

Vilniaus universiteto Teisės fakulteto

Viešosios teisės katedra

Justinos Novikevič

V kurso, Tarptautinės ir Europos Sąjungos

studijų šakos studentės

Magistro darbas

**ES BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TERITORINIS
TAIKYMAS: PROBLEMINIAI ASPEKTAI**

Vadovė: lekt. dr. Gintarė Surblytė-Namavičienė

Recenzentas: asist. dr. Julius Zaleskis

Vilnius

2020

TURINYS

PAGRINDINĖS SĄVOKOS IR SUTRUMPINIMAI.....	2
ĮVADAS	4
1. DUOMENŲ APSAUGOS TEISĖS RAIDA	8
1.1. Duomenų apsaugos teisė iki Bendrojo duomenų apsaugos reglamento įsigaliojimo.....	8
1.2. Duomenų apsaugos teisė po Bendrojo duomenų apsaugos reglamento įsigaliojimo.....	17
2. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO NORMOS DĖL TERITORINIO TAIKYMO: INTERPRETAVIMO IR ĮGYVENDINIMO PROBLEMOS	22
2.1. Bendrojo duomenų apsaugos reglamento normų interpretavimo problemos.....	22
2.1.1. Bendrojo duomenų apsaugos reglamento taikymas pagal buveinės kriterijų .	23
2.1.2. Bendrojo duomenų apsaugos reglamento taikymas pagal į ES duomenų subjektus nukreiptos veiklos kriterijų	26
2.1.3. Bendrojo duomenų apsaugos reglamento taikymas ES neįsisteigusiam duomenų valdytojui, veikiančiam pagal tarptautinę viešąją teisę.....	28
2.2. Bendrojo duomenų apsaugos reglamento įgyvendinimo problemos	30
3. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TERITORINIS TAIKYMAS INTERNETO KONTEKSTE.....	35
IŠVADOS	40
ŠALTINIŲ SĄRAŠAS	42
SANTRAUKA	48
SUMMARY	49

PAGRINDINĖS SĄVOKOS IR SUTRUMPINIMAI

Duomenų apsaugos direktyva arba **Direktyva** – 1990 m. Europos Parlamento ir Tarybos Direktyvą 95/46/EB (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

Bendrasis duomenų apsaugos reglamentas arba **Reglamentas** – (angl. *General Data Protection Regulation*) 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 ir kuriuo panaikinama Direktyva 95/46/EB.

Asmens duomenys arba **Duomenys** – informacija, susijusi su asmeniu (duomenų subjektu), kurio tapatybė gali būti nustatyta arba yra nustatyta.

Duomenų subjektas – fizinis asmuo, kurio asmeniniai duomenys yra renkami, laikomi ir tvarkomi.

Duomenų tvarkymas – bet kokia operacija, atliekama su asmens duomenimis, tiek automatizuotomis, tiek neautomatizuotomis priemonėmis, pavyzdžiui, duomenų rinkimas, keitimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, atskleidimas, naudojimas, ištrynimasis ir kt.

Duomenų valdytojas (angl. *data controller*) – asmuo (tiek fizinis, tiek juridinis), agentūra, valdžios institucija ar kita įstaiga, kuri nustato duomenų tvarkymo tikslus ir priemones

Duomenų tvarkytojas (angl. *data processor*) – asmuo (fizinis arba juridinis) agentūra, valdžios institucija ar kita įstaiga, kuri tvarko asmens duomenis duomenų valdytojo pavedimu.

Priežiūros institucija – nepriklausoma institucija, prižiūrinti duomenų tvarkymo procesus tam tikroje valstybėje, atliekanti konsultavimo funkcijas duomenų apsaugos klausimais bei sprendžianti ginčus dėl galimų nusižengimų duomenų apsaugos srityje.¹

Europos duomenų apsaugos valdyba (EDAV) (angl. *European data protection board*) - nepriklausoma Europos Sąjungos institucija, įsteigta Bendrojo duomenų apsaugos reglamentu bei padedanti užtikrinti nuoseklų duomenų apsaugos taisyklių taikymą visoje Europos Sąjungoje bei skatinti ES duomenų apsaugos institucijų bendradarbiavimą. EDAV

¹ Sąvokos pateiktos 1990 m. Europos Parlamento ir Tarybos Direktyvos 95/46/EB (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 4 straipsnyje.

sudaro nacionalinių duomenų apsaugos institucijų atstovai ir Europos duomenų apsaugos priežiūros pareigūnas (EDAPP).

Europos duomenų apsaugos valdybos (arba EDAV) Gairės dėl Reglamento teritorinio taikymo – 2019 m. lapkričio 12 d. išaiškinimo gairės Nr. 3/2018 dėl Bendrojo duomenų apsaugos reglamento teritorinio taikymo (3 straipsnio) (angl. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation*).

IVADAS

Nagrinėjamos temos aktualumas. Sparčiai besivystant informacinėms technologijoms ir spartėjant pasaulio globalizacijai, duomenų apsauga bei asmenų privatumas tampa vis aktualiau nagrinėjama tema. Dabartinis laikotarpis ypatingas tuo, kad didžiosios bendrovės, organizacijos, veikiančios skaitmeninėje erdvėje, gavo prieigą prie ypatingai didelio kiekio duomenų, o asmens duomenų perdavimas, kaupimas bei naudojimas vis dažniau vyksta ne tik tikslingai, tačiau ir kaip naudojimosi skaitmeninėmis paslaugomis šalutinis poveikis – tai kelia ypatingą pavojų asmens teisei į duomenų privatumą. Žinoma, kaip ir daugelis kitų teisinių sričių, duomenų apsaugos teisė kinta kartu su visuomenės pažanga, todėl, siekiant tinkamo su duomenų apsauga susijusių teisių bei pareigų įgyvendinimo, būtina nuolatos tobulinti jau sukurtus aktualius teisės aktus bei ieškoti naujų, inovatyvių ir galimai susidariusias teisės spragas panaikinančių sprendimų.

Nors duomenų apsaugos teisė pradėta nagrinėti dar XX a., o asmens duomenų apsauga Europos Sąjungos mastu pradėta reglamentuoti priėmus 1990 m. Europos Parlamento ir Tarybos Direktyvą 95/46/EB (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuria valstybės narės buvo įpareigos atitinkamai pakoreguoti nacionalinius teisės aktus perkeltiant į juos atitinkamas Direktyvos normas, visgi 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 ir kuriuo panaikinama Direktyva 95/46/EB, įsigaliojęs 2018 m. gegužės 25 d., sukėlė kone tikrą perversmą duomenų apsaugos teisės srityje, todėl pastaraisiais metais Reglamentas yra ypatingai aktualus ir atidžiai nagrinėjamas teisės aktas. Dar net neįsigaliojęs Bendrasis duomenų apsaugos reglamentas, kaip esminė duomenų apsaugos reforma, sukėlė nemenką sujudimą ne tik Europos Sąjungos valstybių narių nacionalinėje teisėje ir tarptautinėje teisėje, tačiau ir privačiame valstybių narių sektoriuje – įvairios bendrovės, kiti juridiniai asmenys suskubo atnaujinti savo privatumo politiką, informuoti klientus bei kitaip susijusius fizinius asmenis apie pastarųjų duomenų rinkimą, naudojimą bei apie kitus su asmens duomenimis susijusius procesus, taip pat atlikti asmens duomenų inventorizaciją, t. y. peržiūrėti, kokius duomenis įmonės jau tvarko, kaupia, įsitikinti, kad saugomi duomenys yra surinkti teisėtu būdu.

Ši tema aktuali būtent dėl Bendrojo duomenų apsaugos reglamento reikšmingumo duomenų apsaugos teisei ir aktualumo ne tik Europos Sąjungos valstybėms narėms, tačiau ir visam pasauliui. Šis darbas skirtas ne tik aptarti Reglamento teritorinio taikymo problemas, tačiau ir atkreipti dėmesį, kaip, didėjant globalizacijai, šis reiškinys persikelia

ir į teisinį reglamentavimą bei kokius pokyčius viso pasaulio duomenų apsaugos srityje nulėmė Bendrojo duomenų apsaugos reglamento priėmimas.

Darbo tikslas. Pagrindinis šio darbo tikslas yra atskleisti bei aptarti kylančias Bendrojo duomenų apsaugos reglamento teritorinio taikymo problemas bei išanalizuoti galimus Reglamento normų, susijusių su teritoriniu taikymu, trūkumus.

Darbo uždaviniai. Tam, kad būtų pasiektas aukščiau įvardintas tikslas, šiam darbui keliami tokie uždaviniai:

1. Glaustai apžvelgti duomenų apsaugos teisės raidą bei pagrindinius šaltinius. Paminėtina, kad, siekiant nenukrypti nuo magistrinio darbo temos, duomenų apsaugos teisės raida bei šaltiniai bus nagrinėjami per teritorinio taikymo prizmę – darbe siekiama pabrėžti, kuo ypatingas Bendrajame duomenų apsaugos reglamente įtvirtintas teritorinio taikymo modelis bei tokio taikymo naujumas, tuo pačiu apžvelgiant anksčiau ne ES institucijų priimtus teisės aktus duomenų apsaugos srityje, įtvirtinusių panašų teritorinio taikymo modelį.
2. Apžvelgti pagrindines Bendrojo duomenų apsaugos reglamento teritorinio taikymo taisykles – kokiems subjektams Reglamentas aktualus bei kokiais atvejais jis gali būti taikomas.
3. Atskleisti Bendrojo duomenų apsaugos reglamento nuostatų dėl teritorinio taikymo interpretavimą bei iš skirtingo interpretavimo kylančias problemas bei apžvelgti Europos Sąjungos institucijų taikomas priemones, skirtas Bendrojo duomenų apsaugos reglamento pritaikymo skirtingų valstybių narių nacionalinėje teisėje unifikavimui.
4. Aptarti Reglamento teritorinio taikymo aspektus interneto kontekste.
5. Aptarti esmines Reglamento normų dėl teritorinio taikymo įgyvendinimo problemas.

Darbo objektas. Tam, kad būtų tinkamai įgyvendinti šio darbo uždaviniai bei pasiekti tikslai, pagrindinis tyrimo objektas yra Bendrojo duomenų apsaugos reglamento teritorinis taikymas bei su juo susijusios iš pačios teisės normos bei praktinio jos įgyvendinimo kylančios problemos bei iššūkiai. Taip pat darbe bus kreipiamas dėmesys į tai, kuo ypatingas Reglamente įtvirtintas teritorinio taikymo modelis bei, siekiant apžvelgti šį išskirtinumą, bus apžvelgiama, kaip buvo reglamentuojamas asmens duomenų judėjimas

tarp Europos Sąjungos valstybių narių bei trečiųjų šalių ir ar apskritai toks reguliavimas egzistavo iki įsigaliojant Bendrajam duomenų apsaugos reglamentui.

Darbo tyrimo metodai. Tam, kad būtų tinkamai ir visapusiškai išnagrinėti anksčiau įvardinti pagrindiniai darbo objektai bei aptariamos problemos, jų analizei taikomi šie tyrimo metodai:

1. Istorinis. Šis metodas taikytas siekiant apžvelgti asmens duomenų apsaugos teisės raidą teritoriniu aspektu, t. y. išanalizuoti, kaip keitėsi asmens duomenų judėjimo tarp Europos Sąjungos valstybių narių bei kitų valstybių reglamentavimas.
2. Sisteminis. Sisteminis analizės metodas svarbus siekiant išaiškinti Bendrojo duomenų apsaugos reglamento reikšmę visoje teisės sistemoje – ne tik Europos Sąjungos, tačiau ir pasauliniu mastu.
3. Lyginamasis. Šis metodas naudojamas skirtingų Europos Sąjungos teisės aktų, skirtų asmens duomenų apsaugos reguliavimui, palyginti. Taip pat darbe, taikant minėtąjį metodą, atliekamas ir Bendrojo duomenų apsaugos reglamento palyginimas su keliais ne Europos Sąjungos narių priimtais aktualiais ir su asmens duomenų apsauga susijusiais teisės aktais.
4. Loginis. Šis metodas pasitelkiamas argumentuojant pateiktus teiginius bei nagrinėjant aktualias problemas, jų sprendimo būdus bei aiškinant atitinkamas teisės normas.
5. Teleologinis. Teleologinis metodas padeda išaiškinti ir suprasti nagrinėjamų normų turinį.

Darbo originalumas. Pastebėtina, kad asmens duomenų apsauga yra aktuali ir ypatingai aktyviai nagrinėjama tema. Su Bendrojo duomenų apsaugos reglamento priėmimu atsirado ir poreikis šį reglamentą išnagrinėti kuo nuodugniau, todėl ir rašto darbų bei kitų tiriamųjų darbų, susijusių su Bendrojo duomenų apsaugos reglamentu, yra daug, tačiau verta paminėti, kad dauguma jų yra bendresnio pobūdžio, nagrinėjantys platesnes Reglamento dalis ar net visą Bendrąjį duomenų apsaugos reglamentą ir jo reikšmę asmens duomenų apsaugai bei teisės į privatumą įgyvendinimui. Kita vertus, peržvelgus elaba.lvb.lt duomenis, pastebėtina, kad tarp siauresnio pobūdžio mokslinių tiriamųjų darbų, analizuojančių konkrečius Reglamento aspektus, nėra darbų, skirtų aptarti iš Bendrojo duomenų apsaugos reglamento teritorinio taikymo kylančias problemas. Paminėtini Juliaus Zaleskio straipsniai, kuriuose aptariamos Bendrojo duomenų apsaugos reglamento naujovės, tarp jų ir ekstrateritorialus Reglamento poveikis, bei šio privalomojo pobūdžio

teisės akto reikšmė duomenų apsaugos teisei². Tuo tarpu užsienio literatūroje galime rasti daugiau darbų, skirtų aptarti teritorinio Reglamento taikymo aspektus: šio taikymo problematiką aptaria tokie autoriai kaip Graham Greenleaf, Jan Philipp Albrech, Giovanni Buttarelli, Christopher Kuner ir kt.

Svarbiausi šaltiniai. Svarbiausias šaltinis, kuriuo remiantis atliekamas pasirinktų darbo objektų tyrimas, yra Bendrasis duomenų apsaugos reglamentas. Tam, kad būtų pasirinkta tema būtų išnagrinėta kuo visapusiškiau, taip pat nagrinėti ir kiti su duomenų apsauga susiję teisės šaltiniai, kaip antai 1990 m. Europos Parlamento ir Tarybos Direktyva 95/46/EB (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108) ir kt. Darbo objekto nagrinėjimui labai svarbios ir Europos duomenų apsaugos valdybos (EDAV) pateiktos išaiškinimo gairės Nr. 3/2018 dėl Bendrojo duomenų apsaugos reglamento teritorinio taikymo ribų, taip pat ES 29 str. darbo grupės pateiktos oficialios nuomonės duomenų apsaugos teisės klausimais. Darbe taip pat nagrinėjami *International Data Privacy Law* leidiniuose paskelbti įvairių autorių moksliniai darbai.

² ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, t. 103, p. 45-54.

1. DUOMENŲ APSAUGOS TEISĖS RAIDA

Siekiant kuo geriau suprasti, kuo Bendrasis duomenų apsaugos reglamentas yra inovatyvus ir kokios naujovės asmens duomenų apsaugos srityje atsirado kartu su Reglamento priėmimu, svarbu palyginti, kaip fizinių asmenų teisė į duomenų privatumą buvo įgyvendinama iki Reglamento įsigaliojimo ir po to, kai Bendrasis duomenų apsaugos reglamentas įgijo teisinę galią. Todėl pirmoje šio skyriaus dalyje bus apžvelgiama, kokie teisės aktai reglamentavo asmens duomenų apsaugą iki Reglamento priėmimo, tuo tarpu antroje dalyje bus apžvelgiami esminiai duomenų apsaugos teisės pasikeitimai, įtvirtinti Bendrajame duomenų apsaugos reglamente, bei Direktyvos ir Reglamento pagrindiniai skirtumai. Siekiant neperžengti apibrėžtų darbo temos nagrinėjimo ribų, minėtųjų skirtumų analizė bei raidos apžvalga bus atliekama teritorinio taikymo atžvilgiu.

