www.mruni.eu

Edgaras MARKEVIČIUS

DAKTARO DISERTACIJA

# ASMENS DUOMENŲ PERDAVIMO ELEKTRONINĖJE ERDVĖJE TARP EUROPOS SĄJUNGOS IR JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINĖS PROBLEMOS

SOCIALINIAI MOKSLAI,
TEISĖ (S 001)
VILNIUS, 2022

MYKOLO ROMERIO UNIVERSITETAS

MYKOLO ROMERIO UNIVERSITETAS

**Edgaras Markevičius**

# ASMENS DUOMENŲ PERDAVIMO ELEKTRONINĖJE ERDVĖJE TARP EUROPOS SĄJUNGOS IR JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINĖS PROBLEMOS

Daktaro disertacija
Socialiniai mokslai, teisė (S 001)

Vilnius, 2022

Daktaro disertacija rengta 2015–2021 metais Mykolo Romerio universitete, ginama Mykolo Romerio universitete pagal Mykolo Romerio universitetui ir Vytauto Didžiojo universitetui Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

*Mokslinis vadovas:*
prof. dr. Darijus Beinoravičius (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

# TURINYS

## Pagrindinės santrumpos

| | |
|---|---|
| **BDAR** | 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 |
| **CŽV** | Centrinė Žvalgybos Valdyba (angl. *Central Intelligence Agency, CIA*) |
| **Direktyva 95/46** | 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 |
| **Direktyva 2016/680** | 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 |
| **Direktyva 2006/24** | 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB |
| **FTB** | Federalinis Tyrimų Biuras (angl. *Federal Bureau of Investigations, FBI*) |
| **JAV** | Jungtinės Amerikos Valstijos |
| **Kt.** | Kita |
| ***Safe Harbour* susitarimas** | 2000 m. liepos 26 d. Europos Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „Safe Harbor“ susitarimo privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų “Dažnai užduodamų klausimų” |
| ***Privacy Shield* susitarimas** | 2016 m. liepos 12 d. Europos Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB |

| | |
|---|---|
| **Sutartis dėl Europos Sąjungos veikimo** | 1957 m. kovo 25 d. Sutartis dėl Europos Sąjungos veikimo, OL C 326 |
| **PNR** | Lėktuvų keleivių duomenys (angl. *Passenger name records*, *PNR*) |
| **t. t.** | Taip toliau |
| **t. y.** | Tai yra |
| **Žr.** | Žiūrėti |

# ĮVADAS

**Temos aktualumas**. Pastarieji dešimtmečiai pasižymėjo itin sparčia technologijų pažanga, kuri pakeitė daugybę kasdienio gyvenimo sričių. Viena iš labiausiai paveiktų sričių apima asmenų socialinį gyvenimą – bendro darbo, tarpusavio bendravimo priemones ir įpročius. Šiuo metu tapo įprasta rengti ne *gyvus* sutikimus, o telekonferencijas; skambinti nebe GSM ryšiu, o susisiekti videoryšiu (pvz., programėlių *Viber, Messenger, FaceTime* pagalba) ir pan.

Ši technologijų pažanga lemia vis didėjantį asmenų, įmonių ir organizacijų elektroninių ryšių tinklų ir debesų technologijų naudojimą paslaugoms teikti, įrašams kaupti ir tvarkyti būtent elektroninėje erdvėje. Vis platesnis šių ryšių naudojimas suteikia beprecedentę galimybę sistemingai rinkti ir naudoti įvairius duomenis (tame tarpe ir asmens duomenis) skirtingiems tikslams. Technologijų pagalba kaupiama bei apdorojama informacija ir duomenys naudojami ne tik fizinių ir juridinių asmenų poreikių patenkinimo tikslais, tačiau ir įvairiais kitais tikslais.

Itin plačiai paplitusio asmens duomenų kaupimo ir naudojimo kontekste teisine prasme probleminis tampa asmens teisės į privatų gyvenimą užtikrinimas. Nors asmenims ir yra laiduojama teisė į privatumą, tačiau negalima ignoruoti kitų interesų, kurių patenkinimui šie duomenys gali būti naudojami. Šie interesai apima tiek privačius, tiek visuomeninius prioritetus – sunkių nusikaltimų (pavyzdžiui, terorizmo, narkotikų gamybos ir gabenimo, prekybos žmonėmis etc.) prevenciją ir ikiteisminio tyrimo vykdymą, valstybių nacionalinio saugumo užtikrinimą, viešojo administravimo paslaugų teikimą elektroninėmis priemonėmis etc.

Teisinės analizės prasme sudėtingas klausimas visuomet yra susijęs su dviejų interesų – asmens teisės į privatumą bei visuomenės kolektyvinio saugumo intereso – konkurencija bei proporcingo šių interesų balanso nustatymu. Šis klausimas tampa dar sudėtingesniu, kai privatumo apsaugą reikia derinti ne tik konkuruojančių interesų atžvilgiu, tačiau ir tarp skirtingų teisinių sistemų, kuriose tiek privatumo, tiek visuomenės kolektyvinis saugumo interesai yra suprantami ir aiškinami skirtingai.

Europos Sąjungoje teisė į privatumą ir asmens duomenų apsaugą yra saugoma Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 str. nuostatomis bei BDAR reguliavimu. Kadangi teisė į privatumą ir asmens duomenų apsaugą yra laiduojama visiems asmenims, Europos Sąjunga turi užtikrinti, kad šios teisės būtų įgyvendinamos tvarkant asmens duomenis ne tik jos teritorijoje, bet ir perduodant už jos ribų.

Transatlantiniai duomenų srautai tarp Europos Sąjungos ir JAV yra greičiausi ir didžiausi pasaulyje, bei sudaro daugiau nei pusę Europos duomenų srautų ir apie pusę JAV duomenų srautų, todėl JAV ir Europos Sąjunga yra ne tik vienos didžiausių rinkų, bet ir svarbiausios komercinės partnerės skaitmeninių paslaugų srityje[1]. Dėl to teisine ir faktine prasme aktualiausios teisės į privatumą apsaugos problemos kyla iš asmens duomenų perdavimo būtent tarp Europos Sąjungos ir JAV teisinių sistemų.

Teisės į privatumą apsaugos apimties klausimas, jį derinant su valstybės nacionalinio saugumo ar nusikaltimų prevencijos interesais, nėra lengvai nustatomas net ir vienos teisinės sistemos kontekste. Tai patvirtina daugybė ginčų ir didelio atgarsio sulaukę sprendimai, kuriuos priėmė Europos Sąjungos Teisingumo Teismas nagrinėdamas bylas dėl Europos Sąjungos pagrindinių teisių chartijos taikymo, Europos Žmogaus Teisių Teismas – dėl Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos taikymo teisės į privatumą ir asmens duomenų apsaugą srityse.

Autoriaus vertinimu, ši teisės į privatumą apsaugos apimties nustatymo užduotis reikšmingai pasunkėja, kai jį būtina suderinti ne vienos, o kelių teisinių sistemų atžvilgiu. Teisės į privatumą apsauga pagal Europos Sąjungos iškeltą aukštą apsaugos standartą yra sudėtingai suderinama su JAV teisine sistema bei privatumo samprata joje, pirmiausiai, dėl pamatinių JAV teisinės sistemos skirtumų su Europos Sąjungos teisine sistema. Pavyzdžiui, JAV teisėje taikoma trečiosios šalies doktrina[2], pagal kurią, fiziniai asmenys neturi pagrįsto intereso į teisės į privatumą apsaugą tų duomenų atžvilgiu, kuriuos valdo ne jie patys, o tretieji asmenys (pavyzdžiui, bankai, elektroninių ryšių paslaugų teikėjai ir pan.). Todėl JAV teisėsaugos ar žvalgybos institucijos gali gauti šiuos duomenis iš esmės netaikant jokių apsaugos priemonių. Taip pat, pagal JAV Aukščiausiojo Teismo *Clapper* byloje suformuotą praktiką, asmenys negali kreiptis į teismą dėl privatumo apsaugos, jei jie negali įrodyti, kad stebėjimas jų atžvilgiu buvo taikytas[3]. Atsižvelgiant į tai, kad stebėjimo priemonės taikomos slaptai, apie tai nepranešant asmenims (kurių atžvilgiu jos yra taikomos), toks suformuotas precedentas padarė reikšmingą neigiamą poveikį asmenų galimybei ginti savo pažeidžiamas teises.

Be reikšmingų pamatinių požiūrio į teisės į privatumą apimties ir teisinių sis-

---

1 Daniel S. Hamilton ir Joseph P. Quinlan, *The Transatlantic Economy 2020: Annual Survey Of Jobs, Trade And Investment Between The United States And Europe* (2020), 8.

2 Simon Stern, „The Third-Party Doctrine and the Third Person“, *New Criminal Law Review* 16, 3 (2013): 101.

3 „Clapper v. Amnesty International“, CaseText, žiūrėta 2021 m. rugpjūčio 5 d., https://casetext.com/case/clapper-v-amnesty-intl-usa-7.

temų skirtumų tarp Europos Sąjungos ir JAV, svarbūs ir kiti veiksniai, susiję su faktine teisės į privatumą apsaugą JAV. JAV prezidentų Bušo ir Obamos administracijos vykdė prieštaringas nacionalinio saugumo programas, įskaitant tikslinių nužudymų, kankinimų ir asmenų stebėjimo srityse, kurių slaptumas atėmė iš visuomenės galimybę sužinoti tuos veiksmus ir taikomas priemones[4]. Dalį šių taikomų priemonių, jų taikymo mąstą ir reikšmę 2013 m. atskleidė pranešėjas (angl. whistle blower) Edvardas Snoudenas[5], tokiais savo veiksmais pasėjęs nepasitikėjimo sėklą privatumo apsauga JAV teisinėje sistemoje ir faktiškai taikomų stebėjimo priemonių teisėtumu. Šį nepasitikėjimo aspektą puikiai iliustruoja ir Lietuvos teisės doktrinoje pateikiami kritiniai privatumo apsaugos JAV teisinėje sistemoje vertinimai, kad „JAV vykdomas masinis asmens duomenų rinkimas elektroninėje erdvėje yra analogiškas XIII a. galiojusiai antikonstitucine pripažintai teisei Karūnos įgaliotiems asmenims bent kada įsibrauti į bent kurio iš Didžiosios Britanijos valdose esančio asmens namus“[6].

Šios teisinės sistemos sąveikauja, kai asmens duomenys yra perduodami tarp skirtingų subjektų, priklausančių šioms teisinėms sistemoms. Asmens duomenų perdavimas iš Europos Sąjungos subjektams į trečiąsias šalis reguliuojamas BDAR V skyriuje. Jame prioriteto tvarka yra įtvirtinti skirtingi asmens duomenų perdavimo pagrindai iš Europos Sąjungos į trečiąsias šalis (ar tarptautinėms organizacijoms): Europos Komisijos sprendimas dėl tinkamumo, duomenų valdytojo ar tvarkytojo taikomos tinkamos apsaugos priemonės, nukrypti leidžiančios nuostatos. Visi šie duomenų perdavimo pagrindai taikomi siekiant to paties tikslo – užtikrinti, kad nebūtų pakenkta BDAR garantuojamam fizinių asmenų apsaugos lygiui.

Kadangi JAV yra trečioji šalis, remiantis BDAR 45 str. teisiniu reguliavimu, paprasčiausias bei palankiausias sprendimas sureguliuoti asmens duomenų perdavimą tarp Europos Sąjungos ir JAV yra Europos Komisijos sprendimas dėl trečiojoje šalyje (t. y. JAV) užtikrinamos tinkamo lygio privatumo apsaugos.

Europos Komisija tokį sprendimą JAV atžvilgiu (t. y. *Safe Harbour* susitarimą) priėmė 2000-aisiais metais. Dėl Edvardo Snoudeno 2013 m. atskleistų JAV vykdomų stebėjimo programų kilo ne tik daug pasipiktinimo, tačiau ir teisinių ginčų. *Safe Harbo-*

---

4 Sudha N. Setty, *National Security Secrecy: Comparative Effects on Democracy and the Rule of Law* (Cambridge University Press, 2017), 3.

5 Jordi Pujol, „Is This the End of Privacy? Snowden and the Power of Conscience“, *Church, Communication and Culture* 5, 1 (2020): 140-44.

6 Sigutė Stankevičiūtė, „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas“ (daktaro disertacija, Mykolo Romerio Universitetas, 2020), 113 psl., prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka: 9.

*ur* susitarimo teisėtumą ir pagrįstumą 2015 m. vertino Europos Sąjungos Teisingumo Teismas ir jį panaikino[7].

Europos Sąjungos Teisingumo Teismui panaikinus *Safe Harbour* susitarimą, skubiai buvo pradėtos derybos dėl galimo naujo susitarimo sudarymo, kurios baigėsi sėkmingai, 2016 m. sudarius *Privacy Shield* susitarimą. Tačiau laikas parodė, jog *Privacy Shield* susitarimas taip pat turėjo reikšmingų trūkumų, nes Europos Sąjungos Teisingumo Teismas 2020 m. jį taip pat panaikino, kaip neužtikrinantį adekvačios teisės į privatumą apsaugos JAV teisinėje sistemoje[8].

Tokiu būdu, atsižvelgiant į kategoriškas Europos Sąjungos Teisingumo Teismo padarytas išvadas apie teisės į privatumą apsaugos JAV teisinėje sistemoje nepakankamumą, lyginant su Europos Sąjungos teisinėje sistemoje garantuojamu privatumo apsaugos lygiu, vėl atsirado teisinis neapibrėžtumas dėl asmens duomenų perdavimo teisinio pagrindų taikymo. Minėto Europos Sąjungos Teisingumo Teismo sprendimo Schrems II byloje reikšmė yra itin didelė, kadangi joje yra konstatuojami pamatiniai privautmo apsaugos JAV teisinėje sistemoje trūkumai, kurių, autoriaus vertinimu, duomenų valdytojai ar tvarkytojai negali ištaisyti. Tai yra trūkumai, susiję su teisėsaugos institucijų prieiga prie JAV tvarkomų asmens duomenų. Todėl naudojimasis kitu BDAR V skyriuje įtvirtintu asmens duomenų perdavimo teisiniu pagrindu, tikėtina, siekiant perduoti duomenis iš Europos Sąjungos į JAV taip pat yra negalimas, nes bendras asmens duomenų perdavimo principas bei tikslas (užtikrinti, kad nebūtų pakenkta BDAR garantuojamam fizinių asmenų apsaugos lygiui) negalės būti įgyvendintas dėl konstatuotų JAV teisinės sistemos asmens duomenų apsaugos trūkumų.

