per didelis duomenų kaupimas kenkia pagrindinėms teisėms į privatumą ir asmens duomenų apsaugą. Nuomonė Nr. 3/2006 toliau konkretizuoja proporcingumo reikalavimą, aiškindama, kad duomenų saugojimo tvarka turi atitikti tris kriterijus: būtinybė – saugomi tik tie duomenys, kurie yra tiesiogiai susiję su sunkių nusikaltimų tyrimu ar prevencija; ribotumas – saugojimo trukmė ir duomenų tipas turi būti minimalūs; teisinis aiškumas – prieiga prie saugomų duomenų turi būti reglamentuota, kontroliuojama ir audituojama nepriklausomos institucijos. Darbo grupė ypač kritikuoja plačią *„duomenų tvarkymo“* sąvoką, kuri leidžia interpretacijas nuo minimalios metaduomenų saugojimo iki pilnos komunikacijos turinio saugojimo. Tokios praktikos neatitinka proporcingumo ir reikalingumo kriterijų, nes jos peržengia būtiną priemonių ribą, kurią nustato Chartijos 7 ir 8 straipsniai.

Kalbant apie praktinius proporcingumo vertinimo iššūkius, pažymėtina, jog ESTT sprendimai aiškiai nustatė, kad bendro pobūdžio duomenų saugojimas yra neproporcingas (ESTT, *Digital Rights Ireland* C-293/12 ir C-594/12; ESTT, *Tele2 Sverige ir Watson,* C-203/15 ir C-698/15). Tačiau Direktyvos 2002/58/EB 15 straipsnis lieka teisiniu šablonu, neįpareigojančiu valstybių narių nustatyti griežtus kriterijus, kaip šį principą taikyti. Todėl

atsiranda trys pagrindinės problemos – duomenų kategorijų neaiškumas: nėra ES sąrašo, kokie metaduomenys privalo būti saugomi (pvz., ryšio pradžios laikas, skambintojo numeris, vietos duomenys), o nacionalinės taisyklės apima skirtingas kategorijas; saugumo trukmės skirtumai: nors ESTT reikalauja minimalaus laikotarpio, valstybės nustato laikotarpius nuo 4 savaičių (Vokietija) iki 12 mėnesių (Prancūzija), o Lietuvoje – 6 mėnesius. Šios variacijos rodo, kad proporcingumo kriterijus netaikomas vienodai; prieigos kontrolės spragos: ES direktyvos nenumato privalomų audito mechanizmų ar nepriklausomų priežiūros institucijų reikalavimų, todėl nacionalinės prieigos procedūros skiriasi nuo griežtos teisminės priežiūros iki administracinės kontrolės.

Autorės vertinimu, funkcinis duomenų saugojimas – kitaip tariant, duomenų kaupimas konkretaus teisėsaugos tyrimo kontekste – turėtų būti taikomas tik esant aiškiam ryšiui su tam tikromis nusikalstamų veikų kategorijomis, tokiomis kaip organizuotas nusikalstamumas ar seksualiniai nusikaltimai prieš nepilnamečius. Nors Europos Sąjunga neturi tiesioginės kompetencijos priimti teisės aktus, apibrėžiančius nacionalinių baudžiamųjų veikų sudėtį, pagal SESV 83 straipsnį ji gali nustatyti minimalius reikalavimus tam tikrose srityse, taip skatindama vienodesnį duomenų apsaugos standartų taikymą. Šiuo atveju aktualu, kad nepilnamečio sąvoka valstybėse narėse gali skirtis, tačiau, remiantis Jungtinių Tautų Vaiko teisių konvencija (1989, 1 straipsnis), taip pat Europos Komisijos 2021 m. Vaiko teisių strategija (COM(2021) 142 final), rekomenduojama orientuotis į iki 18 metų amžiaus ribą. Be to, įtvirtinus aiškų minimalios priemonės principą, pagal kurį duomenų saugojimo trukmė turėtų būti nustatoma atsižvelgiant į jų svarbą ir poveikį asmens teisėms – pavyzdžiui, vietos nustatymo duomenys galėtų būti saugomi ne ilgiau kaip 30 dienų, o skambučių metaduomenys – ne ilgiau kaip 90 dienų. Valstybės narės turėtų užtikrinti, kad prieigą prie tokių duomenų suteiktų tik nepriklausomi teismai, o priežiūros institucijos atliktų reguliarius auditus, vertintų visos sistemos veikimą, proporcingumo užtikrinimą ir teisinės gynybos prieinamumą asmenims, kurių duomenys yra tvarkomi. Galiausiai, autorės nuomone, siekiant veiksmingai įgyvendinti proporcingumo principą ES mastu, turėtų būti parengtos gairės, aiškiai apibrėžiančios saugotinų duomenų kategorijas, jų minimalios saugojimo trukmės ribas bei teisėtus prieigos kriterijus. Taip pat būtina harmonizuoti prieigos prie duomenų procedūras, pirmenybę teikiant teisminiam sankcionavimui, ir įtvirtinti reikalavimą reguliariai rengti nacionalinių praktikų atitikties ataskaitas. Tokiu būdu proporcingumo principas taptų ne tik abstrakčia teisės nuostata, bet ir praktiniu veiklos standartu, kuris užtikrintų, kad duomenų saugojimo sistemos ES būtų efektyvios, pagrįstos teisės viršenybės principais ir tinkamai suderintos su asmens teisių apsauga.