1.1. Duomenų apsaugos teisė iki Bendrojo duomenų apsaugos reglamento įsigaliojimo

Poreikis užtikrinti asmenų teisę į asmens duomenų apsaugą atsirado visuomenei vis daugiau dėmesio skiriant privatumo svarbai. Civilizacijai progresuojant, didėja ir teisės į privatumą reikšmingumas³, kartu skatinantis visuomenės narius atidžiau saugoti asmens duomenis. Nors skirtingų valstybių nacionalinėje teisėje privatumo doktrina formavosi palaipsniui ir skirtingais būdais (vienos valstybės šios teisės įgyvendinimą užtikrino įstatymų leidybos būdu, kitos – teismų precedentais, o kai kuriose valstybėse – ir teisės doktrinos inspiruota teismų praktika⁴) jau nuo XIX a. pabaigos⁵, tačiau tarptautiniu mastu privatumo koncepcija įtvirtinta tik 1948 m. Jungtinių Tautų generalinės asamblėjos priimtoje Visuotinėje žmogaus teisių deklaracijoje, kurioje teigiama, kad „Niekas neturi

³ ŽIOBIENĖ, Edita. Informacijos apie privatų asmens gyvenimą apsauga. *Konstitucinė jurisprudencija*. 2008, Nr. 3 (11). p. 140.

⁴ *Ibid.*, p. 142.

⁵ Laikoma, kad privatumo koncepcija pradžia įgavo Jungtinėse Amerikos Valstijose, kai dėl perdėto žurnalistų dėmesio 1883 m. sausio 25 d. vykusioms Samuel Warren ir Mabel Bayard (Jungtinių Amerikos Valstijų senatoriaus ir buvusio kandidato į prezidentus Thomas Francis Bayard dukros) vestuvėms ir dėl pavišintų vestuvių detalių, S. Warren kartu su advokatu Louis Dembitz Brandeis 1890 m. paskelbė straipsnį, kuriame išdėstė, kad teisė į privatumą turi būti suvokiama kaip teisė būti paliktam ramybėje bei kad kiekvienas asmuo turi būti apsaugotas nuo jo asmeninio gyvenimo detalių paviešinimo, kai to asmens sutikimas nebuvo gautas. Plačiau žr. GAJDA, Amy. *What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to „The Right to Privacy“* [interaktyvus; žiūrėta 2020 m. kovo 6 d.]. Prieiga per internetą: <<http://educationnewyork.com/files/SSRN-id1026680privacyorigin.pdf>>.

patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsಿನimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsಿನimosi“⁶. Šiame rekomendacinio pobūdžio dokumente įtvirtintą asmens teisę į privatumą vėliau papildė 1950 m. Europos Tarybos priimta Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (toliau – EŽTK). Be minėtų Visuotinėje žmogaus teisių deklaracijoje įtvirtintų nuostatų, kuriomis draudžiama kištis į privatų asmens gyvenimą, EŽTK 8 straipsnis, kaip aiškina Europos Žmogaus Teisių Teismas, papildomai nustato pareigą valstybėms imtis priemonių, kuriomis būtų užtikrinama, kad į asmenų privatų gyvenimą nesikiš ir kiti asmenys⁷. Vadinasi, be pasyvios pareigos nesikišti, valstybėms numatoma ir aktyvioji pareiga apsaugoti asmenų teisę į privatumą.

XX a. antroje pusėje vis daugiau Europos valstybių nacionaliniais teisės aktais įtvirtina normas, reglamentuojančias informacijos, susijusios su asmeniu, apsaugą. Be to, nuo 1973 m. iki pat 2016 m. 120 valstybių (vidutiniškai 2,7 naujos valstybės per vienerius metus) visame pasaulyje priėmė naujus teisės aktus, skirtus užtikrinti asmens duomenų apsaugą⁸. Lietuvoje duomenų apsaugos teisė taip pat formavosi palaipsniui – 1992 m. priimtos Lietuvos Respublikos Konstitucijos 22 straipsnyje įtvirtintas asmens privataus gyvenimo neliečiamumas tapo pirmuoju žingsniu siekiant įtvirtinti asmens teisę ir į jo duomenų neliečiamumą bei apsaugą⁹. 1996 m. Lietuvoje priimtas pirmasis su duomenų apsauga susijęs teisės aktas – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, kuris vėliau, Lietuvai stojant į Europos Sąjungą, pakoreguotas tam, kad atitiktų Duomenų apsaugos direktyvoje numatytus asmens duomenų apsaugos standartus.

Visos Europos, kaip vieningos sistemos, mastu taip pat daugėjo iniciatyvos asmens duomenų apsaugos srityje – Europos Taryba 1968 m. paskelbė 509 Rekomendaciją dėl žmogaus teisių ir šiuolaikinių bei mokslinių technologinių pokyčių¹⁰. Taip pat, remdamasi EŽTK 8 straipsniu, Europos Taryba priėmė įvairias rezoliucijas dėl asmens duomenų apsaugos, kaip antai 1973 m. Rezoliuciją Nr. 73/22 dėl asmenų privatumo apsaugos

⁶ 1948 m. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*, 2006, Nr. 68-2497.

⁷ Europos Žmogaus Teisių Teismas. 2008 m. gruodžio 2 d. sprendimas *K. U. prieš Suomiją* byloje, Nr. 2872/02.

⁸ GREENLEAF, Graham. Countries with Data Privacy Laws – By Year 1973-2016 (Tables), 2017 [interaktyvus; žiūrėta 2020 m. vasario 28 d.]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2996139>.

⁹ Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, Nr. 33-1014.

¹⁰ Europos Taryba. 509 Rekomendacija dėl žmogaus teisių ir šiuolaikinių bei mokslinių technologinių Pokyčių (angl. *Recommendation 509 (1968). Human rights and modern scientific and technological Developments*), 1968 [interaktyvus; žiūrėta 2020 m. vasario 27 d.]. Prieiga per internetą: <[9](http://semanticpace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbmQvbnNveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNDU0NiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdcQ9ZGYvWFJlZi1XRc1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTEONTQ2>>.</p></div><div data-bbox=)

elektroninių duomenų bankų privačiame sektoriuje atžvilgiu ir 1974 m. Rezoliuciją Nr. 74/29 dėl asmenų privatumo apsaugos elektroninių duomenų bankų viešajame sektoriuje atžvilgiu¹¹.

Kita vertus, minėtose rezoliucijose įtvirtintos taisyklės buvo orientuotos į Europos valstybes ir duomenų apsaugos teisės vienodinimą jose, ir tik 1980 m. Ekonominio bendradarbiavimo ir plėtros organizacijos paskelbtos Privatumo gairės tapo pirmuoju jau pasaulinę reikšmę turinčiu duomenų apsaugos šaltiniu. Šio rekomendacinio pobūdžio akto tikslas – įtvirtinti ir tarptautiniu lygiu susisteminti pagrindinius duomenų apsaugos principus. Būtent į Privatumo gairėse įtvirtintus principus Ekonominio bendradarbiavimo ir plėtros organizacija rekomendavo atsižvelgti valstybėms kuriant nacionalinę teisę¹². Tuo tarpu 1981 m. Europos Tarybos priimta Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Konvencija Nr. 108), kurios pagrindinis tikslas yra užtikrinti, kad visų šalių teritorijose būtų gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia – jo teisė į privatų gyvenimą, kai asmens duomenys tvarkomi automatizuotai, tapo pirmąja, pagrindine ir iki šiol galiojančia tarptautine teisine galia turinčia asmens duomenų apsaugos priemone¹³, privaloma vykdyti visoms Konvenciją Nr. 108 pasirašiusioms šalims. Šios daugiašalės sutarties atsiradimą taip pat lėmė siekis suvienodinti duomenų apsaugos įstatymus visoje Europoje. Konvencija Nr. 108, be kita ko, įtvirtinta pareiga užtikrinti, kad būtų imtasi tinkamų apsaugos priemonių duomenų saugumui užtikrinti (7 str.), asmenų teisė gauti informaciją apie savo duomenų rinkimą bei tokio rinkimo tikslus (8 str. a punktas), taip pat teisė reikalauti, kad tie duomenys būtų ištrinti (8 str. c punktas), pareiga valstybėms nustatyti tinkamas priemones konvencijos Nr. 108 įgyvendinimui (13 str.). 2001 m. lapkričio 8 d paskelbtas papildomas Konvencijos Nr. 108 protokolai, kuriuo įtvirtintos trečiosioms valstybėms (konvencijos nepasirašiusioms šalims) taikytinos nuostatos dėl valstybės sienas kertančių duomenų srautų ir dėl privalomo nacionalinių duomenų apsaugos priežiūros institucijų įkūrimo¹⁴. Šiuo papildomu protokolu taip pat nustatyta, kad tais atvejais, kai duomenis norima perduoti Konvencijos Nr. 108

¹¹ Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*, 2014, p. 16 [interaktyvus; žiūrėta 2020 m. kovo 1 d.]. Prieiga per internetą: <http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0020.03/DOC_2>.

¹² ZALESKIS, Julius. *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*. Vilnius: Registrų centras, 2019, p. 45.

¹³ Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*, 2014, p. 16 [interaktyvus; žiūrėta 2020 m. kovo 1 d.]. Prieiga per internetą: <http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0020.03/DOC_2>.

¹⁴ *Ibid.*, p. 17.

nepasirašiusiems valstybėms ar organizacijoms, šios turi užtikrinti, kad asmens duomenų perdavimas bus tinkamai apsaugotas¹⁵. Atkreipiamas dėmesys, kad Konvenciją Nr. 108 gali pasirašyti ir ne Europos Sąjungos valstybės (Konvenciją Nr. 108 jau yra ratifikavusios tokios šalys kaip Urugvajus¹⁶, Argentina¹⁷, Meksika¹⁸, Mauricijus¹⁹ ir kt.), todėl galima teigti, kad šis aktas tapo bene efektyviausia priemone, reguliuojančia asmens duomenų judėjimą (bei tokių duomenų apsaugą) tarp tiek Europos Sąjungai priklausančių, tiek nepriklausančių šalių. Verta paminėti, kad dėl technologijų, o kartu ir priemonių, kuriomis renkami ar kuriose kaupiami fizinių asmenų duomenys, pažangos, 2018 m. spalio 10 d. Europos Taryba paskelbė dar vieną Konvenciją Nr. 108 papildantį protokolą. Juo dar kartą iš dalies pakeičiama 1981 m. priimta Konvencija dėl Asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, tačiau papildomų žymių reikalavimų nesukuriama. Plačiau apie Konvencijos Nr. 108 pakeitimus naujuoju protokolu ir sąsajas su Bendroju duomenų apsaugos reglamentu bus kalbama kitoje šio darbo dalyje.

Europos Sąjunga, siekdama vis geresnio duomenų apsaugos reglamentavimo, neapsiribojo tik anksčiau minėtų įvairaus pobūdžio teisės aktų bei rekomendacijų paskelbimu ir iki Bendrojo duomenų apsaugos reglamento priėmė ir žemiau nurodytus su asmens duomenų teise sietinus aktus:

1. Europos Tarybos Ministrų Komiteto 1983 m. rugsėjo 23 d. rekomendaciją Nr. R (83) 10 dėl asmens duomenų, naudojamų moksliniams tyrimams ir statistikai, apsaugos.
2. Europos Tarybos Ministrų Komiteto 1991 m. rugsėjo 9 d. rekomendaciją Nr. (91) 10 dėl viešosios valdžios institucijų turimų asmens duomenų perdavimo tretiesiems asmenims.

¹⁵ 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Valstybės žinios, 2001, Nr. 32-1059.

¹⁶ Council of Europe. *Personal data protection: Uruguay becomes first non-European state to accede to "Convention 108"*. 2013 [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <<https://www.coe.int/en/web/portal/-/personal-data-protection-uruguay-becomes-first-non-european-state-to-accede-to-convention-108->>.

¹⁷ Council of Europe. Newsroom: *Argentina, 54th Party to Convention 108*. 2019 [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <<https://www.coe.int/en/web/data-protection/-/argentina-54th-party-to-convention-108->>.

¹⁸ Council of Europe. Newsroom: *Welcome to Mexico, 53rd Party to Convention 108*. 2018 [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <<https://www.coe.int/en/web/data-protection/-/welcome-to-mexico-53rd-party-to-convention-108->>.

¹⁹ Council of Europe. News 2016: *International data protection conference: Mauritius joins "Convention 108"*. 2016 [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <https://www.coe.int/en/web/portal/news-2016/-/asset_publisher/StEVOsr24HJ2/content/mauritius-joins-the-data-protection-convention-convention-108->.

3. 1995m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva). Vėliau papildyta 2008 m. lapkričio 27 d. Tarybos pamatiniu sprendimu 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos.
4. 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos Reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas).
5. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) su pakeitimais, padarytais Direktyva 2006/24/EB ir Direktyva 2009/136/EB.
6. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

Iki pat Bendrojo duomenų apsaugos reglamento įsigaliojimo, 1995 m. paskelbta Duomenų apsaugos direktyva buvo pirmoji ir pagrindinė Europos Sąjungoje galiojanti teisinė priemonė, reglamentuojanti asmens duomenų apsaugą, įpareigojanti Europos Sąjungos valstybes nares perkelti Direktyvoje nurodytas nuostatas į jų nacionalinę teisę. Duomenų apsaugos direktyva priimta siekiant dviejų pagrindinių tikslų: apsaugoti pagrindinę teisę į duomenų apsaugą ir užtikrinti laisvą asmens duomenų judėjimą tarp valstybių narių²⁰. Direktyva siekiama apsaugoti Europos Sąjungos piliečių asmens duomenis ne tik juos tvarkant Europos Sąjungos šalių įmonėms, tačiau ir kitų, ne Europos Sąjungos, valstybių organizacijoms, turinčioms fizinę buveinę ar fizinę duomenų valdymo įrangą Europos Sąjungoje. Taikymo sritis plačiau išaiškinama Duomenų apsaugos direktyvos 4 straipsnio 1 dalyje, kurioje nurodoma, kad valstybė narė taiko nacionalinės teisės normas, kurios priimtos vadovaujantis Direktyva, tais atvejais, kai:

²⁰ 2012 m. sausio 25 d. Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52012PC0011>>.

1. duomenų valdytojo²¹ padalinys veikia ES valstybės narės teritorijoje;
2. duomenų valdytojas nėra įsikūręs valstybės narės teritorijoje, tačiau yra įsikūręs ten, kur pagal viešosios teisės taisyklės yra taikoma tos valstybės narės nacionalinė teisė;
3. duomenų valdytojas įsisteigęs ne Europos Sąjungos valstybės narės teritorijoje, tačiau, tvarkydamas asmens duomenis, naudojami automatinė ar kitokia įranga, esančia minėtos valstybės narės teritorijoje, nebent tokia įranga būtų naudojama tiksliai duomenis tranzitu persiunčiant per Bendrijos teritoriją²².