Kitas Europos Sąjungos Teisingumo Teismo sprendime konstatuotas, tačiau iš esmės neplėtotas argumentas yra tas, kad išimtis dėl BDAR netaikymo, siejant su valstybių narių nacionalinio saugumo interesų apsauga, netaikoma trečiųjų šalių atžvilgiu. T. y. priešingai nei Europos Sąjungos valstybės narės, trečiosios šalys (įskaitant ir JAV), su kuriais sudaromi duomenų perdavimo susitarimai, privalo taikyti BDAR reguliavimą asmens duomenų, gaunamų iš Europos Sąjungos, tvarkymui, net kai jis atliekamas ir nacionalinio saugumo interesais. Ši Europos Sąjungos Teisingumo Teismo pozicija

---

[7] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3390590.

[8] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=8508220193825AFC3D98FABEA15645EC?text=&docid=228677&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3350436.

ne tik dėl asmens duomenų perdavimo besiderančius subjektus (pvz., Europos Sąjungą ir JAV) pastato į nelygiavertes pozicijas, tačiau ir sukuria reikšmingas kliūtis sėkmingam susitarimo dėl asmens duomenų perdavimo pasiekimui, nes trečiąją šalį *de facto* reikalauja atsisakyti savo nacionalinio saugumo apsaugos interesų įgyvendinimo iš Europos Sąjungos gaunamų asmens duomenų atžvilgiu.

Dėl nurodytų aplinkybių, šiame darbe siekiama išanalizuoti asmens duomenų perdavimo elektroninėje erdvėje problemas, sąveikaujant Europos Sąjungos ir JAV teisinėms sistemoms – galimų asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinių pagrindų sąlygas, atsižvelgiant į nacionalinio saugumo interesų apsaugą ir Europos Sąjungos Teisingumo Teismo suformuotą praktiką šiuo aspektu.

**Ištirtumas.** Bendrąja prasme, asmens teisė į privatumą yra populiari tema tiek tarp Lietuvos, tiek tarp užsienio teisės mokslininkų. Teisės doktrinoje teigiama, kad mokslininkų susidomėjimui asmens duomenų apsauga žvalgybos ir teisėsaugos srityje įtaką daro į viešumą nutekinama informacija apie asmens duomenų rinkimo mastus ir jų (ne)teisėtą panaudojimą[9]. Tokiai prielaidai turi būti pritariama, atsižvelgiant į teisinio reguliavimo ir teisės doktrinos pokytį asmens duomenų apsaugos srityje po Edvardo Snoudeno 2013 m. nutekintos informacijos apie JAV taikomas asmenų stebėjimo programas.

Viena iš populiarių teisės į privatumą tyrimo sričių buvo asmens santykis su valstybe asmens duomenų apsaugos srityje. Mokslininkai koncentravosi į Edvardo Snoudeno atskleistą informaciją apie valstybių taikomas stebėjimo priemones ir jų santykį su teise į privatumą[10].

Kita populiari mokslinių tyrimų sritis atsivėrė po Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje, kuriuo buvo panaikintas *Safe Harbour* susitarimas. Tuomet teisės į privatumą apsaugos skirtingų teisės sistemų sąveikoje tema įgavo platesnį susidomėjimą. Pasirodė mokslininkų darbai apie duomenų perdavimo iš Europos

[9] Stankevičiūtė, *supra note*, 6: 10.

[10] Zygmunt Bauman ir kt., „After Snowden: Rethinking the Impact of Surveillance“, *International Political Sociology* 8, 2 (2014): 122; Kevin Macnish, „Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World“, *Journal of Applied Philosophy* 35, 2 (2016): 417-32; Debora Halbert ir Stefan Larsson, „By Policy or Design? Privacy in the US in a Post-Snowden World“, *Journal of Law, Technology and Public Policy* 1, 2 (2015): 1; Sören Preibusch, „Privacy Behaviors after Snowden“, *Communications of the ACM* 58, 5 (2015): 48-55.; David Lyon, „Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique“, *Big Data & Society* 1, 2 (2014): 205395171454186; Nora Ni Loideain, „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era“, *Media and Communication (Lisboa)* 3, 2 (2015): 53-62.; Maria Helen Murphy, „The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe?“, *Information & Communications Technology Law* 23, 3 (2014): 192-219.

Sąjungos į JAV galimybes ir teisėtumą[11].

Tarp šios srities tyrimų paminėtinos reikšmingi tyrimai, skirtos sisteminei asmens duomenų perdavimo tarp Europos Sąjungos ir JAV teisinei problematikai analizuoti[12]. Douglas M. Mcleod ir Dhavan V. Shah knygoje *News Frames and National Security. Covering Big Brother*[13] analizuojama įtampos tarp nacionalinio saugumo ir pilietinių laisvių įtampos prigimtis ir esmė. Ji padėjo tiksliau identifikuoti nacionalinio saugumo prigimtį, sampratą ir prasmę JAV teisinėje sistemoje. Svantesson, Dan Jerker B., ir Dariusz Kloza knygoje *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*[14] analizuojamas tarpvalstybinis duomenų srautų režimas, kuris grindžiamas Europos Sąjungos teisinio reguliavimo priemonėmis, tokiomis kaip BDAR, *Safe Harbour* ir daro įtaką kasdieniam duomenų apdorojimui abipus Atlanto bei kaip jie riboja duomenų operacijų apimtį. Ši knyga padėjo suprasti skirtingą Europos ir JAV teisės mokslininkų požiūrį į asmens duomenų perdavimo teisinį reguliavimą vadovaujantis *Safe Harbour* susitarimu, kuris neteko galios 2015 m. Patrick Birkinshaw knyga *Freedom of Information: The Law, the Practice, and the Ideal*[15] suteikė platesnę galimybę suprasti istorinį vyriausybių santykį su duomenų apsauga ir jų prigimtinį interesą prieigai prie asmens duomenų, kaip būtiną reikalavimą, užtikrinant visuomenės saugumą. James Carr ir Patricia Bellia knygoje *The Law of Electronic Surveillance*[16] apžvelgiamas teisinis JAV federalinio lygio asmens duomenų rinkimo el. erdvėje reglamentavimas. Ši knyga padėjo suprasti, kaip JAV teisinėje sistemoje veikia stebėjimo priemonių taikymo mechanizmas.

Tarp Lietuvos teisės mokslininkų teisės į privatumo apsaugą analizė taip pat laikytina populiaria tema. Tarp aktualių darbų pirmiausiai paminėtina šio tyrimo ren-

---

[11] Christina Lam, „Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner", *Boston College International and Comparative Law Review* 40, 3 (2017): 1.

[12] David C. Gray ir Stephen E. Henderson, *The Cambridge Handbook of Surveillance Law* (Cambridge University Press, 2017); Dan Jerker B. Svantesson ir Dariusz Kloza. *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, 2017); Russell A. Miller, *Privacy and Power* (Cambridge: Cambridge University Press, 2017); Austin Sarat, *A World without Privacy* (New York: Cambridge University Press, 2014).

[13] Douglas M. McLeod ir Dhavan V Shah, „News Frames and National Security", *Communication, Society and Politics* (Cambridge University Press, 2014).

[14] Dan Jerker B. Svantesson ir Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, 2017).

[15] Patrick Birkinshaw, *Freedom of Information: The Law, the Practice, and the Ideal. Fourth ed.* (Cambridge University Press, 2010).

[16] James Carr ir Patricia Bellia, *The Law of Electronic Surveillance*, 2017-2 Ed., 1 dalis, (Clark Boardman Callaghan, 2017).

gimo metu apginta S. Stankevičiūtės disertacija tema „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas“[17]. Joje mokslininkė analizuoja bendrosios ir kontinentinės teisės tradicijų šalių bei supranacionalinio lygmens asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo ypatumus dėl teisės į asmens duomenų apsaugą užtikrinimo. Šiame darbe, kaip ir apžvalginėje studijoje apie privatumo apsaugą JAV[18] bei aukščiau minėtose knygose, pateikiama detali JAV teisinio reguliavimo analizė apie asmens duomenų rinkimą teisėsaugos ir žvalgybos tikslais. Tačiau atsižvelgiant į šio tyrimo temą, joje nėra jokios analizės, nukreiptos į šių skritingų teisinių sistemų sąveikos problemas privatumo apsaugos kontekste bei galimus jų sprendimo būdus. Paulius Pakutinskas savo disertacijoje „Elektroninių komunikacijų teisinio reguliavimo modeliai“[19] analizavo elektroninių komunikacijų teisinio reguliavimo modelius, tačiau šio tyrimo atlikimui ji tiesiogiai nėra aktuali, nes joje taip pat neatskleidžiama skritingų teisinių sistemų sąveikos problema. Juliaus Zaleskio monografijoje „Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“[20] analizuojamas bendrasis BDAR teisinis reguliavimas kaip teisinės taisyklės, skirtos apsaugoti asmenis nuo pavojų, kuriuos kelia duomenų tvarkymas. J. Zaleskio monografijoje aiškinamas BDAR reguliavimas, tačiau nėra analizuojama BDAR sąveikos su JAV teisine sistema problematika. Ilonos Petraitytės 2013 m. apgintoje disertacijoje[21] nagrinėti asmens duomenų apsaugos principai, tačiau ji prarado reikšmingą dalį aktualumo 2018 m., įsigaliojus BDAR ir iš esmės gali būti naudinga atliekant istorinę ir lyginamąją asmens duomenų apsaugos reguliavimo analizę.

Kita šiam tyrimui iš dalies aktuali Lietuvos mokslininkų analizuota asmens duomenų apsaugos teisės sritis, susijusi su teisės į privatumą ribojimais, atliekamais baudžiamojo persekiojimo metu (ikiteisminio tyrimo ar kriminalinės žvalgybos priemonių taikymo metu). Pirmiausiai šiuo aspektu paminėtinas Aurelijaus Gutausko

---

17 Stankevičiūtė, *supra note*, 6: 2 skyrius.

18 Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens“, European Parliament, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.

19 Paulius Pakutinskas, „Elektroninių Komunikacijų Teisinio Reguliavimo Modeliai“ (daktaro disertacija, Mykolo Romerio Universitetas, 2009), Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.

20 Julius Zaleskis, *Europos Sąjungos Bendrasis Duomenų Apsaugos Reglamentas Ir Asmens Duomenų Apsaugos Teisė: Monografija* (Vilnius: Registrų Centras, 2019).

21 Ilona Petraitytė, „Asmens Duomenų Teisinės Apsaugos Principai“ (daktaro disertacija, Vilniaus Universitetas, 2013), Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.

mokslinis straipsnis, kuriame analizuojama Lietuvos Aukščiausiojo Teismo praktika, susijusi kriminalinės žvalgybos naudojamomis priemonės ir teisėtu jų skverbimusi į privatų žmogaus gyvenimą[22]. Jame pateikiamos įžvalgos, aktualios kriminalinės žvalgybos taikymo priemonių atveju, tačiau šio tyrimo objektas yra privatumo apsaugos problemos skritingų teisinių sistemų sąveikoje, ypač atsižvelgiant į aktualią problematiką dėl skirtingų valstybių nacionalinio saugumo interesų užtikrinimo. Susijusia tema pasisakė ir Rima Ažubalytė, kuri savo moksliniame straipsnyje analizavo Baudžiamojo proceso kodekso ir Kriminalinės žvalgybos įstatymo spragas dėl asmens duomenų rinkimo el. erdvėje, išryškėjusias Lietuvos teismų praktikoje[23]. Taip pat savo darbuose Gintaras Goda nagrinėjo procesinių prievartos priemonių (tame tarpe ir susijusių su teisės į privatumą ribojimu) Baudžiamojo proceso kodekse sampratas[24], kurios nėra teisioginis šio tyrimo objektas.

Nemažai Lietuvos mokslininkų darbų skirta pamatinių sampratų, susijusių su teise į privatumą ir asmens duomenų apsauga, analizei ir aiškinimui. Mindaugas Civilka ir Lina Šlapimaitė straipsnyje nagrinėjo asmens duomenų sampratą elektroninėje erdvėje[25], Ilona Petraityte savo straipsnyje analizavo asmens duomenų apsaugos sampratą ir santykį su teise į privatumą[26]. Keli Lietuvos mokslininkų darbai[27] nukreipti į teisinius aspektus, susijusius su konkrečių techninių priemonių naudojimą kriminalinės žvalgybos tikslais. Nors šie teisės į privatumą kvalifikavimo aspektai ir aktualūs, tačiau atsižvelgiant į tai, kad jie atskleisti Lietuvos teisės doktrinoje minėtuose darbuose, šiame tyrime dėl to išsamiau nėra nagrinėjami.

**Mokslinis naujumas ir reikšmė**. Šiame tyrime siekiama išanalizuoti asmens

---

[22] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas“, *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

[23] Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema“, *Jurisprudencija* 26, 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02.

[24] Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys“, *Teisė* (2000): 17-27. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija* (Vilnius: Registrų centras, 2014).

[25] Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė*, 96 (2015): 126-148.

[26] Ilona Petraitytė, „Asmens Duomenų Apsauga Ir Teisė į Privatų Gyvenimą“, *Teisė* 80 (2011): 163-74.

[27] Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“, *Teisės problemos* 1, 91 (2016): 25-51; Darius Štitilis ir Marius Laurinaitis, „IP telefonija - iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui“, *Socialinių mokslų studijos* 1 (2009): 205–221; Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas“, *Jurisprudencija : mokslo darbai* 29 (2002): 72–85; Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė* (2017): 84–99, doi:10.15388/Teise.2017.105.11114.

duomenų apsaugos elektroninėje erdvėje problemas, atsirandančias sąveikaujant skirtingoms teisinėms sistemoms. Todėl jame ne tik pateikiama Europos Sąjungos teisinėje sistemoje aktualių asmens duomenų perdavimo į kitas teisines sistemas pagrindų, įtvirtintų BDAR, analizė, tačiau ir atliekamas Europos Sąjungos bei JAV sudarytų asmens duomenų perdavimo susitarimų Safe Harbour bei Privacy Shield vertinimas, atsižvelgiant į Europos Sąjungos Teisingumo Teismo suformuotą praktiką šioje srityje bei Europos Sąjungos bei JAV teisinių sistemų reguliavimą.