Ketvirta, duomenų saugojimo apimtis – tai ne vien techninis klausimas, bet kertinė praktinė problema, kai sprendžiama, kokių tipų elektroninių ryšių duomenys turi būti saugomi ir kokiu tikslu. Duomenų saugojimo direktyva aiškiai apibrėžė, kad privalomas saugojimas turi apimti tik metaduomenis (ryšio šaltinį, paskirties tašką, trukmę ir vietos nustatymo duomenis), o turinys – jokiu būdu (Valcke ir Kosta, 2006, p. 373). Tačiau po Direktyvos 2006/24/EB panaikinimo šių ribų neliko, o e. privatumo direktyvos 15 straipsnis tiesiog nurodo „nacionalinio saugumo, viešojo saugumo ar nusikalstamumo prevencijos“ tikslus be detalių apie konkrečias duomenų kategorijas. Tokiu būdu valstybės narės plačiai interpretuoja saugojimo apimtį – nuo griežtai metaduomenų saugojimo iki plačių naršymo žurnalų ar net interneto turinio registravimo (Valcke ir Kosta, 2006, p. 373).

Praktikoje pastebimas dvilypumas tarp duomenų saugojimo taikymo tyrimo ir prevencijos tikslams. Tyrimo atveju saugomi duomenys naudojami po nusikaltimo padarymo įrodymams rinkti arba siekiant nustatyti įtariamuosius konkrečiuose bylose. Šis modelis, nors ir ribotas, vis dėlto atitinka ESTT proporcingumo kriterijų, nes leidžia nukreipti priemones į konkrečius atvejus. Priešingai, prevencijos modelis – kur duomenys saugomi siekiant prognozuoti ir užkirsti kelią galimai nusikalstamai veiklai – dažnai virsta plačiu masinio stebėjimo įrankiu. Pavyzdžiui, kai kurios valstybės narės naudoja vietos nustatymo ir interneto naršymo duomenis ne tik siekdamos ištirti nusikaltimus, bet ir kurti profilį asmenims, kurių elgesys laikomas *„rizikingu“*, nors jiems nekyla tiesioginė įtarimų banga (Europos Parlamentas, 2014). Kaip jau buvo galima suprasti, nacionalinės praktikos pavyzdžiai atskleidžia, kokios rizikos kyla – Vokietijoje, nors metaduomenys saugomi trumpai, teisinė tvarka neapibrėžia aiškių kriterijų, kada jie gali būti naudojami prevencijai, o tai sudaro sąlygas platesniam prieigos taikymui. Prancūzijoje vienerių metų naršymo žurnalai ir skambučių metaduomenys dažnai pasitelkiami tiek tyrimams, tiek viešojo saugumo operacijoms, įskaitant profiliavimo sistemas, kurios veikia be aiškios teisinės kontrolės. Lietuvoje, nors įstatymas numato šešių mėnesių duomenų saugojimo terminą, *„sunkaus nusikaltimo“* ribos yra neaiškios, tad prevencinė motyvacija dažnai išplečia saugojimo taikymą į mažiau pavojingas veikas.