Atsižvelgiant į paminėtas Duomenų apsaugos direktyvos 4 straipsnio 1 dalies nuostatas, matyti, kad Direktyvos ir nacionalinių ją įgyvendinančių teisės aktų teritorinio taikymo sritį lemia arba duomenų valdytojo padalinio įsteigimo vieta, arba, jeigu duomenų valdytojas yra įsteigtas ne Europos Sąjungoje, naudojamų priemonių ar įrangos buvimo vieta²³, kitaip tariant, pagal Direktyvą ES duomenų apsauga reglamentuojama atsižvelgiant į duomenų valdytojo įsisteigimo vietos kriterijų, tačiau net ir tokiu atveju, kai fizinės buveinės ar įrangos kriterijus išpildomas, svarbu ir tai, ar jo veikla susijusi su duomenų tvarkymu bei naudojimu. Atsižvelgiant į tokį reguliavimą, galima daryti išvadą, jog su technologijų pažanga atsiradus galimybei rinkti bei valdyti duomenis per atstumą, šios Direktyvos nuostatos tapo lengvai „apeinamos“. Kita vertus, šį reguliavimą iš esmės pakeitė Europos Sąjungos teismų praktika. Europos Sąjungos Teisingumo Teismas (toliau – Europos Sąjungos Teisingumo Teismas arba ESTT) 2014 m. gegužės 13 d. sprendime byloje *Google* prieš M. C. González (toliau – *Google Spain* byla)²⁴ be teisės būti pamirštam, teisės būti informuotam, bei kitų duomenų apsaugos teisei svarbių principų taip pat aptarė ir pagrindinius duomenų apsaugos aspektus Direktyvos 4 straipsnio 1 dalies atžvilgiu (išaiškinama teritorinio taikymo sritis, padalinio valstybės narės teritorijoje sąvoka). Duomenų apsaugos direktyvoje įtvirtinta taisyklė, teigianti, kad kiekviena valstybė narė

²¹ Šiame kontekste sąvoka „Duomenų valdytojas“ reiškia tokį fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus; jeigu tvarkymo tikslus ir būdus nusako nacionaliniai arba Bendrijos įstatymai bei norminiai aktai, tai duomenų valdytoją arba specifinius kriterijus, pagal kuriuos skiriamas duomenų valdytojas, gali apibrėžti nacionaliniai arba Bendrijos įstatymai. Sąvoka pateikta 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 355–374.

²² 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 355–374.

²³ ES 29 str. darbo grupė. *Nuomonė Nr. 8/2010 dėl taikytinos teisės* (WP 179) 2010 [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf>

²⁴ Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* byloje, C-131/12, ECLI:EU:C:2014:317.

taiko nacionalinės teisės nuostatas (įtvirtintas pagal Direktyvą) kai tvarkomi asmens duomenys, jeigu „tvarkoma, duomenų valdytojo padaliniui veikiant valstybės narės teritorijoje“ Europos Sąjungos Teisingumo Teismo išaiškinta plečiamai – ESTT patvirtina plačią teritorinę Duomenų apsaugos direktyvos 4 straipsnio 1 dalies a punkto taikymo sritį. *Google Spain* byloje Europos Sąjungos Teisingumo Teismas nustatė, kad paieškos variklį, naudojamą asmens duomenų tvarkymui, eksploatuoja *Google Inc.* - Jungtinėse Amerikos Valstijose įsisteigęs duomenų valdytojas. ESTT aiškina, kad *Google Inc.* buvo neatsiejamai susijęs su *Google* padalinio Ispanijoje veikla, kadangi šio Ispanijos padalinio reklaminė ir komercinė veikla reiškė „priemonę, kuria siekiama padaryti paieškos variklį ekonomiškai pelningą“²⁵. Remiantis šiomis aplinkybėmis, ESTT padarė išvadą, jog nagrinėjamu atveju duomenų tvarkymo veiklai, vykdomai *Google Inc.*, turi būti taikoma Ispanijos teisė. Vis dėlto, šio sprendimo padarinių mastas, kaip teigia ES 29 str. darbo grupė, yra platesnis ir nėra susijęs tik su *Google* paieškos variklio Ispanijoje eksploatavimui taikytinos teisės nustatymu, todėl 2015 m. gruodžio 16 d. ES 29 str. darbo grupė atnaujino 2010 m. priimtą Nuomonę Nr. 8/2010 dėl taikytinos teisės ir paskelbė naują rekomendacinį dokumentą - Atnaujintą nuomonę Nr. 8/2010 dėl taikytinos teisės, atsižvelgiant į ESTT sprendimą byloje *Google Spain*, kurioje apžvelgė tai, kaip ESTT išaiškino ES padalinio veiklos ir ne ES duomenų tvarkytojo duomenų tvarkymo veiklos „neatsiejamą ryšį“ bei Direktyvos 4 straipsnio 1 dalies a punkte įtvirtintą padalinio sąvoką²⁶.

Direktyva taip pat nurodo ir taisykles, taikomas asmens duomenų judėjimui tarp Europos Sąjungos valstybių narių ir trečiųjų šalių – šio duomenų judėjimo reglamentavimui skirti 25 bei 26 Direktyvos straipsniai. Duomenų apsaugos direktyvos 25 str. numatyta, kad tam, jog būtų leidžiamas asmens duomenų judėjimas tarp ES valstybės narės ir trečiosios valstybės, pastaroji turi užtikrinti adekvatų apsaugos lygį, kuris vertinamas atsižvelgiant į duomenų perdavimo operacijos ar operacijų grupės aplinkybes, duomenų pobūdį, tvarkymo operacijos tikslą ir trukmę, duomenų kilmės bei paskirties valstybę ir kt.²⁷ Nustačius, kad trečioji šalis neužtikrina adekvataus apsaugos lygio, asmens duomenys šiai trečiajai valstybei negali būti perduoti²⁸. Tuo tarpu Direktyvos 25 str. 6 dalyje numatyta sąlyga, palengvinanti duomenų judėjimo tarp ES valstybės narės ir trečiosios šalies reglamentavimą – nurodoma, kad Komisija gali nustatyti, jog trečioji šalis adekvatų

²⁵ ES 29 str. darbo grupė. *Atnaujinta nuomonė Nr. 8/2010 dėl taikytinos teisės, atsižvelgiant į ESTT sprendimą byloje Google Spain*, 2015 [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640614>

²⁶ *Ibid.*

²⁷ 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas.

²⁸ *Ibid.*

apsaugos lygį užtikrina savo šalies įstatymais ar tam tikrais tarptautiniais įsipareigojimais, kuriuos ji yra priėmusi. Vadinasi, Europos Komisijai nustačius minėtas aplinkybes (ir išaiškinus jas Direktyvos 31 str. 2 dalyje numatyta tvarka²⁹), trečioji šalis neturi papildomai įrodinėti priemonių, užtikrinančių adekvatų apsaugos lygį. Pavyzdžiui, 2001 m. gruodžio 20 d. sprendimu Europos Komisija nustatė, kad, taikant Direktyvos 25 str. 2 dalį, Kanada laikoma užtikrinančia tinkamą gavėjams Europos Sąjungos valstybių perduodamų asmens duomenų apsaugos lygį pagal Kanados Asmens duomenų apsaugos ir elektroninių dokumentų įstatymą³⁰. Toks sprendimas užtikrina, kad asmens duomenys iš valstybių narių šiai trečiajai šaliai gali būti perduodami nereikalaujant jokių papildomų garantijų.

Visgi, galima teigti, kad nors tam tikros Duomenų apsaugos direktyvos nuostatos nustatė tam tikras taisykles ir ribojimus, taikomus teritoriniu aspektu, kaip antai Direktyvos 4 str. numatyta taikymo apimtį bei 25 str. ir 26 str. nustatytas duomenų judėjimo tarp ES valstybių narių ir trečiųjų šalių taisykles, visgi, šios nuostatos nebuvo tiesiogiai taikomos trečiosioms valstybėms ir teisinių pasekmių automatiškai joms nekėlė.

Dar vienas tarptautinę reikšmę turintis teisės šaltinis - 1990 m. Jungtinių Tautų Generalinės asamblėjos paskelbtos Gairės dėl kompiuterizuotų asmens duomenų bylų reguliavimo. Taip Jungtinių Tautų generalinė asamblėja prisidėjo prie Europos Sąjungos išreikštos iniciatyvos vienodinti įvairių valstybių požiūrį į asmens duomenis bei jų apsaugos teisę³¹.

Viena iš tarptautinių sutarčių, veikiančių duomenų apsaugos teisės srityje, yra 2016 m. liepos 12 d. Europos Komisijos priimtas tarp JAV ir Europos Sąjungos pasirašytas susitarimas „Privatumo skydas“. Pasirašyti šį susitarimą paskatino ES ir JAV siejantys glaudūs transatlantiniai santykiai, kuriuos labiausiai lemia tarp Jungtinių Amerikos Valstijų ir Europos Sąjungos valstybių narių susiformavę tvirti ekonominiai ryšiai bei svarbi šių ryšių dalis – dalijimasis duomenimis. Šios sutarties tikslas – užtikrinti, kad duomenys iš ES į Jungtinėse Amerikos Valstijose esančią organizaciją (esančią „Privatumo skydo“ nare³²)

²⁹ 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmens duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas.

³⁰ Europos Bendrijų Komisija. 2001 m. gruodžio 20 d. sprendimas 2002/2/EB dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB. [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32002D0002&from=en>>.

³¹ ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, p. 46.

³² Tam, kad bendrovė taptų „Privatumo skydo“ sistemos dalyve, ji turi atitinkamai pakoreguoti savo privatumo politiką, kad ši atitiktų susitarime numatytus privatumo principus. Bendrovės privalo kasmet peržiūrėti savo privatumo politiką bei atnaujinti narystę „Privatumo skydo“ sistemoje – to nepadarusios JAV organizacijos nebegali gauti ir tvarkyti duomenų, gautų iš ES pagal „Privatumo skydo“ sistemą. Plačiau apie tai – ES ir JAV „Privatumo skydo“ gairėse. [interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <http://ec.europa.eu/newsroom/document.cfm?doc_id=47770>. Bei EU-U.S. Privacy Shield Framework

būtų perduodami tik tada, kai pastarosios užtikrina, jog visi gauti asmens duomenys bus tvarkomi laikantis griežtų duomenų apsaugos reikalavimų bei taisyklių. Verta paminėti, kad „Privatumo skydo“ pasirašymui kelią atvėrė tuometinio JAV prezidento B. Obamos 2016 m. vasario 24 d. pasirašytas Teisminio teisių gynimo įstatymas, kuris suteikė teisę Europos Sąjungos piliečiams, negyvenantiems Jungtinėse Amerikos Valstijose, JAV teismuose ginčyti neteisėtą ar kitaip neteisingą jų duomenų panaudojimą, taip panaikindamas diskriminaciją pilietybės atžvilgiu duomenų apsaugos srityje. Europos Sąjungos Teisingumo Teismas šiuo įstatymu suteiktas teises ir galimybę tas teises ginti JAV teismuose asmenims, nesantiems JAV piliečiais, vadina esminiu „Privatumo skydo“ susitarimo elementu. Svarbu paminėti, kad „Privatumo skydo“ susitarimo pirmtakė – „Saugaus uosto“ sutartis (angl. „*safe harbour*“ *agreement*), kuri leido ES piliečių duomenis perduoti JAV bendrovėms, pranešusioms JAV Prekybos departamentui, jog jos savanoriškai laikysis „Saugaus uosto“ sprendime išdėstytų principų, nereikalaujant iš jų jokių papildomų saugumo priemonių³³. 2015 m. spalio 6 d. Europos Sąjungos Teisingumo Teismo sprendimu, JAV neužtikrino pakankamos ES gyventojų duomenų apsaugos, todėl „Safe harbour“ susitarimas pripažintas negaliojančiu³⁴. Visgi, dėl poreikio apibrėžti „Safe harbour“ sutartimi reglamentuotus santykius, Europos Sąjunga ir Jungtinės Amerikos Valstijos pasiekė susitarimą, kuriuo buvo nuspręsta, kad JAV įgyvendinus ES duomenų apsaugai taikomus reikalavimus, bus priimta kita sutartis („Privacy shield“ susitarimas) dėl tų pačių teisinių duomenų apsaugos aspektų.

[interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: < <https://www.privacyshield.gov/EU-US-Framework>>. Patikrinti, ar JAV bendrovė yra „Privatumo skydo“ sistemos dalyvė, galima čia: <<https://www.privacyshield.gov/list>>.

³³ Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441). [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02000D0520-20000825>>.

³⁴ 2013 m. Edward Snowden pavišino informaciją apie Jungtinių Amerikos Valstijų vykdomas sekimo programas bei pareiškė susirūpinimą dėl JAV Saugumo agentūros vykdomos veiklos, o tiksliau – ES piliečių duomenų rinkimo, teisėtumo. Po šio pranešimo paaiškėjo, kad JAV valdžios institucijos turėjo prieigą prie tam tikrų „Saugaus uosto“ programoje dalyvaujančių bendrovių surinktų ir tvarkomų ES piliečių duomenų. Atsižvelgdamas į šį pranešimą, Maximillian Schrems kreipėsi į Airijos duomenų apsaugos instituciją su prašymu įvertinti, ar *Facebook*, veikdamas per *Facebook* padalinį Airijoje ir perduodamas duomenis *Facebook* serveriams, esantiems JAV (*Facebook Inc.*), tinkamai ir saugiai tvarkė surinktus duomenis. Byla nukeliavo iki Airijos Aukščiausiojo teismo, o vėliau – ir iki ESTT, kuris įvertino, kaip ES piliečių duomenys iš tiesų yra renkami ir tvarkomi JAV. ESTT nusprendė, kad „Saugaus uosto“ sprendimas neužtikrino tokių asmens duomenų apsaugos principų, kokius numato ES teisės aktai, todėl JAV neužtikrina pakankamos ES esančių asmenų duomenų apsaugos. Remdamasis šiomis išvadomis, ESTT pripažino „Saugaus uosto“ sprendimą negaliojančiu. Plačiau: Europos Sąjungos Teisingumo Teismas. 2015 m. spalio 6 d. sprendimas *Maximillian Schrems prieš Data Protection Commissioner* byloje, C-362/14. [interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>>. Taip pat žr. Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. spaudos konferenciją Nr. 117/15. *The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid*. [interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>>.

1.2. Duomenų apsaugos teisė po Bendrojo duomenų apsaugos reglamento įsigaliojimo

Bendrajam duomenų apsaugos reglamentui dar net neįsigaliojus, visuomenėje jau buvo įžvelgiama šio duomenų apsaugos reforma vadinamo teisės šaltinio įtaka asmens duomenų apsaugos teisei ne tik Europos Sąjungoje, tačiau ir viso pasaulio mastu. Kaip 2016 m. teigė politikas Jan Philipp Albrecht, tuometinis Europos Parlamento narys bei Piliečių laisvių, teisingumo ir vidaus reikalų komiteto pirmininko pavaduotojas, svarbiausia suprasti, kaip Bendrasis duomenų apsaugos reglamentas pakeis ne tik Europos duomenų apsaugos teisę, tačiau ir ne ką mažiau nei visą mums žinomą pasaulį³⁵. Vadinasi, dar prieš įgaudamas teisinę galią Reglamentas jau buvo laikomas globaliai reikšmingu asmens duomenų apsaugos teisės šaltiniu, nes šiuo dokumentu užtikrinama apsauga keliauja kartu su duomenimis. Kitaip tariant, duomenų apsaugos taisyklių taikymas nepriklauso nuo to, kur aktualūs duomenys atsiduria³⁶.

Bendrojo duomenų apsaugos reglamento ekstrateritorialus poveikis dažnai įvardijamas kaip viena iš naujovių duomenų apsaugos srityje. Viena vertus, Reglamentas nėra pirmasis teisės aktas, kurio nuostatos būtų taikomos organizacijoms už tam tikros valstybės ribų. Pavyzdžiui, 2012 m. Singapūro asmens duomenų apsaugos įstatyme (26 m. Nr. 2012) numatyta, kad šio įstatymo normos taikomos visoms organizacijoms, renkančioms asmenų, esančių Singapūre, duomenis, nepriklausomai nuo to, ar toji organizacija turi buveinę Singapūre³⁷.

Tuo tarpu JAV 1998 m. priimtas Vaikų privatumo internete saugos aktas taikomas ir užsienyje veikiančioms internetinėms paslaugoms bei svetainėms, kurių veiklos sritis nukreipta į vaikus, esančius Jungtinėse Amerikos Valstijose arba kurie tikslingai renka informaciją apie JAV esančius vaikus³⁸. O štai Australijos su duomenų apsauga susijusio

³⁵ Albrecht, Jan Philipp. How the GDPR Will Change the World. *European Data Protection Law Review*, Vol. 2, issue 3, 2016, p. 287 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://edpl.lexxion.eu/article/edpl/2016/3/4>>.

³⁶ Europos Komisija. Kokios taisyklės taikomos, jeigu mano organizacija perduoda duomenis už ES ribų? [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_it>.

³⁷ Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), Republic of Singapore Government Gazette, 2012 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://sso.agc.gov.sg/Act/PDPA2012#legis>>.