Atlikdamas šį tyrimą, aktualioje Europos Sąjungos Teisingumo Teismo Schrems II byloje, autorius užčiuopė kertinį probleminį teisės į privatumą ir asmens duomenų apsaugos aspektą, susijusį su trečiosios šalies nacionalinio saugumo intereso įgyvendinimu. Remiantis Europos Sąjungos Teisingumo Teismo išaiškinimais, trečiosios šalies interesas turėti prieigą prie iš Europos Sąjungos subjektų gaunamų asmens duomenų, ginant savo nacionalinį saugumą, yra vertinamas pagal žymiai griežtesnius kriterijus, nei pačių Europos Sąjungos valstybių narių ir, autoriaus vertinimu, yra iš esmės paneigiamas.

Todėl šiame tyrime vertinami galimo naujo susitarimo tarp Europos Sąjungos ir JAV kontūrai, atsižvelgiant į Europos Sąjungos Teisingumo Teismo suformuotą praktiką minėtose bylose, ryšiumi su trečiosios šalies interesu užtikrinti savo nacionalinį saugumą.

Iš pristatytos teisės doktrinos privatumo apsaugos srityje apžvalgos, darytina išvada, kad joje dažniausiai analizuojamos temos, susijusios su (i) bendrąja teisės į privatumą ir asmens duomenų apsaugą samprata; (ii) asmens duomenų perdavimo tarp Europos Sąjungos ir JAV pagrindais; (iii) jų (ne)teisėtumu remiantis jau pasenusia Europos Sąjungos Teisingumo Teismo praktika Schrems byloje, (iv) asmens teisės į privatumą ir asmens duomenų apsaugą ribojimas ikiteisminio tyrimo priemonėmis bei keitimasis šiais duomenimis. Autoriui nepavyko rasti nė vieno mokslinio darbo, kuriame būtų analizuojami asmens duomenų perdavimo į kitą teisinę sistemą teisiniai pagrindai, atsižvelgiant į nacionalinio saugumo intereso įgyvendinimą, jo ribas ar santykį su asmenų teise į privatumą bei asmens duomenų apsaugą kitoje teisinėje sistemoje.

Atliktas tyrimas ir jo rezultatai gali būti naudingi, siekiant įvertinti Europos Sąjungos subjektų atliekamo asmens duomenų perdavimo pagrindų į JAV teisinę sistemą teisėtumą ir pagrįstumą bei atliekant galimo naujo Europos Komisijos sprendimo dėl tinkamos asmens duomenų apsaugos JAV teisinėje sistemoje užtikrinimo lyginamąją analizę.

**Tyrimo objektas**. Šios disertacijos tyrimo objektas yra asmens teisės į privatumą ir asmens duomenų apsaugą ribos elektroninėje erdvėje skirtingose teisinėse sistemose, atsižvelgiant į probleminį teisinių sistemų sąveikos aspektą – valstybių interesą užtikrinti savo nacionalinį saugumą.

**Mokslinė problema**. Disertacijos mokslinė problema formuluojama šiais klausimais:

1. Kokia yra nacionalinio saugumo samprata ir ar jis turi ribas?

2. Ar Europos Sąjungos Teisingumo Teismas sprendimais *Schrems* ir *Schrems II* bylose užkirto kelią susitarimui dėl asmens duomenų perdavimo tarp Europos Sąjungos ir kitos teisinės sistemos (tame tarpe ir JAV) sudarymo?

3. Ar remiantis proporcingumo principu galima pateisinti teisės į privatumą ir asmens duomenų apsaugą ribojimą, taikomą trečios šalies nacionalinio saugumo užtikrinimo tikslais?

4. Ar asmens duomenų perdavimas iš Europos Sąjungos į JAV gali būti laikomas teisėtu taikant standartinių duomenų apsaugos sąlygų institutą pagal BDAR 46 str., kai Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje JAV teisinį reguliavimą pripažino neužtikrinančiu adekvačios teisės į privatumą ir asmens duomenų apsaugos?

5. Kokie yra būtini pokyčiai JAV teisinėje sistemoje, susiję su asmens teisės į privatų gyvenimą ir asmens duomenų apsauga, siekiant galimo susitarimo dėl asmens duomenų perdavimo tarp Europos Sąjungos ir JAV?

**Tyrimo tikslas**. Ištirti asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinius pagrindus ir atsižvelgiant į Europos Sąjungos Teisingumo Teismo praktikoje suformuotą kritiką JAV teisinei sistemai, nustatyti, kokiomis sąlygomis asmens duomenų perdavimas į JAV galėtų būti laikomas teisėtu.

**Tyrimo uždaviniai**. Siekiant nurodyto tikslo, formuluojami tokie uždaviniai:

1. Įvertinti galimus asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinius pagrindus pagal BDAR ir išanalizuoti jų tarpusavio santykį bei priklausomybę;

2. Išanalizuoti Europos Sąjungos Teisingumo Teismo praktiką, susijusią su asmens teisės į privatumą ir asmens duomenų apsauga ir nustatyti reikšmingas privatumo apsaugos JAV teisinėje sistemoje problemas, užkertančias kelią sėkmingam asmens duomenų perdavimui iš Europos Sąjungos į JAV;

3. Išanalizuoti nacionalinio saugumo sampratą ir nustatyti galimas jos ribas pagal Lietuvos, JAV teisinį reguliavimą bei Europos Žmogaus Teisių Teismo praktiką

bylose dėl teisės į privatumą pažeidimo;

4. Identifikuoti proporcingumo principo, kaip pagrindinio teisinio testo, taikomo vertinant asmens teisės į privatumą ir asmens duomenų apsaugą ribojimų teisėtumą, kriterijus bei nustatyti, ar jį taikant gali būti išsprendžiama asmens duomenų perdavimo iš Europos Sąjungos į JAV teisėtumo problema;

5. Įvertinus pamokas iš Europos Sąjungos Teisingumo Teismo praktikos, nustatyti kokios yra galimo teisėto asmens duomenų perdavimo iš Europos Sąjungos į JAV sąlygos.

**Ginamieji teiginiai**:

1. Kai panaikinamas asmens duomenų perdavimo iš Europos Sąjungos į trečiąją šalį pagrindas, taikytas pagal BDAR V skyriaus teisinį reguliavimą, nepakitus asmens duomenų apsaugos lygiui trečiojoje šalyje, asmens duomenų perdavimas į tą pačią trečiąją šalį negali būti teisėtas remiantis kitu BDAR V skyriuje įtvirtintu teisiniu pagrindu.

2. Pagrindinis JAV teisinės sistemos trūkumas, kuris užkerta kelią JAV teisės į privatumą ir asmens duomenų apsaugos reguliavimą pripažinti adekvačiu BDAR V skyriaus prasme, yra susijęs su JAV nacionalinio saugumo intereso įgyvendinimu.

3. Asmens teisės į privatumą ir asmens duomenų apsaugą ribojimo pagrindas, susijęs su valstybės nacionalinio saugumo interesų įgyvendinimu, neturi teisiškai apibrėžtų ribų.

4. Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje netiesiogiai verčia trečiąją šalį, kuri pageidauja būti pripažinta užtikrinančia adekvatų teisės į privatumą ir asmens duomenų apsaugą lygį, atsisakyti savo nacionalinio saugumo interesų įgyvendinimo iš Europos Sąjungos gaunamų duomenų atžvilgiu.

**Metodologija.** Skirtingi mokslinių tyrimų yra naudojami ir derinami tarpusavyje, siekiant tyrimo tikslo ir uždavinių įgyvendinimo.

Duomenys tyrimui buvo renkami remiantis *mokslinės literatūros, teisinių dokumentų analizės, nestruktūruoto ekspertų interviu metodais*. Tyrimui aktualūs duomenys buvo apdorojami *naudojantis sisteminės ir loginės analizės, lingvistiniu, lyginamuoju ir istoriniais metodais*.

*Teisinių dokumentų analizės* bei *lyginamasis metodai* naudoti viso tyrimo metu. Jie turėjo reikšmingą įtaką rengiant antrąjį darbo skyrių, kuriame tiriami asmens duomenų perdavimo į trečiąsias šalis teisiniai pagrindai, įtvirtinti BDAR V skyriuje. Šių metodo taikymas leido atskleisti asmens duomenų perdavimo į trečiąsias šalis teisinių

pagrindų skirtumus, tarpusavio priklausomybę ir santykį siekiant jiems visiems suformuoto bendro taikymo tikslo.

*Istorinis tyrimo metodas* turėjo svarbų vaidmenį viso tyrimo atlikimui. Remiantis juo buvo analizuota nacionalinio saugumo sampratos kilmė ir raida JAV teisinėje sistemoje bei Europos Žmogaus Teisių Teismo praktikoje. *Lyginamasis metodas* sudarė galimybes įvertinti nacionalinio saugumo sampratos ir teisinio reglamentavimo Lietuvos, JAV teisinėse sistemose bei pagal Europos Žmogaus Teisių Teismo praktiką, skirtumus.

*Loginės, sisteminės analizės* tyrimo metodai buvo naudojami viso tyrimo metu. Remiantis jais nuosekliai buvo tiriama tyrimui aktuali medžiaga. Jie buvo labiausiai reikšmingi analizuojant Europos Sąjungos Teisingumo Teismo praktiką dėl asmens teisės į privatumą ribojimų teisėtumo bei identifikuojant proporcingumo principo, kaip pagrindinio teisinio testo, taikomo vertinant asmens teisės į privatumą ir asmens duomenų apsaugą, taikymo sąlygas ir ribas. Kartu su šiais metodais aktyviai naudotas *lingvistinis* metodas, siekiant nustatyti sąvokų skirtumus, galinčius atsirasti dėl vertinių skirtingų sampratų lietuvių ir anglų kalbomis. Šių metodų taikymo tikslas – ištirti buvusį ir esamą asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinį reglamentavimą; teisės į privatumą ribojimo pagrindų teisinį reglamentavimą Europos Sąjungoje ir JAV.

Taikant *teleologinį tyrimo metodą* analizuota ir aiškinta Europos Sąjungos Teisingumo Teismo praktika. Šis metodas naudotas siekiant įvertinti teismo suformuotų išaiškinimų svarbą, atskleisti jų prasmę bei kontekstą ir šias įžvalgas pritaikyti aktualiam teisiniam reguliavimui bei darant išvadas dėl būtinų asmens duomenų perdavimo modelio pakeitimų. Šis metodas buvo itin reikšmingas atskleidžiant Europos Sąjungos Teisingumo Teismo išaiškinimų turinį ir pagrindinę mintį.

*Mokslinės literatūros analizės metodas* naudojamas siekiant atskleisti Europos Sąjungos, JAV ir Lietuvos mokslininkų požiūrį dėl teisės į privatumą ir asmens duomenų apsaugos ribojimų teisėtumo ir jų atliktų mokslinių tyrimų rezultatus. Šio metodo taikymas leido atskleisti tarp JAV mokslininkų dominuojantį kritišką požiūrį į Europos Sąjungos Teisingumo Teismo išaiškinimus *Schrems II* byloje, suprasti jį pagrindžiančias pozicijas bei kodėl šis teismas kaltinamas dviveidiškumu.

Asmens teisės į privatumą apsauga elektroninėje erdvėje pasižymi greitais pokyčiais dėl technologinės elektroninių ryšių ir technologijų raidos. Šiuos pokyčius lemia netikėčiausi, tačiau visuomenėms itin reikšmingi įvykiai, pavyzdžiui pranešėjų (angl.

*whistle-blowers*) paviešinama informacija (Edvardo Snoudeno atveju), ar net atskirų ūkio subjektų sprendimai, darantys įtaką jų produktų ar paslaugų vartotojams visame pasaulyje (pvz., įmonės kaip *Facebook*, *Apple*, *Google* etc.). Todėl *stebėsenos* metodas taikomas siekiant tyrimo tema turėti aktualią informaciją, gebėti suprasti konkrečių sprendimų motyvus ar užsienio mokslininkų pozicijas, prognozuoti būsimus teisinio reguliavimo pokyčius arba tų pokyčių poreikį, dar nepasirodžius teisės aktų pakeitimams ar mokslininkų publikacijoms aktualiais klausimais[28].

*Nestruktūrizuoto interviu metodas* taikomas teisinio reglamentavimo problematikos, atsižvelgiant Europos Sąjungos Teisingumo Teismo išaiškinimus, nustatymui ir atskleidimui. Autorius tyrimo tema diskutavo su prof. Lietuvos Aukščiausiojo Teismo baudžiamųjų bylų skyriaus pirmininku Aurelijumi Gutausku, stažuotės Lenkijoje metu – su prof. Dorota Lis-Staranowicz, prof. Marcin Dabrowski, taip pat su kitais Varmijos ir Mazūrijos universiteto mokslininkais seminarų metu. Interviu metu visiems ekspertams buvo pateikiami nevienodi klausimai, suformuoti atsižvelgiant į kiekvieno eksperto pateiktą informaciją ir mokslinių tyrimų sritį.

[28] Pavyzdžiui, tyrimo rengimo metus stebėtos JAV mokslininko Daniel Justin Solove publikacijos, teisinis tinklaraštis *TeachPrivacy* (https://www.youtube.com/channel/UCqODltywqZCuxprcz72kc-Q), socialinio tinklo LinkedIn grupė *Schrems II – Lawful Data Transfer* ir t.t.

# 1. Asmens duomenų elektroninė erdvėje apsauga Europos Sąjungos ir Jungtinių Amerikos Valstijų teisės sistemose: samprata, raida, turinys

Asmens duomenų apsaugos ypatumai Europos Sąjungos teisės sistemoje: samprata, teisinio reguliavimo tendencijos.

Teisė į asmens duomenų apsaugą yra viena pagrindinių asmens teisių, kurios svarba ir reikšmingumas pripažįstamas skirtingose teisinėse sistemose. Tačiau Europos Sąjungos teisinėje sistemoje jai yra skiriamas ypatingas dėmesys.

Kaip ir pati teisė į asmens duomenų apsaugą, taip ir jos santykis su teise į privatumą, nėra vienareikšmiškas. Autoriaus vertinimu, teisė į asmens duomenų apsaugą gali būti susijusi su bet kuriuo teisės į privatumą aspektu, tačiau ji apima būtent duomenų apie asmens privatų gyvenimą išraiškos (pavyzdžiui, užrašų, nuotraukų ar pan.) apsaugą.