Teisinė ir socialinė kaina, susijusi su prevenciniu duomenų saugojimu, apima du esminius aspektus. Pirmiausia, tai sukuria vadinamąjį *„profilio efektą“*, kai individai, neturintys jokios kriminalinės istorijos, gali būti stebimi ir vertinami pagal automatizuotas rizikos klasifikacijas, o tai kelia grėsmę teisės į nekaltumo prezumpciją principui. Antra, masinis duomenų kaupimas didina duomenų nutekėjimo riziką bei galimybę, kad informacija bus panaudota neteisėtam sekimui ar diskriminacijai – ypač tada, kai prieigos kontrolė yra silpna arba jos visai nėra. Tokios praktikos kritiškai vertinamos ir Europos Sąjungos

teisėje. ESTT savo jurisprudencijoje yra aiškiai konstatavęs, kad prevencinis saugojimas, neturintis tiesioginio ir konkretaus ryšio su jau įvykdytu nusikaltimu, pažeidžia proporcingumo principą. Savo ruožtu EDAV pabrėžia, jog duomenų saugojimo mechanizmai gali būti taikomi tik tais atvejais, kai jie yra būtini konkrečiam tyrimui ar baudžiamajam persekiojimui, o prevencinis motyvas turi būti griežtai ribojamas. Remiantis šia doktrina, autorė siūlo, kad praktikoje būtų taikomi šie standartai: aiškiai apibrėžtas duomenų kategorijų sąrašas (pvz., tik metaduomenys be turinio), minimalus saugojimo laikotarpis (pvz., 30–90 dienų), ir prieigos leidimai, išduodami tik nepriklausomo teismo sprendimu.

Autorės nuomone, siekiant užtikrinti, kad duomenų saugojimo praktikos ES išliktų veiksmingos, tačiau kartu nepažeistų pagrindinių teisių, būtina įgyvendinti keturis pagrindinius principus: **ribotas saugomų duomenų kategorijų sąrašas** – leidžiama saugoti tik metaduomenis, tokius kaip ryšio šaltinis, paskirties taškas, trukmė ir vietos nustatymo duomenys, draudžiant saugoti ryšio turinį. **Minimalūs ir proporcingi saugojimo laikotarpiai** – siūloma nustatyti 30 dienų terminą vietos nustatymo duomenims ir 90 dienų – skambučių metaduomenims. Šie terminai grindžiami siekiu išlaikyti pusiausvyrą tarp operatyvinio teisėsaugos veiksmingumo pradiniuose tyrimo etapuose ir asmens teisės į privatumą apsaugos. Tokia trukmė atitinka proporcingumo principą, kuris įtvirtintas ESTT jurisprudencijoje, pabrėžiančioje, jog trumpesni, diferencijuoti ir tiksliniai saugojimo laikotarpiai geriau suderina saugumo ir privatumo interesus (Juszczak and Sason, 2021, p. 256). **Griežtai reglamentuota ir teisėta prieiga** – prieiga prie saugomų duomenų turėtų būti suteikiama tik pagal teismo sprendimą arba aiškiai apibrėžtą administracinę procedūrą, kuri būtų reguliariai prižiūrima nepriklausomos priežiūros institucijos. Tokia institucija taip pat turėtų atlikti leidimų auditą bei teikti periodines ataskaitas Europos duomenų apsaugos valdybai. **Reguliarus poveikio vertinimas** – turi būti atliekami tiek teisiniai, tiek technologiniai poveikio vertinimai, siekiant įvertinti duomenų saugojimo priemonių efektyvumą, proporcingumą ir jų atitiktį Chartijos nuostatoms. Toks reguliavimo modelis sumažintų esamą teisinį neapibrėžtumą, kuris lemia, kad valstybės narės plėtoja skirtingas duomenų saugojimo praktikas, taip skatindamos reglamentavimo fragmentaciją. Iš esmės **nacionalinių duomenų saugojimo praktikų ir teisinių reikalavimų** įvairovė komplikuoja tarptautinių paslaugų teikėjų veiklą, nes jie priversti prisitaikyti prie nevienodų teisinių reikalavimų skirtingose jurisdikcijose. Vieningi ES standartai ne tik užtikrintų didesnį teisinį aiškumą, bet ir padidintų teisėsaugos institucijų galimybes naudotis duomenimis teisėtų tikslų ribose. Galiausiai, veiksmingas ir nepriklausomas priežiūros mechanizmas galėtų tapti garantija, kad duomenų saugojimo

nuostatos nebus naudojamos kaip pagrindas pertekliniam sekimui ar nesuderinamoms prevencinėms stebėjimo programoms.