³⁸ Vaikų privatumo internete saugos aktas (angl. *Children's Online Privacy Protection Rule ("COPPA")*), 2018 [interaktyvus, žiūrėta 2020 m. kovo 18 d.]. prieiga per internetą: <<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>>.

įstatymo - *Privacy Act 1988 (Cth)* - 5B straipsnyje numatyta, be kita ko, kad šis teisės aktas taikomas:

- Veiklai, susijusiai su Australijos piliečių ar kitų asmenų, laikomų lygiais su Australijos piliečiais, asmenine informacija;
- Australijos organizacijoms;
- Organizacijoms, kurios užsiima verslu Australijoje;
- Situacijoms, kuomet asmeninė informacija buvo renkama ar kaupiama Australijos organizacijos ar kitos, ne Australijos teritorijoje esančios, organizacijos, prieš vykdant veiklą ar jos vykdymo metu;
- Kai organizacija turi ryšį su Australija (angl. *Australian link*)³⁹.

Aukščiau išvardintomis nuostatomis Australijos valdžios institucijos įtvirtino pareigą laikytis duomenų apsaugos nuostatų ne tik Australijoje įsikūrusioms, tačiau ir už šios šalies ribų veikiančioms bendrovėms.

Vadinasi, galima teigti, kad tam tikras ekstrateritorialumo principas jau buvo įtvirtintas kai kurių valstybių duomenų apsaugos įstatymuose dar prieš priimant Bendrąjį duomenų apsaugos reglamentą, todėl tokios taisyklės dėl teritorinio taikymo nėra visiškai naujas reiškinys duomenų apsaugos srityje.

Kita vertus, negalima paneigti to, kad Reglamentas, išplėsdamas Europos Sąjungos duomenų apsaugos teisės teritorinę taikymo sritį, ES mastu įgyvendino naujovę – iki šiol ES priimtuose duomenų apsaugos teisės šaltiniuose nebuvo numatytas toks ar panašus ekstrateritorialumo principas. Be to, kiti svarbūs tarptautiniai duomenų apsaugos teisės šaltiniai (pavyzdžiui, Konvencija Nr. 108, Ekonominio bendradarbiavimo ir plėtros organizacijos paskelbtos Privatumo gairės) apskritai nenustatė konkrečių teritorinės taikymo srities taisyklių, todėl jau toks nuostatų teritorinio reglamento galiojimo atžvilgiu nustatymas yra tam tikra naujovė ES duomenų apsaugos reglamentavime.

Bendrojo duomenų apsaugos reglamento teritorinio taikymo sritis ypatinga tuo, kad jis turi būti taikomas ir atliekant tokį duomenų tvarkymą, kai ES esančių duomenų subjektų duomenis tvarko duomenų valdytojas arba duomenų tvarkytojas, neįsisteigęs nei vienoje iš Europos Sąjungos valstybių narių ir atitinkama duomenų tvarkymo veikla yra susijusi su šiomis sritimis:

- 1) prekių, paslaugų siūlymu duomenų subjektams Europos Sąjungoje, nepriklausomai nuo to, ar už tas prekes ar paslaugas duomenų subjektui reikia mokėti; arba

³⁹ Privacy Act 1988, No. 119, 1988, Australia [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://www.legislation.gov.au/Details/C2020C00025>>.

2) elgesio stebėseną, kai jie veikia Europos Sąjungoje⁴⁰.

Palyginus Reglamento ir Direktyvos normose įtvirtintą taikymo sritį matyti didžiausias skirtumas – iki reglamento įsigaliojimo ES duomenų apsaugos teisės reguliavimas buvo taikomas pagal asmens (tiek fizinio, tiek juridinio), atsakingo už duomenų tvarkymą, įsisteigimo vietos kriterijų⁴¹. Tuo tarpu Bendrojo duomenų apsaugos reglamento nuostatose pabrėžiama ne teritorijos, tačiau veiklos kriterijaus svarba. Galima teigti, kad Reglamentu tarsi panaikinama riba tarp valstybių tais atvejais, kai siekiama apsaugoti asmenų teisę į duomenų privatumą, taip skatinant duomenų apsaugos teisės globalizaciją - Reglamento nuostatos įtvirtina ne Europos Sąjungoje esančių duomenų valdytojų pareigą laikytis ES reikalavimų, kai tvarkomi ES esančių asmenų duomenys, taip pat reguliuoja atvejus, kai asmens duomenis leidžiama perduoti į trečiąsias valstybes arba tarptautinėms organizacijoms.

Žinoma, svarbu nepamiršti, kad nors Bendrasis duomenų apsaugos reglamentas laikomas bene reikšmingiausiu duomenų apsaugos teisės šaltinių, tačiau, visgi, veikia ne vienas. Be Europos Sąjungos direktyvų (pavyzdžiui, didelę reikšmę turinčios 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, kuria saugomos ES piliečių pagrindinės teisės į duomenų apsaugą, kai duomenis naudoja teisėsaugos institucijos. Direktyva siekiama užtikrinti, kad nukentėjusiųjų, liudytojų ir įtariamųjų asmens duomenys būtų tinkamai apsaugoti, kad būtų palengvintas tarpvalstybinis bendradarbiavimas kovojant su nusikalstamumu ir terorizmu⁴²), kitų šaltinių, susijusių su duomenų apsauga tam tikrose konkrečiose srityse, vertinant asmens duomenų apsaugos teisės šaltinius teritoriniu aspektu, svarbu išskirti keletą tarptautinių sutarčių bei konvencijų, tarsi papildančių Reglamentą.

⁴⁰ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁴¹ ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 47.

⁴² 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. *OJ L 119*, 2016, p. 89–131 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680>>.

Viena iš tarptautinių sutarčių, veikiančių duomenų apsaugos teisės srityje, yra jau minėtas tarp JAV ir Europos Sąjungos 2016 m. pasirašytas „Privatumo skydo“ susitarimas. Bendrasis duomenų apsaugos reglamentas draudžia perduoti asmens duomenis į trečiąsias valstybes arba tarptautines organizacijas, nebent šios įgyvendina nustatytus reikalavimus, taikomus duomenų apsaugai, numatomus ES teisės aktuose, arba ta trečioji valstybė ar organizacija, kuriai ketinama perduoti asmens duomenis, Europos Komisijos yra pripažinta tinkama ir iš kurios nereikalaujama jokių papildomų saugumo užtikrinimo priemonių – tai tokios valstybės, kurios atskiru sprendimu yra pripažintos savo teisės aktais užtikrinančios asmens duomenų saugumą (pavyzdžiui, Kanada) arba tarptautinėmis sutartimis užtikrina ES nustatytų asmens duomenų apsaugai taikomų principų įgyvendinimą, kaip šiuo atveju – Jungtinėse Amerikos Valstijose esančios bendrovės, priklausančios „Privatumo skydo“ sistemai.

Anksčiau paminėtas Reglamente nustatytas draudimas perduoti duomenų subjekto, esančio ES, duomenis trečiajai valstybei svarbus vertinant ir Konvencijos Nr. 108 veikimą. Taip pat kai JAV, Konvenciją Nr. 108 pasirašiusios valstybės yra laikomos užtikrinančiomis tinkamą duomenų apsaugą, todėl į jas iš ES gali būti perduodami asmens duomenys be jokių papildomų reikalavimų. Verta paminėti, kad 2018 m. spalio 10 d. Europos Komisija, atsižvelgdama į tai, kad nuo pirminės Konvencijos Nr. 108 versijos sukūrimo, technologijos bei priemonės, kuriomis renkami ar kuriose kaupiami fizinių asmenų duomenys, smarkiai patobulėjo, paskelbė dar vieną Konvenciją Nr. 108 papildantį protokolą, kuris, kaip jau minėta šiame darbe, papildomų reikalavimų nesukuria, tačiau, kaip manoma, tam tikru būdu gali palengvinti ES esančių asmenų duomenų perdavimą į trečiąsias valstybes. Tai įrodo bendrajame duomenų apsaugos reglamento preambulės 105 dalyje įtvirtinta nuostata, pagal kurią Europos Komisija, vertindama valstybę dėl jos tinkamumo užtikrinti asmens duomenų apsaugą, pirmiausia turėtų atsižvelgti į trečiosios valstybės prisijungimą prie Konvencijos 108 ir jos papildomo protokolo⁴³. Be to, 2018 m. spalio 10 d. priimtame Konvencijos Nr. 108 papildomame protokole įtvirtintos nuostatos yra pagrįstos Bendrojo duomenų apsaugos reglamento principais. Pavyzdžiui, naujasis protokolas papildo Konvenciją Nr. 108 tokiomis duomenų subjektų teisėmis kaip teisė reikalauti, kad duomenys būtų ištrinti, taip pat pridedamas reikalavimas įsteigti duomenų apsaugos priežiūros institucijas ir kt.⁴⁴.

⁴³ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁴⁴ Europos Taryba. 2018 m. spalio 10 d. Protokolas, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, TAR, 2020-02-25, Nr. 4015

Lietuvos Respublika Konvenciją Nr. 108 ratifikavo 2000 m., ji pradėjo galioti 2001 m. spalio 1d., tuo tarpu 2018 m. spalio 10 d. priimtą Konvencijos Nr. 108 papildomą protokolą Lietuva ratifikavo 2019 m. lapkričio 7 d. Tiesa, nurodoma, kad minėtasis Konvencijos Nr. 108 papildomas protokolai laikinai taikomas nuo 2020-04-01. (pagal protokolo 37 str., jis įsigalioja pirmą mėnesio dieną, praėjus trims mėnesiams po to, kai visos Konvencijos Nr. 108 šalys pareiškia norą įsipareigoti pagal Protokolą).

Vadinasi, priėmus Bendrąjį duomenų apsaugos reglamentą tokios tarptautinės sutartys kaip Konvencija Nr. 108 ar „Privatumo skydo“ susitarimas ne tik išsaugojo savo teisinę galią, tačiau tapo ir papildomu Reglamento įgyvendinimo įrankiu.

Apžvelgus duomenų apsaugos teisės raidą Europos Sąjungoje, galima teigti, kad iki pat bendrojo duomenų apsaugos reglamento priėmimo nei vienas teisės aktas, veikiantis Europos Sąjungos duomenų apsaugos teisės srityje, nenumatė tokios plačios teritorinio taikymo srities ir šis ekstrateritorialaus taikymo principas, nors tam tikra dalimi jau įgyvendintas kai kuriose pasaulio valstybėse, Europos Sąjungoje yra naujas reiškinys. Taip pat verta atkreipti dėmesį, kad reglamentas, nors ir pagrindinis šaltinis Europos Sąjungos duomenų apsaugos srityje, tačiau veikia ne vienas – šalia veikia bei tam tikrais atvejais reglamentą papildo ir galiojančios Europos Sąjungos direktyvos, susijusios su asmens duomenų apsauga, bei duomenų apsaugai aktualios tarptautinės sutartys.

[interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/d8e8a420c89811e9a56df936f065a619?jfwid=w5secs1kuh>>.

2. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO NORMOS DĖL TERITORINIO TAIKYMO: INTERPRETAVIMO IR ĮGYVENDINIMO PROBLEMAS

2.1. Bendrojo duomenų apsaugos reglamento normų interpretavimo problemos

Bendrasis duomenų apsaugos reglamentas, kaip jau minėta šiame darbe, įnešė naujovių asmens duomenų apsaugos srityje. Viena jų – normos dėl ekstrateritorialaus Reglamento taikymo. Pirmiausia, verta paminėti, kad Bendrasis duomenų apsaugos reglamentas dėl savo teisinio pobūdžio yra tiesiogiai taikomas teisės aktas⁴⁵ ir jo įgyvendinti nacionalinėje teisėje Europos Sąjungos valstybės narės neprivalo, tuo tarpu Duomenų apsaugos reglamentas įpareigojo ES nares perkelti Direktyvos nuostatas į savo nacionalinę teisę. Būtent dėl pastarojo taikymo būdo kiekviena valstybė narė, įgyvendindama Direktyvoje įtvirtintus duomenų apsaugos principus bei taisykles, tam tikras normas galėjo dalinai interpretuoti vis kitaip, todėl Direktyva nesugebėjo užtikrinti visiškai vienodo asmens duomenų apsaugos režimo visoje Europos Sąjungoje, ir įvairiose valstybėse narėse atsirado skirtingas direktyvos aiškinimas. Tuo tarpu reglamentas, dėl tiesioginio taikymo pobūdžio, nustato suderintas duomenų apsaugos taisykles, taip suvienodindamas teisės taikymą bei stengiasi užtikrinti didesnę teisinę tikrumą⁴⁶. Kita vertus, nors bendrajame Duomenų apsaugos reglamente nebeliko nuorodos į valstybių narių nacionalinę teisę (kaip antai buvo nurodyta Duomenų apsaugos direktyvos 4 straipsnyje, susijusiame su teritoriniu Direktyvos taikymu⁴⁷), Reglamentas visgi suteikia teisę valstybėms narėms nukrypti nuo tam tikrų jo normų bei pritaikyti aktualias nacionalinės teisės nuostatas. Štai Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, įsigaliojus Reglamentui, buvo atitinkamai pakoreguotas (nauja redakcija galioja nuo 2018 m. liepos 16 d.). Atnaujintoje redakcijoje reglamentuoti su Bendrojo duomenų apsaugos reglamento reikalavimais susiję aspektai, kuriuos valstybės narės turi teisę reglamentuoti, taip pat tie klausimai, kuriuos

⁴⁵ Sutarties dėl Europos Sąjungos veikimo suvestinė redakcija. Europos Sąjungos oficialusis leidinys, C 326, 2012, 288 str., p. 171 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: < <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=OJ:C:2012:326:TOC>>.

⁴⁶ CHEN, Jiahong. How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation. *International Data Privacy Law*, Vol. 6, No. 4, 2016, p. 311 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/6/4/310/2567746?redirectedFrom=fulltext>>.

⁴⁷ „Kiekviena valstybė narė taiko nacionalines nuostatas, kurias ji priima pagal šią direktyvą, kai tvarkomi asmens duomenys, jeigu <...>”. Plačiau: 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, 4 str. 1 d., p. 363.

valstybėms narėms leidžiama reglamentuoti nacionaliniais teisės aktais⁴⁸. Be to, Reglamento preambulės 10 dalyje nurodyta, kad „Kalbant apie asmens duomenų tvarkymą siekiant laikytis teisinės prievolės, užduoties, vykdomos dėl viešojo intereso arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, atlikimui valstybėms narėms turėtų būti leidžiama išlaikyti arba nustatyti nacionalines nuostatas, kuriomis konkrečiau apibrėžiamas šiame reglamente nustatytų taisyklių taikymas“⁴⁹. Vadinasi, kai to reikalauja viešasis interesas ar kitas teisėtas tikslas, valstybės narės gali taikyti galiojančias nacionalinės teisės nuostatas vietoje atitinkamų reglamento normų, tačiau, galima teigti, kad toks tikslas turi būti pateisinamas ir nepažeisti pamatinių principų (proporcingumo, teisėtumo ir kt.). Šioje dalyje aptariami pagrindiniai teritorinio Reglamento taikymo kriterijai, bei tai, kaip kai kurios su teritoriniu reglamento taikymu susijusios normos ir taikymo kriterijai kelia tam tikrų interpretavimo sunkumų iš dalies dėl skirtingo reglamentavimo, įsivyravusio Europos Sąjungos valstybėse narėse, bei jau minėto kai kurių Reglamento normų lankstumo, taip pat apžvelgiama, kokių priemonių ėmėsi Europos Sąjungos institucijos, siekdamos suvienodinti Reglamento taikymą skirtingose valstybėse.