Šiuo aspektu svarbu pabrėžti, kad teisės doktrinoje taip pat sutinkamos skirtingos nuomonės dėl teisės į privatumą ir teisės į asmens duomenų apsaugą santykio. Vieni mokslininkai teigia, kad teisė į asmens duomenų apsaugą negali būti pripažįstama kaip teisės į privatumą apsaugos instrumentas[29], kiti teigia, kad teisės į asmens duomenų apsaugą apimtis yra platesnė nei teisės į privatumo apsaugą[30]. Tokia pozicija ne tik prieštarauja didelės dalies mokslininkų pateikiamiems teisės į privatumą apibrėžimams (kurie apima ir teisę į asmens duomenų apsaugą), tačiau, autoriaus vertinimu, negali būti laikoma pagrįsta interpretacija. Nors asmens duomenų apsaugos teisinis reguliavimas ir gali turėti kitų tikslų (pavyzdžiui, Europos Sąjungoje BDAR nustatomos taisyklės *inter alia* siekiant laisvo asmens duomenų judėjimo užtikrinimo[31]), tačiau asmens duomenų apsaugos taisyklių taikymo pamatinis tikslas visuomet yra asmens teisės į privatumą apsauga. Pavyzdžiui, tai tiesiogiai liudija BDAR preambulės 4 p. nuostata, kad „Šiuo reglamentu paisoma visų Chartijoje pripažintų ir Sutartyse įtvirtintų pagrindinių teisių ir laisvių bei principų, visų pirma teisės į privatų ir šeimos gyvenimą, būsto neliečiamybę

---

[29] Lee A. Bygrave, „The Place of Privacy in Data Protection Law*", University of New South Wales Law Journal* 24, 1 (2001): 282.

[30] Juliane Kokott ir Christoph Sobotta, „The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law* 3, 4 (2013): 225.

[31] „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)", 1 str., EUR-Lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679.

ir komunikacijos slaptumą, teisės į asmens duomenų apsaugą, minties, sąžinės ir religijos laisvės, saviraiškos ir informacijos laisvės, laisvės užsiimti verslu, teisės į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą ir kultūrų, religijų ir kalbų įvairovės“. Be to, nors doktrinoje teigiama, kad teisė į asmens duomenų apsaugą ir yra savarankiška pagrindinė asmens teisė, tačiau taip pat pripažįstama teigiama, kad ji kilo būtent iš asmens teisės į privatumą[32]. Todėl, autoriaus vertinimu, pažeidžiant asmens teisę į asmens duomenų apsaugą, tuo pačiu bus pažeidžiama ir jo teisė į privatų gyvenimą, tačiau ne atvirkščiai.

Kita vertus, pripažįstant teisės į asmens duomenų apsaugą ir glaudžią sąsają su asmens teise į privatumą bei pritariant doktrinoje pateikiamoms nuomonėms, kad teisė į asmens duomenų apsaugą kilo iš asmens teisės į privatumą, analizuojant teisę į asmens duomenų apsaugą, būtina atskleisti ir asmens teisės į privatumą sampratą.

Teisė į privatumą įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje[33], Europos Žmogaus Teisių Konvencijoje[34], daugumos valstybių rašytinėse konstitucijose[35] ir įstatymuose. Kaip nurodyta ankstesniame skirsnyje, šio darbo analizei reikšmingiausioje – Europos Sąjungos – teisinėje sistemoje, teisės į privatumą apsaugos sistema yra sudėtinė ir daugiasluoksnė.

Visų pirma, teisė į privatumą pripažįstama ir saugoma Europos Sąjungos pagrindinių teisių chartijos 7 str., kuriame nurodoma, kad „Kiekvienas asmuo turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas“, o 8 straipsnyje įtvirtinta, kad „Kiekvienas turi teisę į savo asmens duomenų apsaugą“. Analogiškai, asmenų teisė į asmens duomenų apsaugą yra tiesiogiai įtvirtinta ir sutarties dėl Europos Sąjungos veikimo 16 str. 1 d.[36].

Teisės į privatumą turinys ar ribos nėra aiškiai apibrėžtos. Skirtingi mokslininkai, analizuojantys skirtingas teisines sistemas, savo moksliniuose darbuose pateikia skirtingus teisės į privatumą apibrėžimus. Pavydžiui, D. Solove teigia, kad privatumas yra plati sąvoka, apimanti (be kita ko) minties laisvę, kūno valdymą, vienatvę namuose, asmeninės informacijos kontrolę, laisvę nuo stebėjimo, savo reputacijos apsaugą ir

[32] Stankevičiūtė, *supra note*, 6: 113.

[33] „Europos Sąjungos pagrindinių teisių chartija“, 7 str., EUR-Lex, žiūrėta 2021 m. rugpjūčio 11 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN.

[34] „1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, LRS, 8 str., žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.

[35] Pavyzdžiui, Lietuvos Konstitucijos 22 str., Vokietijos Pagrindinio įstatymo 10 str., Italijos Konstitucijos 15 str. ir t.t.

[36] „Sutartis dėl Europos Sąjungos veikimo“, 16 str. 1 d., Eur-Lex, žiūrėta 2021 m. rugpjūčio 11 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12012E/TXT&from=LT.

apsaugą nuo kratų ir tardymų[37]. Pagal A. Westin, privatumas yra asmenų, grupių ar institucijų reikalavimas patiems nuspręsti, kada, kaip ir kiek informacija apie juos perduodama kitiems[38]. Lietuvos teisės doktrinoje teigiama, kad privataus gyvenimo neliečiamumo sąvoka aiškinama kaip žmogaus galimybė laisvai tuoktis ir sukurti šeimą, gyventi šeimoje ar nutraukti santuoką, neformaliai bendrauti su draugais, užmegzti bei palaikyti ryšius su kitais žmonėmis, turint galimybę ugdyti ir realizuoti save kaip asmenybę[39].

Teisės į privatumą, kuri įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje, apsauga (ypač, kiek tai susiję su asmens duomenų apsauga) detalizuojama kituose Europos Sąjungos teisės aktuose. Šiuo aspektu aktualiausias yra 2018 m. įsigaliojęs BDAR, kuris tapo pirmuoju tokiu išsamiu ir visapusišku, visoje Europos Sąjungoje taikomu pagrindinių teisių į privatumą ir asmens duomenų apsaugą, instrumentu, kurio taikymo sritis[40] ir teritorija[41] yra itin plati.

Greta BDAR, specifiniai asmens duomenų apsaugos aspektai yra reguliuojami kitais teisės aktais. Pavyzdžiui, Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo (Direktyva 2016/680). Kaip nurodo jos pavadinimas, ji nustato taisykles, susijusias su fizinių asmenų apsauga teisėsaugos institucijoms tvarkant jų asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo, baudžiamojo persekiojimo ir kt. susijusiais tikslais bei užtikrina palengvintą teisėsaugos institucijų

---

37 Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2009), 2.

38 Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 7.

39 Karolis Jovaišas, „Konstitucijos II skirsnio "Žmogus ir valstybė" komentaras", *Teisės problemos* (Vilnius: Teisės institutas, 1999), 65.

40 BDAR taikomas taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis. Žr. „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)", *supra note*, 60: 2 str. 1 d.

41 BDAR taikomas asmens duomenų tvarkymui, kai asmens duomenis Sąjungoje tvarko duomenų valdytojo arba duomenų tvarkytojo buveinė, vykdydama savo veiklą, neatsižvelgiant į tai, ar duomenys tvarkomi Sąjungoje, ar ne. *Ibid*, 3 str. 1 d.

keitimąsi tokiais duomenimis[42].

Europos Parlamento ir Tarybos Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje papildo BDAR[43], siekiant apsaugoti fizinių asmenų pagrindines teises ir ypač jų teisę į privatumą, taip pat ir teisėtus juridinių asmenų interesus[44] bei nustato specialias taisykles elektroninių ryšių paslaugų teikimui, ypač susijusias su elektroninių ryšių paslaugų ir susijusių duomenų konfidencialumu (tiek fizinių, tiek juridinių asmenų)[45], neužsakytais pranešimais (angl. *spam*)[46], tinklo ir pačių elektroninių ryšių paslaugų saugumu[47], apribotu duomenų srauto ir buvimo vietos informacijos saugojimu[48], slapukų naudojimo taisykles[49] etc. Šios direktyvos tikslas buvo harmonizuoti nacionalines ryšio konfidencialumo taisykles[50], tačiau tikrovėje situacija atrodo toli nuo suderintos, valstybėms narėms skirtingai įgyvendinus direktyvą bei su iš to išplaukiančiu vienodos valstybių narių piliečių apsaugos trūkumu ir teisiniu netikrumu įmonėms, ypač veikiančioms skirtingose šalyse[51]. Šio tyrimo rengimo metu, Europos Komisija yra pateikusi pasiūlymą dėl šios direktyvos atnaujinimo ir naujo ePrivatumo reglamento priėmimo[52], tačiau jis dar nėra priimtas.

Europos Parlamento ir Tarybos direktyva (ES) 2018/1972 buvo patvirtintas Eu-

---

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“, EUR-Lex, žiūrėta 2021 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX-%3A32016L0680.

43 „Europos Parlamento ir Tarybos Direktyva 2002/58/EB 2002 m. liepos 12 d. dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), L 201, 31/07/2002“, 94, 95 str., EUR-Lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:02002L0058-20091219&from=EN.

44 *Ibid*, preambulės 12 p.

45 „Europos Parlamento ir Tarybos Direktyva 2002/58/EB 2002 m. liepos 12 d. dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), L 201, 31/07/2002“, *supra note*, 65: 5 str.

46 *Ibid,* 13 str.

47 *Ibid,* 4 str.

48 *Ibid,* 9 str.

49 *Ibid,* 5 str. 3 p.

50 *Ibid,* preambulės 8 p.

51 „Europos Komisijos ataskaita dėl viešos konsultacijos apie e-privatumo direktyvos įvertinimą ir peržiūrą“, European Commission, 3, žiūrėta 2021 m. rugpjūčio 11 d., http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40777.

52 „Proposal for an ePrivacy Regulation“, European Commission, žiūrėta 2021 m. rugpjūčio 11 d., https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

ropos elektroninių ryšių kodeksas[53] ir pakeista Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl privatumo ir elektroninių ryšių[54]. Šiuo kodeksu siekiama atnaujinti elektroninių ryšių (telekomunikacijų) tinklų, telekomunikacijų paslaugų, susijusių priemonių ir susijusių paslaugų reguliavimo taisykles, bei tokiu būdu užtikrinti vartotojams saugesnes (ypač teisių į privatumą ir asmens duomenų apsaugos kontekste) elektroninių ryšių paslaugas[55].

Teisę į privatumą taip pat saugo ir Europos Žmogaus Teisių Konvencija, kuri įtvirtinta šios konvencijos 8 str. Kadangi Europos Žmogaus Teisių Konvencija yra savarankiška tarptautinė konvencija, jos santykis su Europos Sąjungos teisine sistema nėra vienareikšmiškas. Viena vertus, ši tarptautinė konvencija yra savarankiška – jos pagrindu yra įkurtas Europos Žmogaus Teisių Teismas, į kurį gali kreiptis asmenys, kurie mano savo tesies esant pažeidžiamas konvenciją ratifikavusios šalies ir Europos Žmogaus Teisių Teismo sprendimai yra privalomi konvenciją ratifikavusioms šalims. Tačiau Europos Sąjunga turi patvirtinusi savarankišką dokumentą, kuriame yra laiduojama pagrindinių žmogaus teisių apsauga – Europos Sąjungos pagrindinių teisių chartiją.

Kita vertus, Europos Sąjungos sutarties 6 str. 2 d. nurodyta, kad Europos Sąjunga prisijungia prie Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos ir šis prisijungimas neturi įtakos sutartyse apibrėžtai Europos Sąjungos kompetencijai[56]. Autorius siekia atkreipti dėmesį, kad šių savarankiškų teisės aktų garantuojama teisės į privatumą apsauga sąveikauja sistemingai. Doktrinoje pripažįstama, kad Europos Sąjungos pagrindinių teisių chartijoje „nurodytų teisių, atitinkančių [Europos Žmogaus Teisių Konvencijos] garantuojamas teises, esmė ir taikymo sritis tokia pat kaip toje konvencijoje nustatyta“, tačiau tai nekliudo Europos Sąjungos teisėje numatyti didesnę apsaugą[57]. Atsižvelgiant į autorių pateikiamus vertinimus, kad „Teisingumo Teismui visada suvokiant, kad būtina visais atvejais įveikti EŽTT nustatytą „minimalaus aukščio

---

[53] „Europos Parlamento ir Tarybos 2018 m. gruodžio 11 d. direktyva (ES) 2018/1972 kuria nustatomas Europos elektroninių ryšių kodeksas“, EUR-Lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32018L1972&from=LT.

[54] Europos Parlamento Ir Tarybos Direktyva 2002/58/EB 2002 m. liepos 12 d. dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), *op. cit.*

[55] „Europos Parlamento ir Tarybos 2018 m. gruodžio 11 d. direktyva (ES) 2018/1972 kuria nustatomas Europos elektroninių ryšių kodeksas“, *op. cit.,* 1 str. 2 d. a) p., 3 d. b) p.

[56] „Europos Sąjungos sutartis“, EUR-Lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:LT:PDF.

[57] Skirgailė Žalimienė, *Europos Sąjungos Pagrindinių Teisių Chartijos, Kaip Individualių Teisių Gynybos Standarto, Taikymas Supra- Ir Nacionaliniu Lygmenimis: Kolektyvinė Monografija* (Vilnius: Vilniaus Universiteto Leidykla, 2019), 56.

apsaugos kartelę““[58], darytina išvada, kad Europos Žmogaus Teisių Konvencija ir Europos Žmogaus Teisių Teismo praktika bylose dėl teisės į privatumą apsaugos yra sudėtinė Europos Sąjungos teisinės sistemos dalis, kuri turi būti vertinama kaip minimalios apsaugos standartas.