Taigi, ES institucijos turėtų neatidėliotinai inicijuoti ne tik naujos direktyvos, bet ir e. privatumo reglamento priėmimą arba esamo papildymo procesą. Atsižvelgiant į tai, kad e. privatumo reglamentas pagal SESV 288 straipsnį yra tiesiogiai taikomas visose valstybėse narėse ir nereikalauja perkelti jo nuostatų į nacionalinę teisę, toks sprendimas leistų užtikrinti vienodą taisyklių taikymą, sumažintų interpretacinius skirtumus ir eliminuotų nacionalinių nukrypimų riziką. Jeigu vis dėlto būtų pasirinktas direktyvos formatas, joje būtina įtvirtinti aiškius, detalius reikalavimus dėl saugomų duomenų kategorijų, laikymo terminų, prieigos sąlygų ir priežiūros mechanizmų. Autorės nuomone, taip būtų galima išvengti šiuo metu egzistuojančios praktikos įvairovės, kuri ne tik apsunkina tarptautinių paslaugų teikėjų veiklą, bet ir kelia grėsmę asmens teisių apsaugos vienodumui ES viduje. Taip pat tikslinga būtų numatyti pereinamąjį laikotarpį, per kurį valstybės narės galėtų suderinti savo teisės aktus su naujuoju ES teisės aktu. Tai padėtų išvengti teisinio neapibrėžtumo, užtikrintų sklandų perėjimą ir leistų išlaikyti pusiausvyrą tarp nacionalinių sistemų stabilumo ir poreikio harmonizuoti duomenų apsaugos standartus. Toks sisteminis požiūris leistų sukurti nuoseklią, proporcingą ir šiuolaikiniams iššūkiams atsparią ES lygmens duomenų saugojimo sistemą, paremtą teisės viršenybės ir pagrindinių teisių apsaugos principais (Juszczak and Sason, 2021, p. 256).

Išvados

1. Duomenų apsauga elektroninių ryšių sektoriuje yra esminė užtikrinant fundamentalių teisių apsaugą, ypatingai sparčios skaitmenizacijos kontekste. Elektroninių ryšių sektoriuje tvarkomi itin jautrūs asmens duomenys – komunikacijos turinio, srauto, lokalizacijos ir identifikavimo duomenys, kurių apsaugai ES taiko specializuotus reikalavimus, įtvirtintus e. privatumo direktyvoje, BDAR.
2. Direktyvos 2002/58/EB 15 straipsnio 1 dalis leidžia valstybėms narėms riboti elektroninių ryšių konfidencialumo teises tik griežtai laikantis teisėtumo, būtinumo ir proporcingumo principų kai tai būtina viešajam interesui – nacionaliniam saugumui, visuomenės saugumui ar nusikalstamumo prevencijai užtikrinti. Bendras ir nediferencijuotas duomenų saugojimas, neatsižvelgiant į konkretų pavojų, prieštarauja Chartijoje įtvirtintoms teisėms į privatumą ir duomenų apsaugą.
3. ESTT ir EŽTT jurisprudencija formuoja aiškius teisės į privatų gyvenimą ir asmens duomenų apsaugos standartus, ypač elektroninių ryšių srityje. Valstybių taikomos priemonės, ribojančios šias teises, turi būti aiškiai nustatytos teisės aktuose, turinčiuose įstatymo galią, taikomos tik būtinais atvejais ir prižiūrimos nepriklausomų teisminių institucijų.
4. Atlikta Vokietijos, Prancūzijos ir Lietuvos nacionalinių praktikų analizė parodė, kad elektroninių ryšių sektoriuje vis dar egzistuoja reguliacinė fragmentacija. Valstybės narės skirtingai interpretuoja e. privatumo direktyvos 15 straipsnį, ypač duomenų saugojimo trukmės, prieigos sąlygų ir *„sunkių nusikaltimų“* sąvokos atžvilgiu. Dėl šios priežasties duomenų subjektų teisės gali būti skirtingai apsaugotos priklausomai nuo valstybės, kurioje jie yra. Atsižvelgiant į tai, būtina užtikrinti teisinį aiškumą ir nuoseklumą ES lygmeniu – e. privatumo reglamentas galėtų tapti pagrindiniu instrumentu, kuris suvienodintų šias nuostatas ir sustiprintų asmens duomenų apsaugos standartų taikymą visose valstybėse narėse.