2.1.1. Bendrojo duomenų apsaugos reglamento taikymas pagal buveinės kriterijų

Tais atvejais, kai asmens duomenys tvarkomi duomenų tvarkytojo ar valdytojo buveinės, esančios Europos Sąjungoje, veikloje, nepaisant to, ar pats tvarkymo „procesas“ atliekamas ES teritorijoje (pavyzdžiui, jei tvarkymui reikalingi serveriai ir kita įranga yra ne Europos Sąjungoje), atitinkamas duomenų tvarkymas turi vykti pagal ES teisės nustatytas duomenų apsaugos taisykles⁵⁰. Šią bendrą teritorinio taikymo taisyklę, kurios aktualumą apibrėžia fizinės buveinės kriterijus, įtvirtina Bendrojo duomenų apsaugos reglamento 3 straipsnio 1 dalis.

Aptariama norma nustato, kad reglamentas taikomas net tais atvejais, kai buveinės kriterijus išpildomas, tačiau patys duomenys tvarkomi ne Europos Sąjungoje. Ši nuostata, teigiama, priimta atsižvelgiant į *Google Spain* byloje Europos Sąjungos Teisingumo Teismo padarytą išvadą, konstatuojančioje, kad tarp ES padalinio veiklos ir ne ES duomenų tvarkytojo duomenų tvarkymo veiklos esant „neatsiejamam ryšiui“, asmens teisės į

⁴⁸ Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. TAR, 2018-07-11, Nr. 11733.

⁴⁹ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁵⁰ ZALESKIS, Julius. *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*. Vilnius: Registrų centras, 2019, p. 104.

duomenų apsaugą įgyvendinimui turi būti taikoma ES teisė⁵¹. Vadinasi, teismų praktikos suformuotą taisyklę, teigiančią, jog duomenų tvarkymo vieta yra vienas esminių kriterijų vertinant, kokia teisė atitinkamu atveju turi būti taikoma, Europos Sąjungos institucijos įgyvendino tiesiogiai taikomu teisės aktu, taip suteikdamas minėtajai taisyklei apibrėžtumo.

Kita vertus, vertinant Bendrojo duomenų apsaugos reglamento 3 str. 1 dalyje įtvirtintą taisyklę, tam, kad būtų užtikrintas vienodas jos taikymas bei interpretavimas, apibrėžtumo reikalauja net keli raktiniai žodžiai ar terminai – tai Sąjungoje esanti buveinė, vykdoma veikla Sąjungoje bei nepaisymas to, ar duomenys tvarkomi Sąjungoje, ar ne.

Vertinant buveinės kriterijaus „sudedamąsias dalis“, pirmiausia svarbu tinkamai nustatyti, kas yra laikoma buveine bei kokia veikla patenka į Reglamento taikymo sritį. Bendrojo duomenų apsaugos reglamento preambulės 22 dalyje nurodoma, kad tais atvejais, kai reali ir veiksminga veikla vykdoma per stabilias struktūras (angl. *with a sufficient degree of stability*), galima teigti, kad yra įsteigta buveinė nepriklausomai nuo jos struktūrinės formos (filialas ar patronuojamoji bendrovė)⁵². Kaip pastebi Europos duomenų apsaugos valdyba Gairėse dėl Reglamento teritorinio taikymo, „stabilios struktūros“ standartas gali būti vertinamas labai skirtingai. Tarkime, tais atvejais, kai pagrindinė duomenų valdytojo veikla yra susijusi su paslaugų teikimu skaitmeninėmis priemonėmis (angl. *the provision of services online*), užtenka, kad veiklą Sąjungos teritorijoje vykdytų bent vienas duomenų valdytojo atstovas ar bendrovės darbuotojas⁵³, tačiau svarbu, kad duomenų tvarkytojo veikla būtų susijusi to darbuotojo ar atstovo, esančio Europos Sąjungoje, veikla. Galima teigti, kad taip dar kartą patvirtinama *Google Spain* byloje ESTT pabrėžta „neatsiejamu ryšio“, esančio tarp ne ES veikiančio duomenų tvarkytojo ir ES padalinio veiklos, svarba⁵⁴.

Kita vertus, EDAV Gairėse dėl Reglamento teritorinio taikymo tiksliai neapibrėžia, kokiais atvejais, kai stabilios veiklos kriterijus yra patenkinamas, galima laikyti, kad bendrovė turi buveinę ES. Gairėse dėl reglamento teritorinio taikymo teigiama, kad, nors duomenų tvarkytojo bendrovė, esanti ne Europos Sąjungoje, neturi filialo ar dukterinės įmonės ES, tai savaime nereiškia, kad duomenų tvarkytojas negali būti laikomas neturinčiu

⁵¹ Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* byloje, C-131/12, ECLI:EU:C:2014:317.

⁵² *Ibid.* 22 dalis, p. 4.

⁵³ Europos duomenų apsaugos valdyba (EDAV) (angl. *European data protection board*). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation, 2019. [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_lt>.

⁵⁴ Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* byloje, C-131/12, ECLI:EU:C:2014:317.

buveinės Europoje. Kita vertus, čia pat EDAV teigia, kad, nors buveinės sąvoka yra ganėtinai plati, taip pat negalima preziumuoti, jog ne ES duomenų tvarkytojas, tarkime, jo internetinei svetainei veikiant ir Europoje, yra įsisteigęs Sąjungoje. Kitaip tariant, Europos duomenų apsaugos valdyba pabrėžia, kad, vertinant buveinės kriterijų, bene svarbiausia yra įvertinti tai, ar duomenų tvarkytojo vykdoma veikla, susijusi su duomenų tvarkymu, turi tiesioginę sąsają su jo buveinės veikla, net jei ta buveinė pati nevykdo jokių duomenų tvarkymo veiksmų. Siekdama vienodo veikimo šios normos kontekste Europos duomenų apsaugos valdyba ragina ne ES organizacijas, esančius duomenų tvarkytojais, įvertinti sąsajas tarp veiklos, dėl kurios reikalingas disponavimas tam tikrais asmens duomenimis, bei tarp duomenų tvarkytojo buveinės ES veiklos – esant tiesioginiam ryšiui tarp šių veiklų tinkamai duomenų apsaugai užtikrinti yra taikoma ES teisė. Be to, įvertinus šiuos aspektus ir jiems indikuojant, jog tam tikroje veikloje turi būti taikomos Reglamento nuostatos, tampa nesvarbu, ar pati duomenų tvarkymo procedūra atliekama Europos Sąjungoje ar trečiojoje valstybėje – galima teigti, kad taip yra visapusiškai apsaugomi ES esančių asmenų duomenys, nepriklausomai nuo to, kurioje šalyje jų duomenimis yra disponuojama.

Kita vertus, tam tikrais atvejais svarbu atskirti duomenų valdytojo ir duomenų tvarkytojo pareigas bei atsakomybę Reglamento 3 str. 1 dalies taikymo kontekste. Be anksčiau aptartos duomenų tvarkytojo veiklos per ES esančią buveinę, galimas dar vienas veikimo būdas – duomenų valdytojas, įsisteigęs ne Europos Sąjungoje, gali pasamdyti duomenų tvarkytoją, įsteigtą ES, bei patikėti jam savo klientų duomenis⁵⁵. Tokiu atveju duomenų valdytojui, įsisteigusiam ne ES, Reglamentas nebus taikomas, tačiau duomenų valdytojo pasamdytas duomenų tvarkytojas, įsisteigęs ES, privalės veikti pagal Bendrojo duomenų apsaugos reglamento nustatytas taisykles bei principus. Tuo tarpu tada, kai duomenų valdytojas, įsisteigęs ES, pasamdo duomenų tvarkytoją, įsisteigusį ne Europos Sąjungos valstybėje narėje, Reglamento nuostatos bus taikomos duomenų valdytojui, tačiau pastarasis turės užtikrinti, kad ne ES įsisteigęs duomenų tvarkytojas laikosi Bendrajame duomenų apsaugos reglamente išdėstytų duomenų apsaugos principų bei taisyklių⁵⁶.

⁵⁵ Europos duomenų apsaugos valdyba (EDAV) (angl. *European data protection board*). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation, 2019. [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_lt>.

⁵⁶ *Ibid.*

2.1.2. Bendrojo duomenų apsaugos reglamento taikymas pagal į ES duomenų subjektus nukreiptos veiklos kriterijų

Bendrojo duomenų apsaugos reglamento 3 str. 2 dalyje aptariami atvejai, kai duomenų valdytojas ar duomenų tvarkytojas neturi jokios fizinės buveinės Europos Sąjungoje. Ši norma bene geriausiai atspindi ekstrateritorialų Reglamento taikymo principą – nustatytos taisyklės pažymi, kad pats faktas, jog duomenų tvarkytojas ar duomenų valdytojas nėra įsisteigęs ES ar duomenų valdytojas nėra pasisamdęs duomenų tvarkytojo, veikiančio Europos Sąjungos teritorijoje, nereiškia, jog šių subjektų veikla, susijusi su disponavimu ES esančių asmenų duomenimis, negali būti reglamentuojama bendrojo duomenų apsaugos reglamento. Reglamento 3 str. 2 dalyje nurodytos dvi sąlygos, kurioms esant reglamentas gali būti taikomas duomenų tvarkymui tais atvejais, kai ES duomenų subjektų asmens duomenis tvarko Europos Sąjungoje neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas, kitaip tariant, tais atvejais, kai jų veikla nukreipta į ES duomenų subjektus (angl. *targeting criterion*). Reglamente nurodyta, kad tokiu atveju duomenų tvarkymo veikla turi būti susijusi su:

1. prekių arba paslaugų siūlymu tokiems duomenų subjektams Sąjungoje, nepaisant to, ar už šias prekes arba paslaugas duomenų subjektui reikia mokėti; arba
2. elgesio, kai jie veikia Sąjungoje, stebėseną.⁵⁷

Pirmiausia, atkreipiamas dėmesys, kad Reglamento normos, susijusios su teritoriniu jo taikymu, ypatingai pabrėžia duomenų subjekto buvimo Europos Sąjungoje kriterijų, t. y. Reglamento nuostatos neišskiria duomenų subjektais asmenų, kurie yra ES piliečiai, turi nuolatinę gyvenamąją vietą vienoje iš Europos Sąjungos valstybių narių ar pagal kitokį asmenų statusą. Tokį lygiavertį taikymą pavirtina ir Reglamento preambulės 14 dalis, kurioje teigiama, kad bendroju duomenų apsaugos reglamentu užtikrinama teisė į duomenų apsaugą fiziniams asmenims, neatsižvelgiant į jų gyvenamąją vietą ar pilietybę⁵⁸. Europos duomenų apsaugos valdybos teigimu, toks Reglamente įtvirtintas lygiavertis požiūris į visus asmenis, esančius ES, kaip duomenų subjektus, atspindi pamatinius Europos Sąjungos teisės principus, o tiksliau – Visuotinės žmogaus teisių deklaracijos 8

⁵⁷ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁵⁸ *Ibid.*

str. įtvirtintą kiekvieno asmens teisę į jo duomenų privatumą⁵⁹. Vadinasi, galima teigti, kad Reglamentas taikomas tam tikra prasme vadovaujantis nediskriminavimo principu.

Siekdama didesnio aiškumo ir šios normos taikymo kontekste, EDAV nurodo, kad Bendrojo duomenų apsaugos reglamento 3 str. 2 d. numatyti veiklos kriterijai turi būti tikslingai nukreipti į ES esančius asmenis⁶⁰. Kitaip tariant, jei Reglamento 3 str. 2 dalyje nurodyta veikla netikslingai ar atsitiktinai yra susijusi su asmeniu, esančiu ES, tokiu atveju minėtoji veikla nepatenka į Reglamento 3 str. 2 dalyje apibrėžtą taikymo sritį. Bendrasis duomenų apsaugos reglamentas taip pat netaikomas tada, kai tam tikros paslaugos yra nukreiptos į asmenis, esančius ne ES, tačiau nenustoją būti teikiamos ir tiems asmenims apsilankius Europos Sąjungoje – šioje situacijoje, vėl gi, svarbus tikslingumo kriterijus, paslaugų teikimas ar elgesio stebėseną turi būti tikslingai orientuota į Europoje esančius asmenis⁶¹. Kita vertus, svarbu pabrėžti, kad tikslingas veiklos nukreipimas į ES esančius asmenis savaime nesukuria pareigų Reglamento taikymo kontekste – ši tikslinga veikla turi būti susijusi su prekių ar paslaugų (tiek apmokamų, tiek neapmokamų) siūlymu ir teikimu arba su asmenų elgesio stebėseną. Be to, veiklos tikslingumas gali būti parodomas įvairiais veiksniais, pavyzdžiui, konkrečios tai ES valstybei narei būdingos valiutos ar kalbos vartojimas, konkrečios ES narės minėjimas ir kt.⁶². Tačiau būtina pabrėžti ir tai, kad tai, jog duomenų valdytojo ar tvarkytojo interneto svetainė, kontaktiniai duomenys (elektroninis paštas ir kt.) yra prieinami asmenims, esantiems Europos Sąjungoje, arba kad vartojama kalba ar valiuta, kuri paprastai vartojama vienoje ir keliuose valstybėse narėse neturėtų savaime reikšti tikslingo ketinimo teikti paslaugas ar prekes, bet tai gali būti pagalbinė priemonė siekiant nustatyti, ar veikla yra nukreipta į ES esančius asmenis siekiant paslaugas teikti konkrečiai jiems⁶³.

Taip pat kaip ir veiklai, susijusiai su prekių ar paslaugų teikimu, asmenų, esančių ES, elgesio stebėseną taip pat turi būti tikslingai nukreipta į Europos Sąjungoje esančius

⁵⁹ Europos duomenų apsaugos valdyba (EDAV) (angl. European data protection board). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation, 2019, p. 14 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_lt>.

⁶⁰ *Ibid.*, p. 15.

⁶¹ *Ibid.*

⁶² ZALESKIS, Julius. *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*. Vilnius: Registrų centras, 2019, p. 105.

⁶³ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

duomenų subjektus. EDAV Gairėse dėl Reglamento teritorinio taikymo pateikia kelis pavyzdžius veiklų, kurios gali būti laikomos elgesio stebėseną:

- vartotojų elgsena pagrįsta reklama (angl. *Behavioural advertisement*);
- slapukų ar kitų informacijos rinkimo bei atsekimo priemonių, pavyzdžiui, pirštų antspaudų rinkimo, naudojimas;
- apklausos bei kiti tyrimai, paremti profiliavimu;
- asmens sveikatos būklės stebėjimas bei rinkimas ir kt⁶⁴.

2.1.3. Bendrojo duomenų apsaugos reglamento taikymas ES neįsisteigusiems duomenų valdytojui, veikiančiam pagal tarptautinę viešąją teisę

Bendrojo duomenų apsaugos reglamento 3 str. 3 dalyje nurodoma, kad „Šis reglamentas taikomas asmens duomenų tvarkymui, kai asmens duomenis tvarko duomenų valdytojas, įsisteigęs ne Sąjungoje, o vietoje, kurioje pagal viešąją tarptautinę teisę taikoma valstybės narės teisė“⁶⁵. Šiam kriterijui įgyvendinti reikalingos dvi sąlygos:

1. Duomenų valdytojas negali turėti Europos Sąjungos valstybės narės teritorijoje įsteigtos buveinės, kuriai galėtų būti taikoma ES teisė⁶⁶;
2. Europos Sąjungos valstybės narės teisė gali būti taikoma už šios valstybės narės ribų, pavyzdžiui, konsulatuose ar diplomatinėse atstovybėse, taip pat ES valstybės narės vėliavos jurisdikciją turinčiuose laivuose, kai šie plaukioja ES teritorijoje esančiuose vandenyse arba už ES ribų, bei virš šių vandenių praskrendantiems orlaiviams⁶⁷.

Antroji sąlyga parodo, kad priimant Bendrąjį duomenų apsaugos reglamentą buvo laikomasi, pagrindinių tarptautinės teisės principų bei taisyklių – išvardytose situacijose ES

⁶⁴ Europos duomenų apsaugos valdyba (EDAV) (angl. European data protection board). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation, 2019, p. 20 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_it>.

⁶⁵ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁶⁶ ZALESKIS, Julius. *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*. Vilnius: Registrų centras, 2019, p. 106.