Teisės į privatumą apsaugos ribos pagal Europos Žmogaus Teisių Konvenciją yra brėžiamos per Europos Žmogaus Teisių Teismo sprendimus. Vadovaujantis šio teismo praktika, privatus gyvenimas laikytinas plačia sąvoka, kurios negalima galutinai apibrėžti[59] ir ji apima fizinį ir psichologinį asmens vientisumą ir skirtingus asmens fizinės ir socialinės tapatybės aspektus[60]. Atkreiptinas dėmesys, kad pagal Europos Žmogaus Teisių Teismo praktiką, asmens teisė į duomenų apsaugą patenka į asmens teisės į privatumą apimtį ir saugoma tuo pačiu teisiniu pagrindu – Europos Žmogaus Teisių Konvencijos 8 str.[61]

Apibendrinant pateiktus argumentus apie teisės į asmens duomenų apsaugą ir asmens teisės į privatumą apsaugą Europos Sąjungos teisinėje sistemoje, darytina išvada, kad privatumas yra garantuojamas skirtingais teisės aktais, tarpusavyje sudarančiais vientisą privatumo apsaugos sistemą. Nė viename iš šių teisės aktų nepateiktas teisės į privatumą apibrėžimas, nes jis, kaip socialinė kategorija, kinta keičiantis tiek technologijoms, tiek pačioms visuomeniniams santykiams. Atsižvelgiant į tai, kad Europos Sąjungoje teisės į privatumą apsauga per pastaruosius dešimtmečius tampa vis labiau sisteminga (pavyzdžiui, patvirtinus Elektroninių ryšių kodeksą, pakeitusį kelias savarankiškas anksčiau aktualias direktyvas) ir unifikuota (vietoje Direktyvos 95/46 įsigaliojo BDAR, o šiuo metu yra svarstomas ePrivatumo reglamento projektas), darytina išvada, kad Europos Sąjungos teisinė sistema vystosi pagal tradicinei kontinentinei teisinei sistemai būdingus bruožus – teikiant prioritetą sistemingam (kodifikuotam) ir imperatyviam teisiniam reguliavimui. Todėl labiausiai tikėtina, kad tolimesniuose šio darbo skyriuose analizuojamos mokslinės problemos bei galimi jų sprendimai Europos Sąjungos teisinėje sistemoje bus pateikiami teisės aktuose, sudarančiuose dar aiškesnę (ar net vientisą) sistemą.

---

[58] *Ibid*, 64.

[59] „Europos Žmogaus Teisių Teismo 1992 m. gruodžio 16 d. sprendimas byloje Nr. 13710/88 Niemietz prieš Vokietiją“, Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-57887.

[60] „Europos Žmogaus Teisių Teismo 2018 m. rugsėjo 25 d. sprendimas byloje Nr. 76639/11 Denisov prieš Ukrainą*“,* Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-186216.

[61] „Europos Žmogaus Teisių Teismo 2017 m. birželio 27 d. sprendimas byloje Nr. 931/13 Satakunnan Markkinapörssi Oy ir Satamedia Oy prieš Suomiją*“,* Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-175121.

Asmens duomenų apsaugos Jungtinių Amerikos Valstijų teisės sistemoje ypatumai: samprata, teisinio reguliavimo tendencijos.

Kaip minėta šiame skyriuje, pripažįstant teisės į asmens duomenų apsaugos glaudžią sąsają su asmens teise į privatumą bei pritariant doktrinoje pateikiamoms nuomonėms, kad teisė į asmens duomenų apsaugą kilo iš asmens teisės į privatumą, analizuojant asmens duomenų apsaugos sampratą, būtina atskleisti ir asmens teisės į privatumą genezę.

Teisės į privatumo apsaugą pagrindas JAV teisinėje sistemoje yra Ketvirtoji JAV Konstitucijos pataisa (angl. *Fourth Amendment*). Tai yra kontraversiška, nes iš tiesų Ketvirtojoje JAV Konstitucijos pataisos tekste teisė į privatumą apskritai nėra minima:

„Žmonės turi teisę būti saugūs savo asmenyse, namuose, dokumentuose ir turte nuo nepagrįstų kratų ir konfiskavimo, negali būti pažeista ir jokie orderiai negali būti išduodami, kaip tik esant tikėtinai priežasčiai, paremtai priesaika ar patvirtinimu, ypač detaliai apibūdinant kratos vietą, asmenis ar daiktus, kuriuos reikia paimti."

Taigi, teisės į privatumą pradžia JAV teisinėje sistemoje susijusi nuo apsauga nuo neteisėtų kratų ir konfiskavimo. Istoriškai, privatumo apsaugos konceptas evoliucionavo nuo šio visiško savarankiškumo savo namuose pripažinimo į platesnę apsaugą nuo valstybės kišimosi į asmenų privatų gyvenimą. Teisės doktrinoje šis pokytis dažniausiai siejamas su 1890 m. S. Warren ir L. Brandeis straipsniu „The Righ to Privacy"[62]. Lietuvos doktrinoje teigiama, kad šis straipsnis yra itin reikšmingas, nes jame „[...] pirmą kartą 1) iškelta asmens privatumo (ir netiesiogiai asmens duomenų) kaip teisinio apsaugos objekto lygiagretaus turtui idėja ir kad asmuo turi turėti teisę būti vienas (angl. *the Right to be Alone*); 2) asmens privatumo ir duomenų apsaugos poreikis siejamas ne su žmogaus prigimtimi ir šimtmečius besivystančiusia jo buitimi, o su inovacijomis, mokslo ir technologijų pažanga"[63].

Autoriaus vertinimu, tokios didelės reikšmės suteikimas šiam straipsniui (kaip pirmojo, suformavusio asmens privatumo idėją), nėra visiškai tikslus. JAV mokslininkų straipsniuose yra teigiama, kad kokybinis JAV Konstitucijos Ketvirtosios pataisos turinio aiškinimo pokytis ir asmens privatumo, kaip savarankiško koncepto, identifikavimas gali būti siejamas su 1886 m. JAV Aukščiausiojo Teismo (Angl. *Supreme Court*)

---

62 Samuel D. Warren ir Louis D. Brandeis, „The Right to Privacy", *Harvard Law Review* 4, 5 (1890): 193– 220, doi:10.2307/1321160.

63 Stankevičiūtė, *supra note*, 6: 21.

išaiškinimais *Boyd* byloje[64]. Teismas šioje byloje nurodė, kad „Šioje nuomonėje išdėstyti principai turi įtakos pačiai konstitucinės laisvės ir saugumo esmei. Jie apima daugiau nei konkreti bylos forma, tuomet buvusi teisme, su atsitiktinėmis aplinkybėmis; jie taikomi visoms vyriausybės ir jos darbuotojų invazijoms į žmogaus namų šventumą ir gyvenimo privatumą. Pažeidimo esmė yra ne jo durų išlaužimas ir rausimasis stalčiuose, bet invazija į jo pamatinę teisę į asmeninį saugumą, asmeninę laisvę ir privačią nuosavybę, kai ši teisė niekada nebuvo prarasta dėl jo įsitikinimo ar dėl kokio nors viešo nusikaltimo“[65].

Taigi, šios bylos pagrindu, JAV teisinėje sistemoje atsirado privatumo apsaugos samprata, kuri kilo iš namų, kaip individo tvirtovės, apsaugos. Dėl šios istorinės kilmės, „amerikietiškajame“ požiūryje į privatumo apsaugą visada dominuoja keli esminiai aspektai: JAV „privatumo“ teisės šaltiniai, kad ir kokie individualūs jie bebūtų, visada linkę įsivaizduoti namus kaip pagrindinę gynybos liniją, o valstybę – kaip pagrindinį priešą[66].

Ši pagrindinė mintis atsispindi vienoje kertinių problemų, atsirandančių sąveikaujant Europos Sąjungos ir JAV teisinėms sistemoms privatumo apsaugos srityje – trečiosios šalies doktrinoje.

Trečiosios šalies doktrinos esmė yra ta, kad asmuo negali tikėtis privatumo apsaugos informacijai apie savo privatų gyvenimą, kurią jis perdavė trečiajai šaliai (pvz. bankui, telekomunikacijų bendrovei etc.)[67]. Ši informacija nebėra saugoma JAV Ketvirtosios Konstitucijos pataisos laiduojama teisine apsauga, nes ji nebegali būti laikoma esančia asmens „namuose“ – t. y. nežinoma kitiems.

Tačiau šis ribotas privatumo apsaugos supratimas su laiku keitėsi ir JAV teisinėje sistemoje. Lietuvos doktrinoje šis virsmas apibūdinamas nurodant, kad „vadovaujantis moderniuoju JAV Ketvirtosios Konstitucijos pataisos aiškinimu, ji saugo ne tik fizinę asmens aplinką, kadangi moderniųjų technologijų amžiuje asmens privatumo poreikis apsiriboja ne tik ja, ji išsiplečia į nematerialią erdvę ir nematerialius objektus, todėl ir šia Konstitucijos pataisa yra saugoma viskas, kam asmuo tikisi privatumo ir ką visuomenė laiko, kad jo tikėjimasis privatumo yra pagrįstas“[68]. Pamatinis pokytis

---

64 „Boyd v. United States“, US Supreme Court Justia, žiūrėta 2021 m. rugpjūčio 6 d., https://supreme.justia.com/cases/federal/us/116/616/

65 *Ibid.*

66 James Q. Whitman, „The Two Western Cultures of Privacy: Dignity versus Liberty“, *The Yale Law Journal* 113, 6 (2004): 1215.

67 Stern, *supra note*, 2: 101.

68 Stankevičiūtė, *supra note,* 6: 53.

šiame privatumo teisinės apsaugos ribų nustatyme siejamas su JAV Aukščiausiojo Teismo sprendimu *Katz* byloje, kurioje jis nurodė, kad JAV Ketvirtoji Konstitucijos pataisa „saugo asmenis, ne fizines vietas“, todėl telefoninių pokalbių turinio perėmimas turi būti laikomas krata, kuriai taikoma JAV Ketvirtosios Konstitucijos pataisos apsauga[69].

Taigi, JAV teisinėje sistemoje, kaip klasikinėje bendrojoje teisinėje sistemoje, teisė į privatumą vystoma teismų precedentais yra ne tik vystoma, bet ir iš esmės – sukurta. Tokia pamatinė šios teisinės sistemos savybė lemia tai, kad tokiais teisės šaltiniais paremta teisė yra sudėtingesnė (nes ji paremta kazuistinėmis taisyklėmis, suformuotomis konkrečiuose ginčuose), mažiau prognozuojama (teisę analizuojantis asmuo negali būti tikras, ar konkretus precedentas bus taikomas jo atveju, ar jo situacija, vis dėlto, skiriasi nuo tos kurioje buvo suformuotas precedentas).

Autoriaus vertinimu, tai yra viena iš sisteminių priežasčių, dėl kurių pastarasis asmens duomenų perdavimo tarp Europos Sąjungos ir JAV teisinis pagrindas (*Privacy Shield* susitarimas) buvo panaikintas Europos Sąjungos Teisingumo Teismo 2020 metais[70]. Privatumo apsauga JAV teisinėje sistemoje yra tiesiog per daug fragmentuota, kad galėtų užtikrintų tokios reikšmingos (pagrindinės) žmogaus teisės tinkamą apsaugą, nes ji sukurta ne įtvirtinant konkrečią teisę į privatumą ir jos ribas, o teismų sprendimuose nustatant individualiais atvejais taikytinas privatumo apsaugos išimtis. Tai yra ypač aktualu, kai privatumo apsaugos adekvatumo standartas yra vertinamas pagal aukštą Europos Sąjungos teisės standartą.

Atsižvelgiant į tai, kad ankstesni JAV ir Europos Sąjungos asmens duomenų perdavimo teisiniai pagrindai (*Safe Harbour* ir *Privacy Shield* susitarimai) buvo panaikinti dėl to, kad JAV teisinėje sistemoje nebuvo garantuojama adekvataus lygio apsauga iš Europos Sąjungos gaunuamiems duomenims, darytina išvada, kad privatumo apsaugos reguliavimas JAV teisinėje sistemoje vystysis pagal kontinentinės teisinės sistemos pavyzdį – bus priimti sisteminiai, privatumo ir asmens duomenų apsaugai skirti teisės aktai.

Teisėkūros procesai niekuomet nebuvo greiti ar paprasti, o ypač – vienoje seniausių pasaulio demokratijų. JAV žiniasklaidoje jau nuo pat Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje (t. y. nuo 2020 m. vidurio) aprašomos sistemingo privatumo ir asmens duomenų apsaugos teisinio reguliavimo iniciatyvos

[69] „Katz v. United States“, US Supreme Court Justia, žiūrėta 2020 m. rugsėjo 4 d., https://supreme.justia.com/cases/federal/us/389/347/.

[70] Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note*, 8.

ir teisėkūros proceso peripetijos[71]. Tokio žingsnio tikisi ir JAV ūkio subjektų teikiamų paslaugų vartotojai Europos Sąjungoje. Europos vartotojų organizacija ryšium su Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje taip pat išreiškė kritišką nuomonę JAV atžvilgiu, reikalaudami reikšmingų permainų JAV teisinėje sistemoje: „jei JAV nepriims tvirtos ir išsamios duomenų apsaugos sistemos, įskaitant privatumo apsaugos įstatymą federaliniu lygmeniu, joks būsimas Europos Sąjungos ir JAV susitarimas dėl duomenų srautų teisme nebus laikomas pagrįstu“[72].

Taigi, kontinentinės teisinės sistemos įkvėptas privatumo ir asmens duomenų apsaugos teisinis reguliavimas, tikėtina, anksčiau ar vėliau atsiras JAV teisinėje sistemoje. Autoriaus vertinimu, tolimesniuose šio darbo skyriuose analizuojamos mokslinės problemos bei galimi jų sprendimai JAV teisinėje sistemoje bus pateikiami teisės aktuose, turinčiuose kontinentinei teisės tradicijai būdingų bruožų. Šis naujasis teisinis reguliavimas, neabejotinai padarys didelę įtaką visam pasauliui, nes būtent JAV yra pagrindinės globalių virštinklinių paslaugų teikėjų būstinės (pvz. *Facebook, Apple, Google* etc.), kurių teikiamos paslaugos yra prieinamos vartotojams visame pasaulyje.

Elektroninės erdvės samprata.

Elektroninė erdvė – atrodo labai akivaizdi ir savaime suprantama sąvoka, kurios apibrėžti būtinybės nėra. Tačiau atliekant teisinius tyrimus, būtent tokius teisinius konceptus (kurie yra akivaizdūs ar atrodo „savaime suprantami“) ir yra sudėtingiausia apibrėžti.