Šaltinių sąrašas

A. Teisės norminiai aktai

1. Visuotinė Žmogaus Teisių Deklaracija (1948). *Valstybės žinios*, 2006, 68-2497.
2. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1950). *Valstybės žinios*, 1995, 40-987.
3. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (1981). *Valstybės žinios*, 2001, 32-1059.
4. Jungtinių Tautų vaiko teisių konvencija (1989). *Valstybės žinios*, 1995, 60-1501.
5. Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB. *OL* 2004 m. specialusis leidimas, 13 sk., 15 t.
6. Europos Parlamento ir Tarybos 2002 m. kovo 7 d. direktyva 2002/21/EB. *OL* L 108, 2002, p. 33–50.
7. Europos Parlamento ir Tarybos 2002 m. liepos 12 d. direktyva 2002/58/EB. *OL* L 201, 2002, p. 37–47.
8. Europos Parlamento ir Tarybos 2006 m. kovo 15 d. direktyva 2006/24/EB. *OL* L 105, 2006, p. 54–63.
9. Europos Parlamento ir Tarybos 2015 m. lapkričio 25 d. reglamentas (ES) 2015/2120. *OL* L 310, 2015, p. 1–18.
10. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679. *OL* L 119, 2016, p. 1–88.
11. Europos Parlamento ir Tarybos 2018 m. gruodžio 11 d. direktyva (ES) 2018/1972. *OL* L 321, 2018, p. 36–214.
12. Lisabonos sutartis (2007 m. gruodžio 13 d.). *OL* C 202/02/390.
13. Sutartis dėl Europos Sąjungos veikimo (SESV). *OL* C 326, 2012, p. 47–390.
14. Europos Sąjungos pagrindinių teisių chartija (2016). *OL* C 202, 2016 6 7, p. 389–405.
15. Europos Komisija (2005). *Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl duomenų saugojimo*. COM(2005) 438 final.
16. Europos Komisija (2021). *Europos Komisijos 2021 m. Vaiko teisių strategija*. COM(2021) 142 final.
17. Europos Komisijos 2017 m. sausio 10 d. pasiūlymas dėl privatumo reglamento. COM(2017) 10 final, 2017/0003(COD).

18. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 1996, 63-1479.
19. Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*, 2004, 69-2382.
20. Lietuvos Respublikos visuomenės informavimo įstatymas. *Valstybės žinios*, 1996, 71-1706.
21. Lietuvos Respublikos baudžiamojo proceso kodeksas. 2000 m. rugsėjo 26 d. Nr. VIII-1968. *Valstybės žinios*, 2000, 89-2741.
22. Vokietijos Telekomunikacijų įstatymas (TKG). *BGBl.* I S. 1490, 2004 [interaktyvus]. https://rm.coe.int/16806af19e.
23. Prancūzijos Pašto ir elektroninių komunikacijų kodeksas (2014). *WIPO Lex* [interaktyvus]. https://www.wipo.int/wipolex/en/legislation/details/14290.

B. Specialioji literatūra

24. DE CEW, Judith (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca.
25. PARENT, William (1983). Recent work on the concept of privacy. *American Philosophical Quarterly*, 20.
26. PURTOVA, Nadezhda (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40–81.
27. PROSSER, William (1960). Privacy. *California Law Review*.
28. ŠTITILIS, Darius; KRIKŠČIŪNAS, Eugenijus ir PETRAUSKAS, Rimantas (2005). *Informacijos saugumo užtikrinimo teisiniai aspektai*. Vilnius: Mykolo Romerio universitetas.
29. VALCKE, Peggy ir KOSTA, Eleni (2006). Privacy and Data Protection in the EU: What Not to Forget. *Communications & Strategies*, 61(1), 103–120.
30. WALDEN, Ian; STEINBRECHER, Sandra and MARINKOVIC, Miroslava (2021). Telecommunications privacy in the age of surveillance. *International Journal of Law and Information Technology*, 29(2), 1717–1727.
31. WARREN, Samuel ir BRANDEIS, Louis D. (1890). The Right to Privacy. Harvard Law Review, IV(5).
32. WESTIN, Alan (1967). *Privacy and Freedom*. New York.