⁶⁷ Europos duomenų apsaugos valdyba (EDAV) (angl. European data protection board). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation, 2019, p. 23 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_it>.

valstybės narės teisė taikoma ne tik duomenų apsaugos srityje, tačiau ir kitose teisės srityje, ir, jei Reglamentas įtvirtintų kitas teisės taikymo taisykles diplomatinių atstovybių, konsulatų, ES valstybės narės vėliavos jurisdikciją turinčių laivų ar orlaivių atvejais, būtų tam tikra dalimi nesilaikoma tarptautinės viešosios teisės nustatytų jurisdikcijos taikymo taisyklių bei principų⁶⁸.

Apibendrinant visas bendrojo duomenų apsaugos reglamento 3 str. numatytas nuostatas bei raktinių žodžių išaiškinimus, galima teigti, būtent minėtųjų raktinių žodžių bei kriterijų (pavyzdžiui, buveinė, į ES duomenų subjektą nukreipta veikla, stabilios struktūros ir kt.) vienodas interpretavimas bei supratimas yra esminis siekis norint suvienodinti skirtingų Europos Sąjungos valstybių narių vykdomą Reglamento įgyvendinimą. Būtent todėl Europos duomenų apsaugos valdyba gairėse dėl teritorinio Reglamento taikymo detaliai paaiškina kiekvieną kartinę reglamento 3 str. normą bei sąvoką ir pabrėžia pagrindinius principus bei sąlygas, reikalingas tam, kad reglamentas būtų laikomas galiojančiu tam tikroje teritorijoje.

⁶⁸ JERVIS, Claire. The curious case of Article 3(3) of the GDPR and its application to diplomatic missions. *International Data Privacy Law*, Vol. 0, No. 0, 2020 [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipaa001/5802596?redirectedFrom=fulltext>>.

2.2. Bendrojo duomenų apsaugos reglamento įgyvendinimo problemos

Bendrojo duomenų apsaugos reglamento priėmimas privertė suklusti tarptautinius verslus, organizacijas bei kitus fizinius ar juridinius asmenis, vienaip ar kitais renkančius, tvarkančius ir naudojančius Europos Sąjungoje esančių asmenų duomenis savo veikloje – duomenų valdytojai ar tvarkytojai, kurių negalėjo „pasiiekti“ direktyvos nuostatos (kitaip tariant, tie duomenų valdytojai ir tvarkytojai, kurie nebuvo įsisteigę ES teritorijoje, neturėjo joje buveinės ar atitinkamos įrangos bei priemonių), staiga įgavo pareigą laikytis Europos Sąjungos reglamentavimo duomenų apsaugos srityje. Reglamento 3 straipsnyje įtvirtinti teritorinio taikymo kriterijai panaikino siauriau apibrėžtus Duomenų apsaugos direktyvoje ar kituose Europos Sąjungos duomenų apsaugos teisės šaltiniuose numatytus įsisteigimo, „fizinio buvimo“ ES teritorijoje kriterijus, kuris palaipsniui turėtų užkirti kelią bet kokiems bandymams „apeiti“ Europos Sąjungos institucijų nustatytus duomenų apsaugos standartus. Kyla klausimas, ar Europos Sąjunga bei jai pavaldžios duomenų apsaugos institucijos yra pasirengusios užtikrinti tinkamą bendrojo duomenų apsaugos reglamento įgyvendinimą už Europos Sąjungos ribų.

Kiekviena valstybė ar sąjunga, kaip antai nagrinėjamu atveju – Europos Sąjunga, ketindama teisės aktuose įtvirtinti ekstrateritorialų taikymo principą, be kita ko, turi apsvaistyti, ar toks taikymas duos norimų rezultatų. Pirmiausia, svarbu yra nustatyti, ar tokiam išplėtam teritoriniam taikymui pagrindas suteikiamas tarptautinėje teisėje, t. y. ar ekstrateritorialaus poveikio teisės aktą įgyvendinti siekianti šalis turi pagrindą tai padaryti pagal tarptautines sutartis, konvencijas, reglamentus bei kitus teisės šaltinius. Jei toks išplėstas teritorinis taikymas būtų nustatytas be jokio teisinio pagrindo, tikėtina, kad šalis (aptariamam atveju – duomenų valdytojas ir duomenų tvarkytojas) galėtų paprasčiausiai jo nesilaikyti bei ginčyti tokio plataus teritorinio taikymo teisėtumą, bei, pavyzdžiui, užfiksavus galimus duomenų apsaugos teisės pažeidimus, nepateikti ES duomenų apsaugos institucijų reikalaujamos informacijos, reikalingos kruopščiam bei tiksliam tyrimui atlikti (duomenų valdytojams bei duomenų tvarkytojams galimybė ginčyti reglamento taikymo ne Europos Sąjungos šalims teisėtumą gali būti palanki net ir dėl taikomų baudų dydžio⁶⁹).

⁶⁹ Bendrajame duomenų apsaugos reglamente nustatytos duomenų valdytojams ar tvarkytojams taikomos iki 10 mln. Eurų (arba 2 proc. bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė) baudos už 83 str. 4 d. išvardytų nuostatų pažeidimus, taip pat iki 20 mln. (4 proc. bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė) baudos už 83 str. 5 d. išvardytų nuostatų pažeidimus. Plačiau: 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 82-83.

Kita vertus, vertinant pagrindus, kuriais remiantis toks platus teritorinis taikymas įgyvendinamas, svarbu tai, kokią sritį atitinkamas teisės aktas reglamentuoja. Asmens duomenų apsauga yra vertinama kaip viena prigimtinių žmogaus teisių, taip pat kaip teisės į privatumą koncepcija, ginama tiek tarptautiniais teisės aktais (kaip, pavyzdžiui, Visuotinės žmogaus teisių deklaracijos), tiek nacionaliniais teisės aktais (kaip antai Lietuvos Respublikos Konstitucijos). Daugumos valstybių nacionalinėje teisėje įtvirtinti duomenų apsaugos principai bei nustatytas teisės į duomenų privatumą reikšmingumas (dalyje valstybių – kaip konstitucinė žmogaus teisė⁷⁰), ragina organizacijas, dėl kurių veiklos jos patenką į Bendrojo duomenų apsaugos reglamento taikymo sritį, vadovautis Reglamento nuostatomis bei numatytas taisykles įgyvendinti savo privatumo politikoje. Ne veltui literatūroje išskiriamas ieškinio „moralinis“ pagrindas – jei ieškinys negali būti pagrįstas visuomenės morale, šaliai pavojinga jį pareikšti, tačiau kai ieškinys pareiškiamas pagrįstai siekiant nepažeisti visuomenės moralės principų, atsakovui, kuriam ieškinys ar skundas pareikštas, pavojinga jį ignoruoti⁷¹. Dan Jerker B Svantesson teigimu, vertinant „jurisdikciją peržengiančio“ (ekstrateritorialaus) ieškinio pagrįstumą, reikia pripažinti, kad tokie ieškiniai yra, jei ne būtinybė, tai mažų mažiausiai pasekmė veiklos, kuri atliekama duomenis perduodant tarp kelių skirtingų valstybių⁷². Visgi, galima teigti, kad tinkamas Bendrojo duomenų apsaugos reglamento įgyvendinimas priklauso tiek nuo jo teritorinio taikymo teisėtumo, tiek nuo galimybės pagrįsti ieškinio reikalavimus galimai kilsiančiame ginče.

Kita vertus, galima būtų teigti, kad reikalavimas ne ES bendrovėms, siekiančioms gauti pelno iš veiklos, nukreiptos į Europos Sąjungos rinką, laikytis Europos Sąjungos teisės aktų, saugančių duomenų subjektus nuo piktnaudžiavimo disponavimu jų asmens duomenimis, yra pagrįstas. Tačiau tam tikros taisyklės, kaip teigia Dan Jerker B Svantesson, yra perteklinė administracinė našta, kaip, pavyzdžiui, ne ES organizacijai, turinčiai itin ribotą sąveiką su Europos Sąjungos duomenų subjektais, įtvirtintas reikalavimas įgyvendinti reglamento nustatytas administracines priemones, kaip antai duomenų apsaugos pareigūno paskyrimą⁷³. Tokių priemonių įgyvendinimas įmonėms gali brangiai kainuoti, todėl tokių privalomų priemonių taikymas ne ES bendrovei, turinčiai ribotą sąveiką su Europos Sąjungos gyventojais, galėtų būti laikomas neproporcingu, todėl

⁷⁰ Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, Nr. 33-1014 (1992-11-30).

⁷¹ SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, Vol. 5, No. 4, 2015, p. 233 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/5/4/226/2404462?redirectedFrom=fulltext>>.

⁷² *Ibid.*, p. 227.

⁷³ *Ibid.*

suprantama, jog tam tikros bendrovės, įsisteigusios už ES ribų, šių reikalavimų gali nepaisyti. Kita vertus, reikalavimą įgyvendinti tokias tinkamai duomenų apsaugai reikalingas priemones galima laikyti pagrįstomis ir proporcingomis, kai šie reikalavimai nustatomi įmonėms, kurios aktyviai veikia Europos Sąjungos rinkoje. Kitu atveju toks reguliavimas kenktų viso Reglamento patikimumui⁷⁴.

Tiesa, įdomu tai, kad nors vis dar diskutuojama, ar įgyvendintos galutinės Reglamento versijos normos dėl teritorinio taikymo įgyvendinimo yra teisiškai pagrįstos, pirminės 2012 m. pasiūlytos versijos normos dėl teritorinio taikymo atrodė žymiai kontraversiškesnės. 2012 m. pasiūlyta versija numatė, kad Europos Sąjungoje gyvenantys asmenys galės remtis Reglamento normomis net tada, kai bus išvykę į ne ES šalis. Vadinas, duomenų apsaugos teisės nuostatos, įtvirtintos Reglamentu, būtų „sekusios“ paskui Europos Sąjungos gyventojus, šiems keliaujant po pasaulį. Pavyzdžiui, Europos Sąjungos piliečiui ar kitam asmeniui, turinčiam gyvenamąją vietą Europos Sąjungoje, nukeliavus į Australiją ir sudarius sutartį su vietine bendrove, iš tos sutarties atsirandanti veikla, susijusi su duomenų subjekto informacijos rinkimu turėtų būti reglamentuota ES teisės aktais. Toks teritorinis taikymas teiktų neadekvačią pirmenybę Europos Sąjungos duomenų subjektams ir būtų vargiai įgyvendinamas⁷⁵.

Verta atkreipti dėmesį į tai, kad tikėtina, jog daugeliu atveju ne ES bendrovės gali savanoriškai pakoreguoti savo privatumo politiką tam, kad bendrovės vidaus taisyklės atitiktų Bendrajame duomenų apsaugos reglamente nustatytus duomenų apsaugos principus, be jokių priverstinių priemonių. Pagrindinė to priežastis – siekis nepakenkti įmonės reputacijai. Ne ES bendrovei atsisakius veikti Europos Sąjungoje pagal joje nustatytus duomenų apsaugos standartus, gali kilti klausimas, ar tikrai ne ES įsteigta bendrovė sugebės užtikrinti tinkamą asmens duomenų apsaugą. Pastebima, kad, Europos Sąjungos Teisingumo Teismui priėmus sprendimą *Google Spain* byloje, greita *Google* reakcija ir veikimas atitinkamai pagal sprendime išdėstytas išvadas, tam tikra prasme apsaugojo *Google* nuo žalos bendrovės reputacijai, galėjusios kilti dėl neprisiimtos atsakomybės ar vengiant veikti pagal ES numatytus duomenų apsaugos standartus⁷⁶. Būtent dėl siekio išsaugoti gerą bendrovės įvaizdį, ne ES veikiantiems duomenų valdytojams ir tvarkytojams siūloma imtis savarankiškų ir aktyvių veiksmų duomenų apsaugos srityje –

⁷⁴ SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, Vol. 5, No. 4, 2015, p. 233 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/5/4/226/2404462?redirectedFrom=fulltext>>.

⁷⁵ *Ibid.*, p. 230.

⁷⁶ Slaughter and May. New rules, wider reach: the extra-territorial scope of the GDPR. 2016 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <<https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf>>.

Reglamentu siekiama skatinti įmones įsteigti su duomenų apsauga susijusius bendrovės organus, prižiūrinčius įmonės veiklą duomenų tvarkymo ar valdymo veikloje bei užtikrinančius tinkamą bendrajame duomenų apsaugos reglamente nustatytų normų įgyvendinimą.

Dar viena norma, padedanti užtikrinti, kad Bendrojo duomenų apsaugos reglamento 3 str. įtvirtintos taisyklės dėl teritorinio Reglamento taikymo bus įgyvendintos, yra Reglamento nuostatos dėl sąlygų, keliamų duomenų perdavimui į trečiąsias valstybes.

Bendrojo duomenų apsaugos reglamento IV skyriuje aptariamos sąlygos bei principai, kurių privalu laikytis norint perduoti ES duomenų subjektų duomenis į ne ES šalis. Pagrindinis principas, nurodomas Reglamento IV skyriuje – trečiosios šalies prievolė užtikrinti, kad ES duomenų subjektų informacijos perdavimui bus keliami Bendrajame duomenų apsaugos reglamente įtvirtinti duomenų apsaugos standartai⁷⁷.

Bendrojo duomenų apsaugos reglamento IV skyriuje taip pat nurodomi du būdai, taikomi duomenų perdavimui:

1. duomenų perdavimas remiantis sprendimu dėl tinkamumo;
2. duomenų perdavimas taikant tinkamas apsaugos priemones.

Pirmuoju atveju, Europos Komisijai priėmus sprendimą, jog tam tikra trečioji valstybė ar teritorija užtikrina tinkamo lygio duomenų apsaugą (pavyzdžiui, nacionalinės teisės aktais), kurie atitinka Europos Sąjungos keliamus reikalavimus duomenų apsaugai, ES duomenų subjektų duomenys gali būti perduodami šiai trečiajai šaliai be jokių papildomų reikalavimų. Tokios situacijos pavyzdys – šiame darbe jau minėtas Kanados atvejis. 2001 m. gruodžio 20 d. sprendimu Europos Komisija nustatė, kad, taikant Direktyvos 25 str. 2 dalį, Kanada yra laikoma užtikrinančia tinkamą gavėjams Europos Sąjungos valstybių perduodamų asmens duomenų apsaugos lygį pagal Kanados Asmens duomenų apsaugos ir elektroninių dokumentų įstatymą⁷⁸. Vertindama apsaugos lygio tinkamumą, Europos Komisija atsižvelgia į trečiojoje valstybėje galiojančius teisės aktus, tų aktų įgyvendinimą, taip pat į teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms ir kt.⁷⁹ Be to, Europos Komisija įvertina ir tai, ar trečiojoje šalyje veikia tam tikros

⁷⁷ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁷⁸ Europos Bendrijų Komisija. 2001 m. gruodžio 20 d. sprendimas 2002/2/EB dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB. [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32002D0002&from=en>>.

⁷⁹ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

nepriklausomos institucijos, kurių tikslas yra užtikrinti tinkamą duomenų apsaugos lygį, bei tų institucijų veiklos veiksmingumą⁸⁰. Taip pat trečiosios šalies priimtus tarptautinius įsipareigojimus pasirašytomis dvišalėmis ar daugiašalėmis sutartimis, kiek tie įsipareigojimai susiję su duomenų apsauga⁸¹. Tiesa, priėmusi sprendimą dėl trečiosios šalies tinkamumo, Europos Komisija toliau reguliariai atlieka vertinimą taikydama tuos pačius tinkamumo kriterijus, siekdama užtikrinti, kad neatsirado papildomų veiksmų, dėl kurių trečioji šalis, anksčiau paskelbta tinkama, nebegalėtų užtikrinti tinkamos duomenų apsaugos kriterijų (Reglamento 45 str. 4 d.).

Antruoju atveju duomenų perdavimas galimas tais atvejais, kai trečioji šalis įsipareigoja taikyti papildomas apsaugos priemones, kuriomis būtų užtikrinamas tinkamas duomenų perdavimo saugumas. Tai reiškia, kad trečioji šalis turi Europos Komisijos nurodytomis priemonėmis pašalinti spragas, dėl kurių ne ES valstybėje taikomi duomenų apsaugos standartai neatitinka ES teisės aktuose nurodytų duomenų apsaugos principų bei taisyklių⁸². Kaip ir pirmuoju atveju, taip ir šiuo Europos Komisija taiko nuoseklumo užtikrinimo mechanizmą⁸³.