Lietuvos teisės doktrinoje tyrimai, susiję su elektronine erdve, buvo populiarūs pastarąjį dešimtmetį. Skirtingi autoriai analizuoja teisinio reguliavimo ar jo įgyvendinimo problemas, susijusias su elektronine erdve. Pavyzdžiui, Darius Štitilis savo moksliniuose darbuose nagrinėja tapatybės vagystės elektroninėje erdvėje problemas[73]; asmens identifikavimo fizinėje ir elektroninėje erdvėje teisinio reguliavimo prielaidas[74]. Mindaugas Kiškis ir Lina Šlapimaitė straipsnyje nagrinėja asmens duomenų sampratos

---

[71] Cameron F. Kerry, „One year after Schrems II, the world is still waiting for U.S. privacy legislation“, žiūrėta 2021 m. rugpjūčio 30 d., https://www.brookings.edu/blog/techtank/2021/08/16/one-year-after-schrems-ii-the-world-is-still-waiting-for-u-s-privacy-legislation/.

[72] „EU Top Court Sides with Consumer Privacy in EU–US Data Shambles“, BEUC, žiūrėta 2021 m. rugpjūčio 2 d., https://www.beuc.eu/publications/eu-top-court-sides-consumer-privacy-eu-us-data-shambles/html.

[73] Darius Štitilis ir Marius Laurinaitis, „Tapatybės Vagystė Elektroninėje Erdvėje“, *Informacijos Mokslai* 50 (2009).

[74] Darius Štitilis ir kt., „Asmens Identifikavimo Fizinėje Ir Elektroninėje Erdvėje Teisinio Reguliavimo Prielaidos“, *Jurisprudencija* 18, 2 (2011): 703-24.

elektroninėje erdvėje problemas[75]. Kitame straipsnyje M. Kiškis nagrinėja intelektinės nuosavybės elektroninėje erdvėje ypatumus ir teisinį reglamentavimą[76]. Visuose šiuose darbuose elektroninės erdvė nauduojama kaip fonas pagrindinės problemos analizei, tačiau pati elektroninės erdvės samprata ar jos ribos moksliniuose darbuose nėra analizuojama.

Lietuvos teisiniame reguliavime elektroninės erdvės samprata nors ir vartojama, tačiau nėra įtvirtinta. Pavyzdžiui, elektroninės erdvės sąvoka vartojama Lietuvos Respublikos saugios laivybos[77], Lietuvos Respublikos asmens tapatybės kortelės ir paso[78], Lietuvos Respublikos valstybės informacinių išteklių valdymo[79] įstatymuose yra vartojama, tačiau nė viename jų nėra apibrėžiama.

Šiuo aspektu atkreiptinas dėmesys į elektroninės erdvės sampratos giminingumą kibernetinės erdvės sampratai. Nustatyti semantinį skirtumą tarp jų atrodo sudėtinga ir, autoriaus vertinimu, elektroninė erdvė ir kibernetinė erdvė laikytinos sinonimais, angliškos sąvokos *cyberspace* vertiniais. Tokią prielaidą geriausiai patvirtina tarptautinės konvencijos „*Convention on Cybercrime*“[80] pavadinimo vertimas į Lietuvių kalbą, kuris skamba „Konvencija dėl elektroninių nusikaltimų“[81].

Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinė erdvė apibrėžiama kaip „aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija“[82]. Atliekant šio sąvokos semantinę analizę, darytina išvada, kad kibernetinė erdvė apima tiek pačius įrenginius (pvz. kompiuterius), kurie elektroninę informaciją siunčia ar gauna, tiek ryšių infrastruktūrą šiems perdavimams atlikti, tiek pačią elektroninę informaciją.

---

75 Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė* 96 (Vilnius: Vilniaus Universitato Leidykla, 2015).

76 Mindaugas Kiškis, „Intelektinės Nuosavybės Elektroninėje Erdvėje Ypatumai Ir Teisinis Reglamentavimas“, *Teisė* 71 (Vilnius: Vilniaus Universiteto Leidykla, 2009).

77 „Lietuvos Respublikos saugios laivybos įstatymas“, LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.107736/asr.

78 „Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas“, LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f26839f08f5011e48028e9b85331c55d/asr.

79 „Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas“, LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/asr.

80 „Convention on Cybercrime“, Council of Europe, žiūrėta 2021 m. rugpjūčio 6 d., https://rm.coe.int/1680081561.

81 „2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų“, LRS, žiūrėta 2021 m. rugpjūčio 6 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195.

82 „Lietuvos Respublikos kibernetinio saugumo įstatymas“, 2 str. 6 d., LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.

Lietuvos Respublikos kibernetinio saugumo įstatyme nurodyta, kad jame vartojamos sąvokos suprantamos taip, kaip *inter alia* jos apibrėžtos ir Lietuvos Respublikos elektroninių ryšių įstatyme. Todėl, analizuojant kibernetinės erdvės sąvokos esmę ir atsižvelgiant į Lietuvos Respublikos elektroninių ryšių įstatyme vartojamas sąvokas, darytina išvada, kad kibernetinės erdvės sampratą *inter alia* sudaro elektroninių ryšių infrastruktūra[83] (pvz. antenos, linijos, skirtos elektroninių ryšių veiklai vykdyti), elektroninių ryšių tinklas[84] (pvz. tinklo įranga, skirta perduoti signalus) bei galiniai įrenginiai[85] (pvz. kompiuteriai). Atsižvelgiant į nurodytus argumentus, šiame darbe elektroninės erdvės ir kibernetinės erdvės sąvokos bus vartojamos sinonimais.

Autorius siekia atskirai atkreipti dėmesį, į prieštaringas elektroninės ir kibernetinės erdvės sampratas, sutinkamas Lietuvos teisės doktrinoje. Viename Lietuvos teisės mokslininkės tyrime teigiama, kad *Harvardo* ir *Stanfordo* universitetų mokslininkų grupė nustatė tokia elektroninės erdvės apimtį:

„a) fizinę infrastruktūrą ir telekomunikacijų įrenginius plačiąja prasme, kurie dalyvauja kompiuterių tinklų ryšyje (SCADA įrenginius, išmaniuosius telefonus, planšetes, kompiuterius, serverius ir t. t.);

b) kompiuterių sistemas ir susijusią programinę įrangą, kuri užtikrina aplinkos operacines funkcijas ir ryšius;

c) tinklus tarp kompiuterių sistemų;

d) tinklų tinklus, kurie jungia kompiuterių sistemas;

e) vartotojų prieigos ir tarpinių maršrutų taškus;

f) duomenis (angl. *constituent data or resident data*).“[86]

---

[83] Elektroninių ryšių infrastruktūra – fizinės infrastruktūros, kurią sudaro aparatūra, įrenginiai, įskaitant antenas, linijos, vamzdynai, kabeliai, kanalai, kolektoriai, šuliniai, atraminės konstrukcijos, bokštai, stiebai, statiniai, statinių įvadai, statinių inžinerinės sistemos, skirstomosios spintos ir kitos priemonės, visuma, skirta elektroninių ryšių veiklai vykdyti. Žr. „Lietuvos Respublikos elektroninių ryšių įstatymas“, 3 str. 12 d., LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/asr.

[84] Elektroninių ryšių tinklas – perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį. Žr. *Ibid*, 3 str. 16 d.

[85] Galinis įrenginys – leidžiantis priimti ir (arba) perduoti informaciją įrenginys ar jo atitinkama dalis, skirti tiesiogiai ar netiesiogiai bet kokiomis priemonėmis būti prijungti prie viešųjų ryšių tinklų. Žr. *Ibid*, 3 str. 22 d.

[86] Stankevičiūtė, *supra note*, 6: 35.

Atsižvelgdama į tokią elektroninės erdvės sampratą, autorė teigia, kad Lietuvos Respublikos kibernetinio saugumo įstatyme yra pateikta siauresnė elektroninės erdvės samprata, neapimanti aukščiau pateikto apibrėžimo c), d) ir e) punktų[87].

Su tokia teisės doktrinoje pateikiama išvada autorius negali sutikti. Kaip matyti, S. Stankevičiūtės vertinimu, elektroninės erdvės samprata neapima su informacijos perdavimu susijusios įrangos plačiąja prasme (t. y. tinklų įrangos ir prieigą vartotojams suteikiančios įrangos). Tuo tarpu Lietuvos Respublikos kibernetinio saugumo įstatyme *expressis verbis* nurodyta, kad kibernetinė erdvė suprantama kaip aplinka, kurią sudaro *inter alia* ryšių ir informacinių technologijų įranga[88]. Todėl nėra jokio teisinio ar faktinio pagrindo su informacijos perdavimu susijusios įrangos neįtraukti į kibernetinės erdvės sampratą.

Kita elektroninės erdvės samprata, su kuria autorius nesutinka, yra apibrėžta Teisės informatikos ir informatikos teisės vadovėlyje, kuriame ji apibūdinama kaip „pasaulinė viešai ir visuotinai prieinama kompiuterių tinklų sistema, per kurią yra keičiamasi informacija“[89].

Analogiškai Teisės informatikos ir informatikos teisės vadovėlio atvejui, paminėtina, kad M. Civilkos ir L. Šlapimaitės straipsnyje elektroninės erdvės sąvoka taip pat yra sutapatinama su interneto sąvoka: „jeigu straipsnyje specialiai nenurodyta kitaip, terminai „internetas“ ir „elektroninė erdvė“ vartojami kaip sinonimai“[90]. Minėti autoriai elektroninės erdvės sąvoką taip pat sieja tik su „internetu“ – duomenų perdavimo sistema ir, tikėtina įranga.

Autoriaus vertinimu, semantiškai vertinant elektroninės erdvės sąvoką, akivaizdu, kad ji apima ne tik signalų perdavimo įrenginius ir infrastruktūrą. Kitaip tariant, elektroninė erdvė turi apimti ir įrenginius (pvz. kompiuterius), kurie suteikia galimybę ta kompiuterių tinklų sistema pasinaudoti, kad būtų galima keistis informacija – ją siųsti ir gauti. Tuo tarpu aiškinant elektroninės erdvės sampratą taip siaurai, kokia jos sąvoka pateikiama minėtame vadovėlyje, ji yra nepagrįstai apribojama (i) išimtinai tik tinklo įranga (t. y. tinklų sistema, per kurią yra keičiamasi informacija) ir (ii) tik visuotinai prieinama tinklų sistema.

Tokiu būdu, Teisės informatikos ir informatikos teisės vadovėlio bei minėto

---

87 *Ibid.*

88 „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note*, 104: 2 str. 6 d.

89 Mindaugas Kiškis ir kt., *Teisės informatika ir informatikos teisė: vadovėlis* (Vilnius: Mykolo Romerio universitetas, 2006), 11.

90 Civilka ir Šlapimaitė, *supra note*, 97: 1.

mokslinio straipsnio autoriai elektroninės erdvės sampratą nepagrįstai sutapatino su elektroninių ryšių tinklo sąvoka[91], neįtraukdami nei galinių įrenginių, nei pačios informacijos, kuri jais yra perduodama.

Taip pat autorius siekia atkreipti dėmesį, kad Europos teisinėje sistemoje elektroninės erdvės ar kibernetinės erdvės sąvokos nėra nustatytos. Tokia sąvoka nėra minima nei BDAR, nei Europos elektroninių ryšių kodekse[92], nei direktyvoje dėl privatumo ir elektroninių ryšių[93], nei direktyvoje dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Europos Sąjungoje užtikrinti[94].

Europos Sąjungos teisės doktrinoje, kaip ir Lietuvos mokslininkų publikacijose, elektroninės erdvės sąvoka dažnai yra minima, tačiau tik kitų teisinių problemų kontekste ir atskirai neanalizuojama[95]. Autoriui pavyko rasti vieną mokslinį straipsnį, kuriame elektroninė erdvė yra priešpastatoma informacijos perdavimo protokolui ar informacijos saugojimo platformai ir yra identifikuojama kaip technologija, skirta socialiniam bendravimui[96]. Elektroninė erdvė šiame moksliniame tyrime buvo analizuojama kaip socialinis reiškinys – vieta bendruomenėms vystytis ir egzistuoti be įprastų realios erdvės laiko ir erdvės apribojimų[97].

Tokia Europos teisės mokslininkų atlikta analizė ir daromos išvados neprieštarauja elektroninės erdvės sampratai, kaip ją šio tyrimo vykdymo tikslu identifikuoja autorius, iš esmės remdamasis Lietuvos Respublikos kibernetinio saugumo įstatyme pateikta kibernetinės erdvės sąvoka. Pateikiamas elektroninės erdvės, kaip terpės socialiniams santykiams kurtis ar vystytis, konceptas neprieštarauja sąlyginai techniniam apibrėžimui (kildinamam iš minėto įstatymo), o autoriaus vertinimu, gali būti identifi-

---

91 „Lietuvos Respublikos elektroninių ryšių įstatymas“, *supra note*, 105: 3 str. 16 d.

92 „Europos Parlamento ir Tarybos 2018 m. gruodžio 11 d. direktyva (ES) 2018/1972 kuria nustatomas Europos elektroninių ryšių kodeksas“, *supra note*, 75.

93 „Europos Parlamento ir Tarybos Direktyva 2002/58/EB 2002 m. liepos 12 d. dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), L 201, 31/07/2002“, *supra note*, 65.

94 „2016 m. liepos 6 d. Europos Parlamento ir Tarybos Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“, EUR-Lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016L1148.

95 Žr. pvz., Nikolas Ott ir Hugo Zylberberg, „A European Perspective on the Protection of Personal Data in Cyberspace: Explaining How the European Union Is Redefining Ownership and Policies of Personal Data beyond National Borders“, *Kennedy School Review* 16 (2016): 69-75; George Christou, „The Collective Securitisation of Cyberspace in the European Union“, *West European Politics* 42, 2 (2019): 278-301; Georgios I. Zekos, „Cyberspace and IPRs Stimulus on Foreign Direct Investment in the European Union“, *Journal of Internet Law* 20, 6 (2016): 3.

96 Balazs Ratai, „Understanding Lessig: Implications for European Union Cyberspace Policy“, *International Review of Law, Computers & Technology* 19, 3 (2005): 278.

97 *Ibid.*

kuojamas kaip vienas iš elektroninės erdvės panaudojimo tikslų. Aplinkybė, kad elektroninė erdvė, kaip priemonė kurti, saugoti ir perduoti duomenis, gali būti naudojama socialinių ryšių vystymo tikslais, mokslinių tyrimų vykdymo tikslais, ar bet kokiais kitais tikslais, nedaro jokios įtakos elektroninės erdvės sampratai ar riboms.