C. Teismų praktika

Europos Žmogaus Teisių Teismas

33. *Klass and others v. Germany* [EŽTT], Nr. 5029/71, [1978-09-06].
34. *Dudgeon v. United Kingdom* [EŽTT], Nr. 7525/76, [1983-02-24].
35. *X and Y v. Netherlands* [EŽTT], Nr. 8978/80, [1985-03-26].
36. *Malone v. United Kingdom* [EŽTT], Nr. 8691/79, [1984-08-02].
37. *Kruslin v. France* [EŽTT], Nr. 11801/85, [1990-04-24].
38. *Niemietz v. Germany* [EŽTT], Nr. 13710/88, [1992-05-29].
39. *Tanrıkulu v. Turkey* [EŽTT], Nr. 23763/94, [1999-07-08].
40. *Rotaru v. Romania* [EŽTT], Nr. 28341/95, [2000-05-04].
41. *Foxley v. United Kingdom* [EŽTT], Nr. 33274/96, [2000-09-20].
42. *Segerstedt-Wiberg and others v. Sweden* [EŽTT], Nr. 62332/00, [2006-09-06].
43. *Copland v. United Kingdom* [EŽTT], Nr. 62617/00, [2007-04-03].
44. *Zakharov v. Russia* [EŽTT], Nr. 47143/06, [2015-12-04].
45. *Szabó and Vissy v. Hungary* [EŽTT], Nr. 37138/14, [2016-01-12].

Europos Sąjungos Teisingumo Teismas

46. *Digital Rights Ireland* [CJEU], Nr. C-293/12 ir C-594/12, [2014-04-08]. ECLI:EU:C:2014:238.
47. *Tele2 Sverige* ir *Watson* [CJEU], Nr. C-203/15 ir C-698/15, [2016-12-21]. ECLI:EU:C:2016:970.
48. *Ministerio Fiscal* [CJEU], Nr. C-207/16, [2018-10-02]. ECLI:EU:C:2018:788.
49. *La Quadrature du Net* [CJEU], Nr. C-511/18, [2020-10-06]. ECLI:EU:C:2020:791.
50. *Prokuratuur* [CJEU], Nr. C-746/18, [2021-03-02]. ECLI:EU:C:2021:152.
51. *Privacy International* ir *Ligue des droits humains* [CJEU], Nr. C-793/19 ir C-794/19, [2022-09-20]. ECLI:EU:C:2022:601.
52. *G. D.* prieš *Commissioner of An Garda Síochána* ir kt. [CJEU], Nr. C-140/20, [2022-04-05]. ECLI:EU:C:2022:258.
53. *A. G.* prieš *Lietuvos Respublikos generalinę prokuratūrą* [CJEU], Nr. C-162/22, [2023-09-07]. ECLI:EU:C:2023:631.
54. *LD v. Poland* [CJEU], Nr. C-548/21, [2023-12-21]. ECLI:EU:C:2023:1011.

55. *Bezirkshauptmannschaft Landeck* [CJEU], Nr. C-548/21, [2024-10-04]. ECLI:EU:C:2023:89.

Lietuvos Respublikos Konstitucinis Teismas

56. Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas. *Valstybės žinios*, 2000, 39-1105.
57. Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas. *Valstybės žinios*, 2005, 1-7.

Vokietijos Federalinis Konstitucinis Teismas

58. Bundesverfassungsgericht 2010 m. sprendimas, 1 BvR 256/08.

D. Internetiniai šaltiniai

59. BEREC (2023). *Report on data retention practices in the EU* [interaktyvus]. https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-current-cybersecurity-challenges-and-dependencies-in-electronic-communication-networks.
60. Computer Law & Security Review (2020). Data protection, scientific research, and the role of information. Computer Law & Security Review, 37, 105412 [interaktyvus]. https://www.sciencedirect.com/science/article/pii/S0267364920300170.
61. Conseil d'État (2021). *Connection data: the Council of State conciliates the implementation of European Union law and the effectiveness of the fight against terrorism and crime* [interaktyvus]. https://www.conseil-etat.fr/en/news/connection-data-the-council-of-state-conciliates-the-implementation-of-european-union-law-and-the-effectiveness-of-the-fight-against-terrorism-and.
62. ENISA (2023). *Threat Landscape for Data Protection and Privacy* [interaktyvus]. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
63. Europos Audito Rūmai (2022). *5G diegimas Europos Sąjungoje: Specialioji ataskaita Nr. 03/2022* [interaktyvus]. https://www.eca.europa.eu/lt/publications?did=60614.