Šias Europos Sąjungos nustatytas taisykles galima laikyti papildomu garantu, užtikrinančiu, kad ES duomenų subjektų asmeninė informacija nebus perduodama nepatikimiems duomenų valdytojams ar duomenų tvarkytojams. Galima teigti, kad tais atvejais, kai duomenų valdytojas ar duomenų tvarkytojas, neįsisteigęs ES, vengia laikytis Reglamento nuostatų, tokiu atveju duomenų perdavimas toms trečiosioms šalims yra negalimas.

Vadinasi, galima išskirti kelias esmines reglamento įgyvendinimo problemas teritoriniu aspektu. Visų pirma, vertintinas Bendrojo duomenų apsaugos reglamento plataus teritorinio taikymo teisėtumas bei pagrįstumas. Antra, net jei Reglamento ekstrateritorialaus taikymo principas pripažįstamas turinčiu teisinį pagrindą, ne ES esantys duomenų valdytojai ar duomenų tvarkytojai, turintys ribotą sąsają su ES duomenų subjektais, gali nesiimti Reglamente nustatytų priemonių (kaip antai duomenų apsaugos pareigūno paskyrimo), kurios būtų laikomos perteklinėmis. Nesiėmus kai kurių priemonių, visapusiškas ir nuoseklus reglamento įgyvendinimas mažai tikėtinas.

⁸⁰ *Ibid.*

⁸¹ 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*, p. 1-88.

⁸² *Ibid.*

⁸³ *Ibid.*

3. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TERITORINIS TAIKYMAS INTERNETO KONTEKSTE

Viena iš Bendrojo duomenų apsaugos reglamento priėmimo prielaidų – technologijų, įvairaus pobūdžio ryšio priemonių pažanga, kurios lemia ir valstybių sienų svarbos mažėjimą. Skaitmeninėje erdvėje tarsi „nykstant“ visoms valstybių sienoms, kartu nyksta ir tos virtualios erdvės reglamentavimui skirtų teisės aktų ribos. Technologijoms tobulėjant, tampa vis paprasčiau keistis duomenimis „per atstumą“ neperžengiant vienos šalies ribų, sunkiai rastume sritį, kurioje vienu ar kitu būdu įvairaus pobūdžio asmens duomenys nebūtų kaupiami skaitmeninėje erdvėje. Europos Komisijos teigimu, pasitikėjimo internetine aplinka stiprinimas yra ekonomikos augimo pagrindas, o vartotojai, nepasitikintys šia aplinka, vengia pirkti internetu ir naudotis naujomis paslaugomis – tai galėtų nulėmti inovatyvaus naudojimosi naujomis technologijomis tendencijos sulėtėjimą. Būtent todėl Europos Sąjungos institucijos savo darbotvarkėje didelį vaidmenį skiria asmens duomenų apsaugai⁸⁴. Be to, duomenų rinkimo, kaupimo bei perdavimo mastai sparčiai didėja ir tokia informacija paprastai nėra perduodama paties asmens, tačiau surinkta kitų asmenų⁸⁵ ar net automatizuotai, pavyzdžiui, naudojant „slapukus“ (angl. *cookies*)⁸⁶ ar tam tikrus algoritmus, apie kuriuos duomenų subjektas gali net nežinoti. Todėl, būtent dėl kylančių sunkumų reguliuojant duomenų srautus skaitmeninėje erdvėje, virtuali grėsmė yra įvardijama kaip vienas didžiausių pavojų, kylančių duomenų apsaugai.

Europos Sąjunga, vykdydama ES valstybėse narėse esančių asmenų duomenų priežiūrą ir kontrolę bei siekdama tinkamo asmens teisės į duomenų privatumą įgyvendinimo, prisiima pareigą apsaugoti šiuos duomenis ir virtualioje interneto erdvėje – tai įrodo ne tik su duomenų apsauga internete susijusių teisės šaltinių kūrimas (kaip antai 2002 m. liepos 12 d. Direktyva dėl privatumo ir elektroninių ryšių (2002/58/EB) ir jos pakeitimai, 2016 m. liepos 6 d. direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti ir kt.), tačiau ir Europos Sąjungos Teisingumo Teismo praktika (*Google Spain* byla), o dabar dar ir

⁸⁴ 2012 m. sausio 25 d. Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52012PC0011>>.

⁸⁵ BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 2016, Vol. 6, Issue 2, p. 77 [interaktyvus; žiūrėta 2020 m. kovo 14 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article/6/2/77/2404469>>.

⁸⁶ Slapukai (angl. *cookies*) – tai duomenų rinkiniai, registruojami internauto kompiuteryje tuo metu, kai jis naršo interneto svetainėje

Bendrasis duomenų apsaugos reglamentas. Anot Europos duomenų apsaugos priežiūros pareigūno Giovanni Buttarelli, Bendrasis duomenų apsaugos reglamentas yra, nors ir ne idealus, tačiau iki šiol pats ambicingiausias siekis apsaugoti dabartinės kartos asmens duomenis skaitmeninėje erdvėje⁸⁷. Reglamentas turi globalią reikšmę dėl siekio riboti bei kontroliuoti duomenų judėjimą tarp ES valstybių narių bei trečiųjų šalių, tiesiogiai reguliuojant net ir ne Europos Sąjungos duomenų valdytojų ar duomenų tvarkytojų veiklą asmens duomenų apsaugos kontekste⁸⁸.

Asmens duomenys dažnai išskiriami kaip „valiuta“, turinti didelę vertę ekonomikoje. Tokios kompanijos kaip *Google*, *Facebook*, *Twitter*, kurių veikla yra susijusi tiek su asmenų informacijos kaupimu, tiek su reklama, veikia asmens duomenimis paremtos ekonomikos pagrindu, o jų veikla atskleidžia duomenų rinkimo, kaupimo, analizavimo reikšmingumą. Duomenų ekonomika iškelia pagrindinį iššūkį asmens duomenų apsaugai bei asmenų teisei į privatumą – tai rizika, kylanti individo galimybei kontroliuoti savo „skaitmeninę tapatybę“ bei internete atsidūrusių duomenų judėjimą⁸⁹. Nors tam tikra prasme dalies bendrovių pelno gavimas iš asmens duomenų gali būti laikomas asmens privatumo pažeidimu, nėra teisinio pagrindo uždrausti tokias veiklas. Kita vertus, kompanijoms, ypač veikiančioms skaitmeninėje erdvėje, taikomi griežti reikalavimai siekiant užtikrinti duomenų subjektų teisę į informacijos privatumą.

Dažnai duomenų subjektų informacija renkama automatizuotais būdais. Automatizuotos priemonės – tai paprastai tokios priemonės, kurios veikia dėka technologijų ir kurioms žmogaus pagalbos nereikia (vienas tokių pavyzdžių gali būti slapukų naudojimas, t. y. automatizuotas informacijos, tokios kaip IP adresas, duomenų subjekto naršymo įpročiai ir kt. rinkimas). Bendrojo duomenų apsaugos reglamento 22 straipsnis reglamentuoja automatizuotą atskirų sprendimų priėmimą, įskaitant profiliavimą, Reglamentui įsigaliojus, privaloma gauti asmens, kurio duomenis ketinama rinkti, sutikimą dėl tokių veiksmų atlikimo. Slapukų naudojimui turi būti duodamas aiškus duomenų subjekto sutikimas aktyviais veiksmais (sutikimas pagal nutylėjimą nėra galimas). Taip pat asmeniui turi būti suteikiama informacija apie tai, koku tikslu renkami jo duomenys ir kiek

⁸⁷ BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 2016, Vol. 6, Issue 2, p. 77 [interaktyvus; žiūrėta 2020 m. kovo 14 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article/6/2/77/2404469>>.

⁸⁸ CHRISTOPHER Kuner, ir kt. The GDPR as a chance to break down borders. *International Data Privacy Law*, Vol. 7, Issue 4, 2017, p. 231 [interaktyvus; žiūrėta 2020 m. kovo 9 d.]. Prieiga per internetą: <<https://doi.org/10.1093/idpl/ix023>>.

⁸⁹ COLANGELO, Giuseppe, MAGGIOLINO, Mariateresa. Data accumulation and the privacy– antitrust interface: insights from the Facebook case. *International Data Privacy Law*, 2018, Vol. 8, No. 3 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/8/3/224/5198967>>.

laiko jie bus saugomi. Tokią pareigą gauti aiškų sutikimą patvirtina ir Europos Sąjungos Teisingumo Teismo praktika - po Vokietijos Aukščiausiojo Federalinio Teismo prašymo pateikti prejudicinį sprendimą, ESTT didžioji kolegija priėmė sprendimą byloje *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH*⁹⁰, kuriuo nurodė, kad asmuo turi sutikti, jog jo įrenginyje būtų įdiegti bei naudojami slapukai bei pabrėžė, kad toks sutikimas privalo būti duodamas aktyviais veiksmais⁹¹. Tai reiškia, kad tais atvejais, kai sutikimas su slapukų naudojimu yra iš anksto pažymėtas, neįmanoma objektyviai nustatyti, ar asmuo, nepanaikindamas varnelės prie tariamo sutikimo, iš tikrųjų sutiko, kad būtų tvarkomi jo asmens duomenys. Be to, Europos Sąjungos Teisingumo Teismo teigimu, internetinės svetainės naudotojams turi būti suteikiama aiški informacija apie tai, kaip veikia naudojami slapukai bei kokios pasekmės duodamo sutikimo naudoti slapukus. Tiesa, slapukų naudojimą, kaip tam tikrų interneto naudotojų įpročių stebėjimą galima vertinti Reglamento 3 str. 2 d. 2 punkto aspektu – slapukų naudojimas gali būti prilyginamas interneto vartotojų, kaip duomenų subjektų, elgesio stebėsenos procesui. Vadinasi, ne ES bendrovė, kaip duomenų valdytojas ar duomenų tvarkytojas, savo internetinėje svetainėje naudojanti slapukus ir jų pagalba gaunanti ES esančių duomenų subjektų duomenis, yra atskaitinga Europos Sąjungai dėl tokios savo vykdomos veiklos, t. y. jos veiklai, susijusiai su disponavimu ES duomenų subjektų informacija, yra taikomos Bendrojo duomenų apsaugos reglamento nuostatos.

Bendrojo duomenų apsaugos reglamento 3 straipsnio 2 dalis turi ypatingai didelę reikšmę nustatant, ar tam tikroje skaitmeninėje erdvėje renkami duomenys gali būti saugomi Reglamento nuostatų ne tik tais atvejais, kai duomenys renkami automatizuotomis priemonėmis. Spartėjant pasaulio globalizacijai, skirtingų valstybių rinka vis mažiau kontroliuojama sienų – prekės bei paslaugos laisvai keliauja ne tik „fiziškai“, tačiau ir skaitmeninėje erdvėje. Norint įsigyti tam tikrą prekę ar paslaugą užtenka apsilankyti įmonės internetinėje svetainėje ir, pateikus reikalingus duomenis, įsigyti paslaugą ar prekę. Tinkamos duomenų apsaugos vertinimo aspektu reikšmingiausia prekės ar paslaugos

⁹⁰ Ginčas tarp Vokietijos Konkurencijos Tarybos bei kompiuterinius žaidimus internetu siūlančios bendrovės Planet49 GmbH kilo po to, kai minėtoji bendrovė, 2013 m. organizavo loteriją. Norintys dalyvauti loterijoje asmenys turėjo užpildyti registracijos formą, kurioje taip pat buvo pateiktos dvi nuorodos su žymimaisiais langeliais, kurių vienas, dėl slapukų naudojimo, jau buvo iš anksto pažymėtas, taip galimai siekiant gauti dalyvaujančių interneto vartotojų sutikimą dėl slapukų naudojimo. Vokietijos Konkurencijos Taryba iškėlė klausimą dėl tokių veiksmų teisėtumo. Plačiau: Europos Sąjungos Teisingumo Teismas. 2019 m. spalio 1 d. sprendimas *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH* byloje, Nr. C-673/17.

⁹¹ Europos Sąjungos Teisingumo Teismas. 2019 m. spalio 1 d. sprendimas *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH* byloje, Nr. C-673/17.

įsigijimo proceso dalis – asmens duomenų pateikimas. Įsigijimo metu reikalaujama pateikti informacija, tokia kaip vardas, pavardė, elektroninio pašto adresas ar telefono numeris bei banko sąskaitos duomenys yra asmens duomenys, todėl, net jei ES esantis asmuo prekes ar paslaugas perka iš trečiųjų, ne ES esančių, bendrovių, pastarosios tampa ES duomenų subjektų informacijos rinkėjais, t. y. duomenų valdytojais bei duomenų tvarkytojais, nes siūlomos prekės ar paslaugos pasiekia ES rinką. Vadinasi, Reglamento 3 straipsnyje įtvirtintos nuostatos dėl veiklos, nukreiptos į ES duomenų subjektus ir jų duomenų rinkimą, padeda reguliuoti asmens informacijos judėjimą skaitmeninėje erdvėje tiek tarp Europos Sąjungos valstybių narių, tiek tarp ES šalių bei organizacijų ar bendrovių, esančių už Europos Sąjungos ribų.

Verta atkreipti dėmesį į tai, kad Reglamentas tvarko teisinius konkrečiai asmeninių duomenų teisinius klausimus, tačiau, duomenis tvarkant automatizuotai, sunku nubrėžti aiškią ribą tarp asmeninių ir ne asmeninių duomenų. Nuolatinis duomenų analizės sistemų bei algoritmų tobulėjimas palengvina duomenų rinkinių susiejimą, t. y. iš tam tikrų tariamai ne asmeninių duomenų rinkimo galimai gaunamą asmeninę informaciją⁹². Vadinasi, Reglamentas, nors ir tam tikra dalimi apriboja asmens duomenų gavimą automatizuotomis priemonėmis (pavyzdžiui, įpareigojant duomenų valdytojus bei duomenų tvarkytojus pirmiausia gauti asmens, kurio duomenys renkami, sutikimą), tačiau toks ribojimas gali būti ne visada įgyvendinamas – visų pirma dėl to, kad sunku sureguliuoti duomenų judėjimą bei atpažinti, kada skaitmeninėje erdvėje dideliais mastais renkami ne asmens duomenys suteikia tam tikrą asmeninę informaciją apie duomenų subjektą, taip leisdamas duomenų valdytojui bei tvarkytojui sugauti prieigą prie bent dalies asmeninių duomenų.

Kaip jau minėta, Direktyvos nuostatos dėl teritorinio taikymo rėmėsi į buveinės vietos kriterijų, todėl su internetu bei technologijų pažanga atsiradusi galimybė duomenis tvarkyti per atstumą suteikė galimybę išvengti Direktyvos taikymo duomenis tvarkant už Europos Sąjungos ribų. Kita vertus, jau aptarta Reglamente įtvirtinta nuostata dėl veiklos kriterijaus (Bendrojo duomenų apsaugos reglamento 3 str. 1 ir 2 dalys) yra labai svarbi siekiant apsaugoti asmens duomenis šiais disponuojant skaitmeninėje erdvėje – panaikintas buveinės kriterijus ir įtvirtintas veiklos, nukreiptos į ES duomenų subjektus, kriterijus nulemia skaitmeninėmis priemonėmis duomenis renkančių duomenų valdytojų ir tvarkytojų atsakomybę Reglamento nuostatų atžvilgiu. Būtent todėl naujų teritorinio taikymo nuostatų galima teigti, kad su Bendrojo duomenų apsaugos reglamento priėmimu

⁹² FINCK, Michèle, PALLAS, Frank. They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, Vol. 0, No. 0, 2020 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz026/5802594?searchresult=1>>.