Atsižvelgdamas į visus šiame skyriuje pateiktus argumentus ir iš esmės remdamasis Lietuvos Respublikos kibernetinio saugumo įstatyme pateikta kibernetinės erdvės sąvoka, autorius šiame tyrime elektroninės erdvės sąvoką naudos kaip sampratą, apibūdinančią visumą techninės įrangos, kuri skirta kurti, siųsti, perduoti bei priimti elektroninei informacijai, įskaitant tiek galinius įrenginius (pvz. kompiuterius), tiek ryšių infrastruktūrą šiems perdavimams atlikti (pvz. tarnybines stotis, maršrutizatorius etc.), tiek pačią informaciją.

## 2. Asmens duomenų apsaugos, perduodant asmens duomenis tarp skirtingų teisinių sistemų elektroninėje erdvėje, teisiniai pagrindai.

Pasaulis, kuriame gyvenimas tapo skaitmeninis, grindžiamas duomenimis, žiniomis ir tinklais. Jame prekių ir paslaugų pardavimas nėra įmanomas be intensyvaus ir tikslaus duomenų perdavimo. Sąvoka „skaitmeninė ekonomika“ tinkamai apibūdina šį pokytį. Duomenys, informacija ir žinios yra pagrindiniai gamybos elementai – perkeltine prasme jie yra „naujoji nafta“ šiandieniniame pasaulyje[98]. Kai kuriose srityse, duomenys, informacija ir žinios yra verslo šerdyje: tai liečia ne tik socialinius tinklus, tačiau ir mokėjimo paslaugas, informacinių technologijų industriją ir kt. sritis. Šiandieniniame pasaulyje, duomenų ir informacijos perdavimo pagrindu veikiančių verslų svarbą ekonomikai ir visuomeniniam gyvenimui iliustruoja aplinkybė, kad pasaulio turtingiausiųjų asmenų dešimtuke, informacinių sistemų pagrindu sukurtų verslų savininkų yra net šeši[99], o be tarptautinio duomenų perdavimo ne tik nebūtų galimybės naudotis daugybe virštinklinių paslaugų, kurių prieinamumas laikomas savaime suprantamu (pvz., tokių kaip *Messenger*, *Instagram*, *Gmail*, *WhatsApp* ir t. t.) tačiau taip pat būtų reikšmingai suvaržytas tarptautinis bendradarbiavimas teisėsaugos, žvalgybos institucijų ir pan.

Nepaisant duomenų perdavimo tarp skirtingų teisinių sistemų svarbos, teisinis duomenų perdavimo reglamentavimas nėra paprastas. Šią duomenų perdavimo sritį reglamentuoja tarptautinės teisės, žmogaus teisių ir valstybės suvereniteto principai, kurių reguliavimo tikslai dažnai būna labai skirtingi: privačių duomenų ir privatumo apsauga, komercinių paslapčių, intelektinės nuosavybės, nacionalinio saugumo, žodžio laisvės apsauga ir kt.[100]. Nors apie transatlantinį duomenų perdavimą nemažai rašė ir diskutavo tiek ES, tiek JAV mokslininkai[101], tačiau praktika rodo, kad surasti kompromisą tokioms galingoms ekonomikoms kaip Europos Sąjungos ir JAV nėra lengva bet

[98] Daniel Possler, Sophie Bruns ir Julia Niemann-Lenz, „Data Is the New Oil--But How Do We Drill It? Pathways to Access and Acquire Large Data Sets in Communication Science.” *International Journal of Communication*, (2019): 3894, žiūrėta 2021 m. kovo 16 d., https://ijoc.org/index.php/ijoc/article/download/10737/2763.

[99] „Pasaulio turtingiausių asmenų sąrašas“, žiūrėta 2021 m. kovo 16 d., https://www.forbes.com/real-time-billionaires/#1dcf6c0b3d78.

[100] „Tarptautinių susitarimų tarp Europos Sąjungos ir JAV sąrašas“, EUR-lex, žiūrėta 2021 m. kovo 16 d., https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html.

[101] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (Springer, 2013).; Marcelo Arenas ir kt., *Foundations of Data Exchange* (Cambridge: Cambridge University Press, 2014).

kuriuo klausimu, jau nekalbant apie tokią visuomenei bei nacionaliniams interesams reikšmingą problemą, kaip teisės į privatumą apsauga.

Sėkmingo susitarimo dėl privatumo apsauugos pasiekimas yra komplikuotas ne tik dėl sudėtingo ekonominių besitariančiųjų interesų derinimo, bet ir dėl skirtingų Europos Sąjungos ir JAV duomenų teisinio reguliavimo principų. JAV teisiniam reguliavimui būdingas teritorinis privatumas ir specifinės taisyklės konkrečioms duomenų rūšims[102], t. y. skirtingas teisinis režimas taikomas skirtingoms duomenų rūšims ir jų turėtojams (pavyzdžiui, informacija apie asmens išlaidas gali būti laikoma konfidencialia kai ją kaupia pats asmuo, bet ta pati informacija, kai ją saugo bankas, nebėra saugoma). Tuo tarpu Europos Sąjungos režimas yra pagrįstas viena bendra asmens duomenų kategorija (kuri suprantama labai plačiai), o jų naudojimas sankcionuojamas pagal skirtingus duomenų naudojimo tikslus, pvz. sudarytos sutarties vykdymui, gavus duomenų subjekto sutikimą etc.[103].

Autoriaus vertinimu, asmens duomenų tvarkymo reguliavimo supratimui aktualu išskirti tris skirtingas asmens duomenų tvarkymo kategorijas: teisėsaugos tikslais (šiuo metu reguliuojami Direktyva 2016/680[104]), nacionalinio saugumo tikslais (kuriems netaikomi Europos Sąjungos teisės aktai) ir asmens duomenų tvarkymas kitais tikslais (pvz. teikiant elektroninių ryšių paslaugas, virštinklines paslaugas, vykdant komercines sutartis – šiuo metu reguliuojami BDAR).

Šio tyrimo temos atskleidimo tikslu pirmiausiai yra aktualu išanalizuoti teisinį asmens duomenų perdavimo iš Europos Sąjungos į JAV pagrindą, reglamentuotą būtent BDAR, nes jis yra ne tik faktiškai ir komerciškai jautriausia sritis (kadangi transatlantiniai duomenų srautai tarp Europos Sąjungos ir JAV yra greičiausi ir didžiausi pasaulyje, bei sudaro daugiau nei pusę Europos duomenų srautų ir apie pusę JAV duomenų srautų; JAV ir Europos Sąjungos yra svarbiausios komercinės partnerės kalbant

---

[102] „29 straipsnio darbo grupės 1999 m. sausio 26 d. nuomonė Nr. 5092/98/EN/final“, European Commission, žiūrėta 2021 m. kovo 16 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf.

[103] „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)“, *supra note*, 60.

[104] „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“, EUR-Lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex-%3A32016L0680.

apie skaitmenines paslaugas[105]), bet kaip rodo aktuali Europos Sąjungos Teisingumo Teismo praktika *Schrems* bei *Schrems II* bylose – ir itin aktuali teisinė problema. Todėl tolimesniuose šio skyriaus skirsniuose yra atliekama asmens duomenų perdavimo į trečiąsias šalis pagrindų, įtvirtintų BDAR V skyriuje, analizė bei identifikuojamos jų taikymo problemos, atsižvelgiant į Europos Sąjungos Teisingumo Teismo praktiką bei doktrinoje pateikiamas mokslininkų nuomones.

## 2.1. Asmens duomenų perdavimo į trečiąsias šalis reguliavimas pagal Bendrąjį duomenų apsaugos reglamentą

BDAR yra įtvirtinta, kad asmens duomenys, kurie yra tvarkomi arba kuriuos ketinama tvarkyti juos perdavus į trečiąją valstybę arba tarptautinei organizacijai, gali būti perduodami tik tuo atveju, jei duomenų valdytojas ir duomenų tvarkytojas, laikydamiesi kitų BDAR nuostatų, laikosi BDAR V skyriuje nustatytų sąlygų, be kita ko, susijusių su tolesniu asmens duomenų perdavimu iš tos trečiosios valstybės ar tarptautinės organizacijos į kitą trečiąją šalį ar kitai tarptautinei organizacijai[106].

BDAR asmens duomenų perdavimui į trečiąsias valstybes arba tarptautinėms organizacijoms reglamentuoti yra skirtas atskiras skyrius – V-asis BDAR skyrius. Šiame BDAR skyriuje yra įtvirtinti keli savarankiški asmens duomenų perdavimo įteisinimo būdai - duomenų perdavimas remiantis sprendimu dėl tinkamumo[107], duomenų perdavimas taikant tinkamas apsaugos priemones[108], kitos asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai sąlygos[109]. Pažymėtina, kad šie asmens duomenų perdavimo pagrindai turi hierarchiją (aukščiausias – 45 str. įtvirtintas Europos Komisijos sprendimas dėl tinkamumo) ir paskesnis asmens duomenų perdavimo teisinis pagrindas gali būti taikomas tik tuomet, kai aukštesnis pagal hierarchiją teisinis pagrindas neegzistuoja.

Atkreiptinas dėmesys į bendrąjį principą, kad BDAR V skyriaus nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui[110]. Europos Sąjungos Teisingumo Teismas yra konstataveęs,

[105] Hamilton ir Quinlan, *supra note*, 1: 8.

[106] „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)“, *supra note,* 60: 44 str.

[107] *Ibid*, 45 str.

[108] *Ibid*, 46 str.

[109] *Ibid*, 49 str.

[110] *Ibid*, 44 str.

kad šia nuostata siekiama užtikrinti šio aukšto asmens duomenų apsaugos lygio tęstinumą, kai asmens duomenys perduodami į trečiąją šalį, kad ir kokiu BDAR V skyriuje įtvirtintu teisiniu pagrindu tai bebūtų daroma[111].

Atsižvelgiant į tai, kad aukščiau išvardinti BDAR įtvirtinti asmens duomenų perdavimo įteisinimo būdai yra savarankiški, toliau pateiksime trumpą jų apžvalgą ir atskleisime pagrindinius jų skirtumus.

### 2.1.1. Asmens duomenų perdavimas remiantis sprendimu dėl tinkamumo.

BDAR 45 str. 1 d. įtvirtinta bendra Europos Komisijos teisė priimti sprendimą, kad atitinkama trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Tuomet perduoti asmens duomenis į šią trečiąją valstybę arba tarptautinei organizacijai galima bei tokiam duomenų perdavimui specialaus leidimo nereikia.

BDAR taip pat imperatyviai įtvirtintas išsamus sąrašas vertinamojo pobūdžio aplinkybių, į kuriuos Europos Komisija, turi atsižvelgti svarstydama galimybę priimti sprendimą dėl trečiosios valstybės arba atitinkamos tarptautinės organizacijos užtikrinamo apsaugos lygio tinkamumo:

„a) teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, atitinkamus bendruosius ir atskiriems sektoriams skirtus teisės aktus, įskaitant susijusius su visuomenės saugumu, gynyba, nacionaliniu saugumu, baudžiamąja teise ir valdžios institucijų prieiga prie asmens duomenų, taip pat tokių teisės aktų įgyvendinimą, duomenų apsaugos taisykles, profesines taisykles ir saugumo priemones, įskaitant taisykles dėl tolesnio asmens duomenų perdavimo į kitą trečiąją valstybę ar kitai tarptautinei organizacijai, kurių laikomasi toje valstybėje arba kurių laikosi ta tarptautinė organizacija, teismų praktikos precedentus, taip pat veiksmingas ir vykdytinas duomenų subjektų teises ir veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones;

b) tai, ar yra ir ar veiksmingai veikia viena ar kelios nepriklausomos priežiūros institucijos trečiojoje šalyje arba kurioms yra pavaldi tarptautinė organizacija ir kurių atsakomybė yra užtikrinti, kad būtų laikomasi duomenų apsaugos taisyklių ir jos būtų vykdomos, įskaitant tinkamus vykdymo įgaliojimus padėti duomenų subjektams naudotis savo teisėmis ir patarti, kaip tai daryti, ir bendradarbiauti su valstybių narių

[111] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note*, 8: 92 – 93 p.,

priežiūros institucijomis; ir

c) atitinkamos trečiosios valstybės arba tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus ar kitus įsipareigojimus, atsirandančius dėl teisiškai privalomų konvencijų ar priemonių, taip pat dėl jų dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma kiek tai susiję su asmens duomenų apsauga“[112].

Atkreiptinas dėmesys, kad visi šie BDAR išvardinti aspektai yra savarankiški ir vertintini kiekvienu individualiu atveju. Būtent dėl jų (ne)tinkamo nustatymo praktikoje kyla ginčai, kurių pasekmė – BDAR 45 str. pagrindu Europos Komisijos priimto *Privacy Shield* susitarimo panaikinimas. Pavyzdžiui, *Schrems II* bylos atveju buvo vertinama Europos Komisijos sprendimo dėl *Privacy Shield* susitarimo atitiktis BDAR 45 str. 2 d. a) p. nuostatai, kad vertindama trečiosios šalies užtikrinamo apsaugos lygio tinkamumą Komisija, be kita ko, privalo atsižvelgti į „veiksmingas ir vykdytinas [įgyvendinamas] duomenų subjektų [kurių asmens duomenys perduodami] teises“[113], „teisės aktus, įskaitant susijusius su visuomenės saugumu, gynyba, nacionaliniu saugumu, baudžiamąja teise ir valdžios institucijų prieiga prie asmens duomenų“[114], „veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones“[115].

Europos Komisija, įvertinusi trečios šalies ar teritorijos, su kuria pageidaujama sudaryti susitarimą dėl asmens duomenų perdavimo, apsaugos lygio tinkamumą (*inter alia* pagal BDAR 44 str. 2 d. nurodytus aspektus), priimdama įgyvendinimo aktą nusprendžia, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamo lygio apsaugą[116]. Praktikoje, Europos Komisija yra pripažinusi adekvatų asmens duomenų apsaugos lygį

---

[112] „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)“, *supra note,* 60: 44 str. 2 d.

[113] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note, 8:* 177 p.

[114] *Ibid*, 179 - 181 p.

[115] *Ibid*, 188 p.