64. Europos duomenų apsaugos priežiūros pareigūnas (2015). Nuomonė Nr. 4/2015, rugsėjo 11 d. [interaktyvus]. Prieiga per internetą: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_lt.pdf.
65. Europos duomenų apsaugos valdyba (2019). *Gairės 2/2019 dėl asmens duomenų tvarkymo vaiko apsaugos kontekste* [interaktyvus]. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_lt.pdf.
66. Europos duomenų apsaugos valdyba (2019). *Nuomonė 5/2019 dėl e. privatumo direktyvos ir BDAR sąveikos* [interaktyvus]. https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_lt.pdf.
67. Europos duomenų apsaugos valdyba (2021). *Gairės 01/2021 dėl pranešimo apie asmens duomenų saugumo pažeidimus pavyzdžių* [interaktyvus]. https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_lt.pdf.
68. Europos Komisija (2023). *Komunikatas dėl asmens duomenų apsaugos reformos pažangos* [interaktyvus]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0901.
69. Europos Komisija (2023). *Pasiūlymas – Tarybos direktyva dėl sandorių kainodaros. COM(2023) 529 final* [interaktyvus]. https://data.consilium.europa.eu/doc/document/ST-12954-2023-INIT/lt/pdf.
70. Europos Sąjungos Taryba (2014). *Europos Sąjungos gairės dėl saviraiškos laisvės internete ir realiame gyvenime* [interaktyvus]. https://data.consilium.europa.eu/doc/document/ST-9647-2014-INIT/lt/pdf.
71. Europos Taryba (2003). *Memorandumas dėl duomenų saugojimo teisėtumo*.
72. eucrim (2022). *CJEU: German rules on data retention not in line with EU law* [interaktyvus]. https://eucrim.eu/news/cjeu-german-rules-on-data-retention-not-in-line-with-eu-law/.
73. ES 29 straipsnio darbo grupė (2001). *Nuomonė Nr. 10/2001 dėl duomenų apsaugos principų elektroninėje erdvėje* [interaktyvus]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp53_en.pdf.
74. ES 29 straipsnio darbo grupė (2005). *Nuomonė Nr. 4/2005 dėl asmens duomenų tvarkymo internetinėse paieškos sistemose* [interaktyvus].

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf.

75. ES 29 straipsnio darbo grupė (2006). *Nuomonė Nr. 3/2006 dėl IP adresų kaip asmens duomenų* [interaktyvus]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp119_en.pdf.
76. ES 29 straipsnio darbo grupė (2007). *Nuomonė Nr. 4/2007 dėl duomenų saugojimo direktyvos įgyvendinimo* [interaktyvus]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
77. ESTT (2018). *Informacijos suvestinė: duomenų apsauga ir elektroniniai ryšiai* [interaktyvus]. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_lt.pdf.
78. ESTT (2021). *Informacijos suvestinė: naujausia praktika dėl duomenų saugojimo*.
79. Human Rights Monitoring Institute (2017-09-12). *Lithuania continues mass collection of personal data under invalid EU directive* [interaktyvus]. https://www.liberties.eu/en/stories/lithuania-mass-data-retention/12859.
80. JILG, Melissa Laura Antonie (n.d.). *The Future of Data Retention in the EU — Possible Law Enforcement Measure or Disproportionate Illusion?* Master's thesis, Law, EULISP Double Degree Programme: Leibniz University Hannover and University of Oslo. [interaktyvus]. https://www.duo.uio.no/bitstream/handle/10852/98480/The_Future_of_Data_Retention_Master_Thesis.pdf?sequence=1&isAllowed=y.
81. JUSZCZAK, Adam and SASON, Elisa (2021). Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning? *eucrim*, 4, 238–266 [interaktyvus]. https://doi.org/10.30709/eucrim-2021-020.
82. Jones Day (2016). *The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws* [interaktyvus]. https://www.jonesday.com/en/insights/2016/08/the-data-retention-saga-continues-european-court-of-justice-and-eu-member-states-scrutinize-national-data-retention-laws.
83. Krašto apsaugos ministerija (2024). *Nacionalinė kibernetinio saugumo būklės ataskaita 2023* [interaktyvus]. https://kam.lt/leidiniai/nacionaline-kibernetinio-saugumo-bukles-ataskaita-kam-2024/.