Europos Sąjunga žengė didelį žingsnį link griežtesnės asmens duomenų apsaugos. Kita vertus, Europos Sąjunga yra pasirengusi dar labiau patobulinti asmens duomenų apsaugą internetinėje erdvėje – Europos Sąjungos iniciatyva priimti E. Privatumo reglamentą, kuris padėtų sukurti išsamią ES duomenų apsaugos ir ryšių konfidencialumo sistemą, veiktų kartu su Reglamentu bei leistų pasiekti dar didesnę duomenų apsaugos lygį skaitmeninėje erdvėje.

Darytina išvada, kad Bendrojo duomenų apsaugos reglamento nuostatos dėl teritorinio taikymo (Reglamento 3 straipsnis) padeda sureguliuoti ne tik duomenų judėjimą tarp ES valstybių narių bei trečiųjų šalių apskritai, tačiau ir asmens duomenų judėjimą skaitmeninėje erdvėje – tokiu būdu Europos Sąjunga užtikrina, kad ES esančių asmenų duomenys, kad ir kokių formatu pateikti, renkami ar tvarkomi bebūtų, bus tinkamai apsaugoti.

IŠVADOS

1. Kalbant apie duomenų apsaugos teisės raidą Europos Sąjungoje, daroma išvada, kad Bendrasis duomenų apsaugos reglamentas yra pirmasis ES duomenų apsaugos srityje veikiantis teisės aktas, įtvirtinęs platų teritorinio taikymo modelį (ekstrateritorialumo principas), nors tam tikra dalimi ekstrateritorialų poveikį turintys teisės aktai, susiję su duomenų apsauga, jau anksčiau buvo įgyvendinti keliuose kitose pasaulio valstybėse, kaip antai Singapūre, Australijoje, Jungtinėse Amerikos Valstijose ir kt. Taip pat verta atkreipti dėmesį, kad reglamentas, nors ir laikomas pagrindiniu šaltiniu Europos Sąjungos duomenų apsaugos srityje, tačiau veikia ne vienas – šalia veikia bei tam tikrais atvejais reglamentą papildo ir galiojančios Europos Sąjungos direktyvos, susijusios su asmens duomenų apsauga, bei duomenų apsaugai aktualios tarptautinės sutartys. Vadinasi, vertinant ar taikant Reglamento nuostatas, svarbu kartu vertinti ir kitus su duomenų apsaugos teise susijusius teisės šaltinius.
2. Vienas didžiausių Reglamento ir Direktyvos skirtumų - normose dėl teritorinės taikymo srities nustatyti kriterijai – iki reglamento įsigaliojimo ES duomenų apsaugos teisės reguliavimas buvo taikomas pagal asmens (tiek fizinio, tiek juridinio), atsakingo už duomenų tvarkymą, įsisteigimo vietos kriterijų. Tuo tarpu Bendrojo duomenų apsaugos reglamento nuostatose ypatingai pabrėžiama ne teritorijos, tačiau veiklos kriterijaus svarba.
3. Bendrojo duomenų apsaugos reglamento ypatingas požymis yra jo taikymas tiek tiems duomenų valdytojams ir duomenų tvarkytojams, kurie yra įsisteigę Europos Sąjungoje bei turi buveinę ES, tiek tiems, kurie vizinės buveinės ES teritorijoje neturi, tačiau jų veikla yra nukreipta į ES esančius asmenis bei jų duomenis.
4. Bendrojo duomenų apsaugos reglamento 3 str. numatytų nuostatų, raktinių žodžių bei kriterijų (pavyzdžiui, buveinės, į ES duomenų subjektą nukreiptos veiklos, stabilios struktūros ir kt.) vienodas interpretavimas bei supratimas yra esminis siekis norint suvienodinti skirtingų Europos Sąjungos valstybių narių vykdomą Reglamento įgyvendinimą. Europos duomenų apsaugos valdyba Gairėse dėl Reglamento teritorinio taikymo detaliai paaiškina kiekvieną kartinę reglamento 3 str. normą bei sąvoką ir pabrėžia pagrindinius principus bei sąlygas, reikalingas tam, kad reglamentas būtų laikomas galiojančiu tam tikroje teritorijoje, taip padėdama suvienodinti reglamento taikymą skirtingose valstybėse narėse.
5. Esminės Reglamento įgyvendinimo problemos teritoriniu aspektu - visų pirma, tai Bendrojo duomenų apsaugos reglamento plataus teritorinio taikymo teisėtumas bei

pagrįstumas. Antra, ne ES esantiems duomenų valdytojams ar duomenų tvarkytojams, turintiems ribotą sąsają su ES duomenų subjektais Reglamente nustatytos galimai perteklinės priemonės (kaip antai duomenų apsaugos pareigūno paskyrimo). Nesiėmus kai kurių priemonių, visapusiškas ir nuoseklus reglamento įgyvendinimas mažai tikėtinas.

6. Europos Sąjunga užtikrina, kad ES esančių asmenų duomenys, kad ir koku formatu pateikti, renkami ar tvarkomi bebūtų, bus tinkamai apsaugoti. Tai užtikrina Bendrojo duomenų apsaugos reglamento nuostatos dėl teritorinio taikymo (Reglamento 3 straipsnis), kurios padeda sureguliuoti duomenų judėjimą tarp ES valstybių narių bei trečiųjų šalių net ir skaitmeninėje erdvėje.

ŠALTINIŲ SĄRAŠAS

1. Tarptautinės sutartys

- 1.1. 1948 m. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*, 2006, Nr. 68-2497.
- 1.2. 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. *Valstybės žinios*, 2001, Nr. 32-1059.
- 1.3. Europos Taryba. 2018 m. spalio 10 d. Protokolas, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, TAR, 2020-02-25, Nr. 4015 [interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/d8e8a420c89811e9a56df936f065a619?jfwid=w5ecs1kuh>>.
- 1.4. EU-U.S. Privacy Shield Framework [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://www.privacyshield.gov/EU-US-Framework>>.
- 1.5. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441). [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02000D0520-20000825>>.

2. Europos Sąjungos teisės aktai

- 2.1. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas.
- 2.2. Sutarties dėl Europos Sąjungos veikimo suvestinė redakcija. Europos Sąjungos oficialusis leidinys, C 326, 2012, [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=OJ:C:2012:326:TOC>>.
- 2.3. 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OL L 119*.

- 2.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. *OJ L 119*, 2016, p. 89–131 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680>>.

3. Nacionaliniai Lietuvos Respublikos teisės aktai

- 3.1. Lietuvos Respublikos Konstitucija. *Valstybės žinios, Valstybės Žinios*, 1992, Nr. 33-1014 (1992-11-30)
- 3.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. TAR, 2018-07-11, Nr. 11733.

4. Nacionaliniai užsienio šalių teisės aktai

- 4.1. Privacy Act 1988, No. 119, 1988, Australia [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://www.legislation.gov.au/Details/C2020C00025>>.
- 4.2. Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), Republic of Singapore Government Gazette, 2012 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://sso.agc.gov.sg/Act/PDPA2012#legis>>.
- 4.3. Vaikų privatumo internete saugos aktas (angl. *Children's Online Privacy Protection Rule ("COPPA")*), 2018 [interaktyvus, žiūrėta 2020 m. kovo 18 d.]. prieiga per internetą: <<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>>.

5. Specialioji literatūra

- 5.1. ALBRECH, Jan Philipp. How the GDPR Will Change the World. *European Data Protection Law Review*, Vol. 2, issue 3, 2016 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://edpl.lexxion.eu/article/edpl/2016/3/4>>.
- 5.2. BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 2016, Vol. 6, Issue 2, p. 77-78

- [interaktyvus; žiūrėta 2020 m. kovo 14 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article/6/2/77/2404469>>.
- 5.3. CHEN, Jiahong. How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation. *International Data Privacy Law*, Vol. 6, No. 4, 2016 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/6/4/310/2567746?redirectedFrom=fulltext>>.
 - 5.4. CHRISTOPHER Kuner, ir kt. The GDPR as a chance to break down borders. *International Data Privacy Law*, Vol. 7, Issue 4, 2017 [interaktyvus; žiūrėta 2020 m. kovo 9 d.]. Prieiga per internetą: <<https://doi.org/10.1093/idpl/ix023>>.
 - 5.5. COLANGELO, Giuseppe, MAGGIOLINO, Mariateresa. Data accumulation and the privacy– antitrust interface: insights from the Facebook case. *International Data Privacy Law*, Vol. 8, No. 3, 2018 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/8/3/224/5198967>>.
 - 5.6. FINCK, Michèle, PALLAS, Frank. They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, Vol. 0, No. 0, 2020 [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz026/5802594?searchresult=1>>.
 - 5.7. GAJDA, Amy. *What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to „The Right to Privacy“* [interaktyvus; žiūrėta 2020 m. kovo 6 d.]. Prieiga per internetą: <<http://educationnewyork.com/files/SSRN-id1026680privacyorigin.pdf>>.
 - 5.8. GREENLEAF, Graham. Countries with Data Privacy Laws – By Year 1973-2016 (Tables), 2017 [interaktyvus; žiūrėta 2020 m. vasario 28 d.]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2996139>.
 - 5.9. SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, Vol. 5, No. 4, 2015, p. 226-234 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <<https://academic.oup.com/idpl/article-abstract/5/4/226/2404462?redirectedFrom=fulltext>>.
 - 5.10. ZALESKIS, Julius. *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*. Vilnius: Registrų centras, 2019
 - 5.11. ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, p.45-54.

5.12. ŽIOBIENĖ, Edita. Informacijos apie privatų asmens gyvenimą apsauga. *Konstitucinė jurisprudencija*. 2008, Nr. 3 (11).

6. Teismų praktika

- 6.1. Europos Žmogaus Teisių Teismas. 2008 m. gruodžio 2 d. sprendimas *K. U. prieš Suomiją* byloje, Nr. 2872/02.
- 6.2. Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* C-131/12, ECLI:EU:C:2014:317.
- 6.3. Europos Sąjungos Teisingumo Teismas. 2015 m. spalio 6 d. sprendimas *Maximillian Schrems prieš Data Protection Commissioner* byloje, C-362/14.
- 6.4. Europos Sąjungos Teisingumo Teismas. 2019 m. spalio 1 d. sprendimas *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH* byloje, Nr. C-673/17.

7. Soft Law šaltiniai

- 7.1. Europos Taryba. 509 Rekomendacija dėl žmogaus teisių ir šiuolaikinių bei mokslinių technologinių Pokyčių (angl. *Recommendation 509 (1968). Human rights and modern scientific and technological Developments*), 1968 [interaktyvus; žiūrėta 2020 m. vasario 27 d.]. Prieiga per internetą: <<http://semanticpace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbnceG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNDU0NiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRClBVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTEONTQ2>>
- 7.2. Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*, 2014, p. 16, [interaktyvus; žiūrėta 2020 m. kovo 1 d.]. Prieiga per internetą: <http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0020.03/DOC_2>.
- 7.3. ES 29 str. darbo grupė. *Nuomonė Nr. 8/2010 dėl taikytinos teisės* (WP 179) 2010 m. [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf>.

- 7.4. ES 29 str. darbo grupė. *Atnaujinta nuomonė Nr. 8/2010 dėl taikytinos teisės, atsižvelgiant į ESTT sprendimą byloje Google Spain*, 2015 m. [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640614>.
- 7.5. Europos Bendrijų Komisija. 2001 m. gruodžio 20 d. sprendimas 2002/2/EB dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB. [interaktyvus; žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32002D0002&from=en>>.
- 7.6. ES ir JAV “Privatumo skydo” gairėse. [interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <http://ec.europa.eu/newsroom/document.cfm?doc_id=47770>.
- 7.7. 2012 m. sausio 25 d. Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52012PC0011>>
- 7.8. Europos duomenų apsaugos valdyba (EDAV) (angl. European data protection board). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation, 2019, [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_lt>.

8. Kiti šaltiniai

- 8.1. Council of Europe. Personal data protection: Uruguay becomes first non-European state to accede to “Convention 108”. 2013 m. [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <<https://www.coe.int/en/web/portal/-/personal-data-protection-uruguay-becomes-first-non-european-state-to-accede-to-convention-108>>.
- 8.2. Council of Europe. Newsroom: Argentina, 54th Party to Convention 108. 2019 m. [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <<https://www.coe.int/en/web/data-protection/-/argentina-54th-party-to-convention-108>>.

- 8.3. Council of Europe. Newsroom: *Welcome to Mexico, 53rd Party to Convention 108*. 2018 m. [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <<https://www.coe.int/en/web/data-protection/-/welcome-to-mexico-53rd-party-to-convention-108>>.
- 8.4. Council of Europe. News 2016: *International data protection conference: Mauritius joins "Convention 108"*. 2016 m. [interaktyvus; žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <https://www.coe.int/en/web/portal/news-2016/-/asset_publisher/StEVosr24HJ2/content/mauritius-joins-the-data-protection-convention-convention-108->>.
- 8.5. Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. spaudos konferencija Nr. 117/15. *The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid*. [interaktyvus; žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>>.
- 8.6. Europos Komisija. Kokios taisyklės taikomos, jeigu mano organizacija perduoda duomenis už ES ribų? [interaktyvus; žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_lt>.
- 8.7. Slaughter and May. New rules, wider reach: the extra-territorial scope of the GDPR. 2016 [interaktyvus; žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <<https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf>>.

SANTRAUKA

Informacinių technologijų plėtra ir spartėjanti pasaulio globalizacija nulemia duomenų apsaugos bei asmenų privatumo reikšmės didėjimą, duomenų apsauga tampa vis aktualiau nagrinėjama tema. Didžiosios bendrovės, organizacijos, veikiančios skaitmeninėje erdvėje, gavo prieigą prie ypatingai didelio kiekio duomenų, o disponavimas asmens duomenimis vyksta ne tik tikslingai, tačiau ir kaip naudojimosi skaitmeninėmis paslaugomis šalutinis poveikis – tai kelia ypatingą pavojų asmens teisei į duomenų privatumą. Dėl spartėjančios globalizacijos ir visuomenės pažangos būtina nuolatos tobulinti jau sukurtus aktualius teisės aktus bei ieškoti naujų, inovatyvių ir galimai susidariusias teisės spragas panaikinančių sprendimų. Būtent dėl šios priežasties, siekiant reformuoti dabartinę duomenų apsaugos teisę, buvo priimtas Bendrasis duomenų apsaugos reglamentas, kurio viena didžiausių naujovių – plačiai interpretuojamos nuostatos dėl teritorinio taikymo. Siekiant visapusiškai išnagrinėti šią naujovę Europos Sąjungos duomenų apsaugos teisės srityje, darbas padalintas į kelias dalis.

Pirmoje dalyje apžvelgiama duomenų apsaugos teisės raida, anksčiau priimti duomenų apsaugos srityje veikę teisės aktai bei jų taikymas teritoriniu aspektu. Taip pat pasikeitimai, įvykę po Bendrojo duomenų apsaugos reglamento įsigaliojimo.

Antroje dalyje apžvelgiamos iš Reglamento nuostatų dėl teritorinio taikymo kylančios interpretavimo problemos bei galimi šių normų įgyvendinimo sunkumai, o trečioje dalyje apžvelgiama duomenų apsaugos problematika interneto kontekste.

SUMMARY

The development of technologies and fast globalization process of the world determine the growing importance of data protection and personal privacy. Data protection became increasingly important topic. Large companies, organizations operating in the digital space have gained access to a particularly large amount of data, and the disposal of personal data is not only targeted, but is also known as a side effect of digital services' usage, which poses a particular threat to the individual's right to privacy of data. Accelerating globalization and progress of society necessitate the continuous improvement of existing legislation and the search for new, innovative solutions that solves potential legal gaps and issues. For this reason, the General Data Protection Regulation (GDPR) has been adopted in order to reform the current data protection law. One of the major innovations of GDPR is the broad interpretation of the provisions on territorial approach. In order to fully examine this innovation in the field of data protection law in European Union, this work has been divided into several parts.

The first part provides an overview of the development of data protection law, previous data protection legislation and its territorial application as well as major changes implemented by the General Data Protection Regulation.

The second part reviews the problems of interpretation arising from the provisions of the Regulation which are related to territorial application and possible difficulties in the implementation of these norms. The third part reviews the issues of data protection in the context of the Internet.