84. PETRAITYTĖ, Agnė (2013). *Teisės viešumo principas vs asmens duomenų apsauga* [interaktyvus]. https://cris.mruni.eu/server/api/core/bitstreams/b0c9416a-c27a-40d2-b1c9-03730046d3fd/content.
85. Ryšių reguliavimo tarnyba (2022). *2021 metų veiklos ataskaita* [interaktyvus]. https://www.rrt.lt/d/2021-m-rrt-veiklos-metine-ataskaita-3/.
86. Tarptautinė telekomunikacijų sąjunga (2024). *Global Cybersecurity Index 2022* [interaktyvus]. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.
87. Valstybinė duomenų apsaugos inspekcija (2019). *Asmens duomenų apsaugos gairės duomenų subjektams* [interaktyvus]. https://vdai.lrv.lt/uploads/vdai/documents/files/01%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20DUOMENU%20SUBJEKTAMS%202019-10-16.pdf.
88. Valstybinė duomenų apsaugos inspekcija (2023). *2023 m. veiklos apžvalga* [interaktyvus]. https://vdai.lrv.lt/media/viesa/saugykla/2024/3/nLYMpcYmDDQ.pdf.
89. Valstybinė duomenų apsaugos inspekcija (2024). *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams, 4 versija, 2024-08-13* [interaktyvus]. https://vdai.lrv.lt/public/canonical/1725443426/586/VDAI_saugumo_priemoniu_gaires-2024-08-19.pdf.

Santrauka

Europos Sąjungos valstybių narių įgaliojimų apimtis užtikrinant asmens duomenų tvarkymą ir privataus gyvenimo apsaugą elektroninių ryšių sektoriuje

Greta Gužauskaitė

Magistro darbe analizuojama, kaip elektroninių ryšių sektoriuje tvarkomi asmens duomenys siejasi su asmens teise į privataus gyvenimo apsaugą. Tyrimo ašis – e. privatumo direktyvos 15 straipsnio 1 dalies taikymas valstybėse narėse ir jo sąveika su BDAR, ESTT bei EŽTT praktika. Pirmojoje darbo dalyje atskleidžiamas privatumo sampratos teisinis turinys pagal EŽTK 8 straipsnį, ES teisę ir nacionalinius šaltinius. Antrojoje dalyje analizuojama e. privatumo direktyvos ir BDAR sąveika, ypatingą dėmesį skiriant proporcingumo ir teisėtumo principų taikymui. Trečiojoje dalyje vertinami būsimo e. privatumo reglamento siūlomi pakeitimai, galintys reikšmingai paveikti esamą teisinį balansą tarp saugumo poreikių ir pagrindinių teisių apsaugos. Tyrimo rezultatai parodė, kad nacionaliniai teisės aktai ir praktika dažnai neatitinka ES bei EŽTT nustatytų standartų, o tai kelia riziką tiek teisių pažeidimams, tiek teisinio aiškumo trūkumui. Darbo išvadose pabrėžiamas aiškių teisinių kriterijų būtinumas ir vieningos ES praktikos svarba siekiant užtikrinti tinkamą asmens duomenų apsaugą elektroninių ryšių srityje.

Summary

The scope of the powers of European Union member states to ensure the protection of personal data and privacy in the electronic communications sector

Greta Gužauskaitė

The master's thesis explores how the processing of personal data in the electronic communications sector relates to the right to respect for private life. The core focus of the research is the application of Article 15(1) of the ePrivacy Directive in EU Member States and its interaction with the GDPR, as well as with the case law of the CJEU and the ECtHR. The first part of the thesis outlines the legal substance of the concept of privacy under Article 8 of the ECHR, EU law, and national legal sources. The second part analyses the interplay between the ePrivacy Directive and the GDPR, with particular emphasis on the principles of proportionality and legality. The third part evaluates the proposed amendments under the future ePrivacy Regulation, which may significantly impact the existing legal balance between security needs and the protection of fundamental rights. The findings of the study reveal that national legislation and practices often fail to meet the standards established by EU law and the ECtHR, posing risks both to individual rights and legal certainty. The conclusions underscore the necessity for clear legal criteria and a harmonised EU-wide approach to ensure adequate protection of personal data in the electronic communications sector.