[116] „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)“, *op. cit.*, 44 str. 3 d.

taikančiomis šalimis Andorą[117], Argentiną[118], Kanadą[119] (komercines organizacijas), Izraelį[120], Japoniją[121], Šveicariją[122] etc. Pastebėtina, kad šiame sąraše nebėra *Privacy Shield* susitarimo su JAV, kuris buvo panaikintas Europos Sąjungos Teisingumo Teismo sprendimai byloje *Schrems II*[123].

Taip pat pabrėžtina, kad Europos Komisija turi pareigą įsitikinti trečios šalies, teritorijos ar tarptautinės organizacijos siūlomo asmens duomenų apsaugos lygio tinkamumu ne tik konkretaus sprendimo priėmimo metu, tačiau ir po jo. BDAR imperatyviai įtvirtinta, kad Europos Komisija turi nuolat stebėti pokyčius trečiosiose valstybėse ir tarptautinėse organizacijose, kurie galėtų daryti poveikį pagal BDAR 45 str. 3 d. priimtų sprendimų ir pagal Direktyvos 95/46/EB 25 str. 6 d. priimtų sprendimų veikimui[124] bei privalo atlikti periodines peržiūras (kuriomis atsižvelgiama į visus atitinkamus pokyčius trečiojoje valstybėje ar tarptautinėje organizacijoje), ne rečiau nei kas ketverius metus[125].

Šis aspektas yra ne tik itin svarbus ir turėjo praktinę reikšmę Europos Sąjungos

---

117 „Europos Komisijos 2010 m. spalio 19 d. sprendimas dėl tinkamos asmens duomenų apsaugos Andoroje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2010/625/ES)", EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32010D0625&from=EN.

118 „Europos Komisijos 2003 m. birželio 30 d. sprendimas dėl adekvačios asmens duomenų apsaugos Argentinoje, remiantis Europos Parlamento ir Tarybos direktyva 95/46/EB Nr. 2003/490/EB", EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32003D0490&from=BG.

119 „Europos Komisijos 2001 m. gruodžio 20 d. sprendimas dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2002/2/EB)", EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32002D0002.

120 „Europos Komisijos 2011 m. sausio 31 d. sprendimas dėl Izraelio Valstybės užtikrinamos tinkamos asmens duomenų apsaugos automatizuoto asmens duomenų tvarkymo srityje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2011/61/ES", EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32011D0061&from=PL.

121 „Europos Komisijos 2019 m. sausio 23 d. sprendimas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Japonijoje pagal Asmeninės informacijos apsaugos įstatymą Nr. (EU)2019/419", EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019D0419&from=EN.

122 „Europos Komisijos 2000 m. liepos 26 d. sprendimas dėl Šveicarijoje teikiamos pakankamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2000/518/EB", EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX-%3A32000D0518.

123 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II")", *supra note,* 8.

124 „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)", *supra note,* 60: 45 str. 4 d.

125 *Ibid*, 45 str. 3 d.

Teisingumo Teismui sprendimo *Schrems* byloje priėmimo metu (t. y. 2015 metais), bet ir kontraversiškas nes teismas turėjo vertinti *Safe Harbour* susitarimo, kuris buvo sudarytas prieš 15 metų, įgyvendinimo aspektus. Bendra taisyklė, kildinama iš Europos Sąjungos Teisingumo Teismo išaiškinimų *Jippes* byloje, yra tokia, kad „Bendrijos teisės akto teisėtumas negali priklausyti nuo retrospektyvaus jo veiksmingumo įvertinimo. Kai Bendrijos įstatymų leidėjas yra įpareigotas įvertinti ateityje numatomų priimti taisyklių poveikį ir tų padarinių negalima tiksliai numatyti, jo vertinimas gali būti kritikuojamas tik tuo atveju, jei jis akivaizdžiai neteisingas, atsižvelgiant į informaciją, kurią jis turėjo kvestionuojamo teisės akto rengimo metu“[126]. Todėl remiantis šia suformuota praktika, atrodytų, kad paskesni įvykiai, susiklostę po kvestionuojamo teisės akto priėmimo, neturėtų turėti lemiamos reikšmės svarstant dėl teisės akto teisėtumo.

Tačiau iš BDAR 45 str. 4 d. turinio analizės akivaizdu, kad asmens duomenų apsaugos atžvilgiu yra numatoma išimtis, kuri, pabrėžtina, suteikia ne teisę, o tęstinę pareigą Europos Komisijai įsitikinti trečios šalies, teritorijos ar tarptautinės organizacijos siūlomo asmens duomenų apsaugos lygio tinkamumu, net ir po atitinkamo teisės akto priėmimo. Šiuo aspektu išsamesnė teisinė analizė dėl galimybės vertinti seniai priimtų teisės aktų atitiktį jų taikymo metu galiojančiai praktikai analizuojama šio tyrimo 3.2 skirsnyje.

Galiausiai, BDAR įtvirtina ne tik Europos Komisijos teisę prižiūrėti trečios šalies, teritorijos ar tarptautinės organizacijos siūlomo asmens duomenų apsaugos lygio tinkamumą, bet ir reaguoti į pasikeitusias aplinkybes. Kai Europos Komisija nusprendžia, kad trečioji valstybė, teritorija arba nurodytas vienas ar keli sektoriai trečiojoje valstybėje, arba tarptautinė organizacija nebeužtikrina tinkamo lygio apsaugos, kaip apibrėžta BDAR 45 str. 2 d., Europos Komisija privalo reikiamu mastu įgyvendinimo aktais panaikinti arba iš dalies pakeisti konkretų savo priimtą sprendimą, arba sustabdyti jo galiojimą nustatydama, kad jis netaikomas atgaline data[127]. Atkreiptinas dėmesys, kad BDAR yra įtvirtintas pro-vartotojiškas asmens duomenų apsaugos modelis, kai Europos Komisija turi pareigą pirma sustabdyti priimtą sprendimą dėl trečiosios šalies, teritorijos ar tarptautinės organizacijos tinkamo lygio apsaugos, o tik po to pra-

---

[126] „Europos Sąjungos Teisingumo Teismo 2001 m. liepos 12 d. sprendimas byloje Nr. C-189/01 Jippes ir kt.“, 84 p., InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=46530&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3389081.

[127] „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)“, *supra note,* 60: 45 str. 5 d.

dėti konsultacijas su ja, siekdama, kad padėtis, dėl kurios buvo priimtas sprendimas dėl apsaugos tinkamumo pripažinimo sustabdymo, būtų ištaisyta[128].

Apibendrinant pateiktą BDAR 44 – 45 str. reguliavimo analizę, darytina išvada, kad BDAR 45 str. 3 d. įtvirtintas duomenų perdavimo pagrindas remiantis Europos Komisijos sprendimu dėl tinkamumo yra pagrindinis ir teisėkūros prioritetizuojamas teisinis mechanizmas, suteikiantis teisinį pagrindą asmens duomenų perdavimui iš Europos Sąjungos į trečiąją šalį, teritoriją ar tarptautinę organizaciją. Toks Europos Komisijos sprendimas dėl trečios šalies teritorijos ar tarptautinės organizacijos taikomo asmens duomenų apsaugos tinkamo lygio įgalina visus asmens duomenų valdytojus ir tvarkytojus be jokių papildomų specialių leidimų perduoti asmens duomenis kitiems trečiojoje šalyje (teritorijoje ar tarptautinėje organizacijoje) veikiantiems duomenų tvarkytojams.

### 2.1.2. Asmens duomenų perdavimas taikant tinkamas apsaugos priemones.

BDAR 46 str. 1 d. įtvirtinta galimybė perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai tuo atveju, jeigu nėra priimtas Europos Komisijos sprendimas dėl tinkamumo pagal BDAR 45 str. 3 d. Duomenų valdytojams arba duomenų tvarkytojams suteikiama teisė perduoti asmens duomenis į trečiąją valstybę, teritoriją arba tarptautinei organizacijai tik tuo atveju, jeigu duomenų valdytojas arba duomenų tvarkytojas yra nustatęs tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis[129].

Šios tinkamos apsaugos priemonės gali būti nustatomos vienu iš šių alternatyvių atveju:

„a) teisiškai privalomu ir vykdytinu valdžios institucijų arba įstaigų tarpusavio dokumentu;

b) įmonėms privalomomis taisyklėmis pagal BDAR 47 str.;

c) standartinėmis duomenų apsaugos sąlygomis, kurias Komisija priima laikydamasi BDAR 93 str. 2 d. nurodytos nagrinėjimo procedūros;

d) standartinėmis duomenų apsaugos sąlygomis, kurias priima priežiūros institucija ir pagal BDAR 93 str. 2 d. nurodytą nagrinėjimo procedūrą patvirtina Komisija;

[128] *Ibid*, 45 str. 6 d.

[129] „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)“, *supra note,* 60: 46 str. 1 d.

e) patvirtintu elgesio kodeksu pagal BDAR 40 str. kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis; arba

f) patvirtintu sertifikavimo mechanizmu pagal BDAR 42 str. kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis.“.[130]

Taigi, BDAR 46 str. įtvirtinti net šeši skirtingi pagrindai, kaip duomenų valdytojai ir tvarkytojai gali įteisinti asmens duomenų perdavimą į trečiąją valstybę, teritoriją arba tarptautinei organizacijai, jeigu nėra priimtas Europos Komisijos sprendimas dėl tinkamumo pagal BDAR 45 str. 3 d.

Šiuo aspektu atkreiptinas dėmesys į nedidelį skirtumą tarp aplinkybių, kuriomis BDAR 45 str. pagrindu turi įsitikinti Europos Komisija, priimdama sprendimą dėl tinkamumo, ir duomenų valdytojams ir/arba duomenų tvarkytojams, siekiant perduoti duomenis į trečiąją šalį, teritoriją ar tarptautinę organizaciją, lyginant su BDAR 46 str. pagrindu. Pagal BDAR 45 str. Europos Komisija turi įsitikinti, kad trečiojoje valstybėje, teritorijoje arba atitinkamoje tarptautinėje organizacijoje užtikrinama „tinkamo lygio apsauga“, tuo tarpu BDAR 46 str. pagrindu perduoti asmens duomenis galima tik jei „duomenų valdytojas arba duomenų tvarkytojas yra nustatęs „tinkamas apsaugos priemones“ bei suteikia galimybę naudotis „vykdytinomis duomenų subjektų teisėmis“ ir „veiksmingomis duomenų subjektų teisių gynimo priemonėmis“.

Taigi, pagrindinis skirtumas tarp BDAR 45 str. ir 46 str. įtvirtintų tinkamo asmens duomenų apsaugos lygio nustatymo pareigų yra susijęs su skirtumu tarp sąvokų „tinkamo lygio apsauga“ trečiojoje šalyje bei „tinkamų apsaugos priemonių“, taikomų duomenų tvarkytojo ar valdytojo.

Paviršutinišku vertinimu, šios sąvokos ir įtvirtintos pareigos atrodytų turėtų būti vertinamos kaip sinonimai, ypač atsižvelgiant į tai, kad jos yra įtvirtintos tame pačiame BDAR skyriuje (V skyriuje), kurio visos nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui[131].

Nors BDAR 46 str. aiškiai nenurodytas iš šio straipsnio kylančių reikalavimų,

---

[130] „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)“, *supra note,* 60: 46 str. 2 d.

[131] *Ibid*, 44 str.

susijusių su „tinkamomis apsaugos priemonėmis“, „vykdytinomis [įgyvendinamomis] teisėmis“ ir „veiksmingomis teisių gynimo priemonėmis“, pobūdis, tačiau atkreiptinas dėmesys, kad BDAR preambulės 107 p. nurodyta, kad jeigu „trečioji valstybė, teritorija arba nurodytas sektorius trečiojoje valstybėje <…> nebeužtikrina tinkamo lygio duomenų apsaugos[,] <…> perduoti asmens duomenis tai trečiajai šaliai <…> turėtų būti draudžiama, išskyrus atvejus, kai įvykdomi šiame reglamente nustatyti reikalavimai, susiję su perdavimu taikant tinkamas apsaugos priemones“.

Atitinkamai, BDAR preambulės 108 p. nurodyta, kad jei sprendimas dėl tinkamumo nepriimtas, tinkamos apsaugos priemonės, kurių pagal to paties reglamento 46 str. 1 d. turi imtis duomenų valdytojas arba duomenų tvarkytojas, turi „kompensuoti nepakankamą duomenų apsaugą trečiojoje valstybėje“ siekiant „užtikrinti, kad būtų laikomasi duomenų apsaugos reikalavimų, ir užtikrinti tvarkant duomenis Sąjungoje tinkamas duomenų subjektų teises“.

Pateiktų BDAR ir preambulės nuostatų analizė sukuria *idem per idem* situaciją, iš kurios nėra jokios logiškai priimtinos išeities. Nors BDAR preambulės 107 p. yra *expressis verbis* pripažįstama duomenų perdavimo į trečiąją šalį galimybė (nors ji ir neužtikrina tinkamo lygio duomenų apsaugos), kai duomenų tvarkytojas ar valdytojas taiko „tinkamas apsaugos priemones“, tačiau jau kitame BDAR preambulės punkte ši galimybė yra paneigiama, nes duomenų tvarkytojas ar valdytojas privalo „užtikrinti, kad būtų laikomasi duomenų apsaugos reikalavimų, ir užtikrinti tvarkant duomenis Sąjungoje tinkamas duomenų subjektų teises“, nors galimybių tai padaryti jis neturi dėl ydingo (nepakankamo) trečiosios šalies teisės į privatumą teisinio reguliavimo.

Pabrėžtina, kad Europos Sąjungos Teisingumo Teismas, komentuodamas BDAR 46 str. nurodytas sąvokas „tinkamomis apsaugos priemonėmis“, „vykdytinomis [įgyvendinamomis] teisėmis“ ir „veiksmingomis teisių gynimo priemonėmis“ *Schrems II* byloje konstatavo, jog tinkamomis apsaugos priemonėmis turi būti užtikrinta, kad asmenims, kurių asmens duomenys perduodami į trečiąją šalį remiantis standartinėmis duomenų apsaugos sąlygomis, kaip ir perduodant duomenis pagal sprendimą dėl tinkamumo, būtų suteikiamas iš esmės lygiavertis apsaugos lygis, koks garantuojamas Europos Sąjungoje[132].

Taigi, Teismas *de jure* sutapatino skirtingas BDAR 45 str. ir 46 str. įtvirtintas sąvokas „tinkamo lygio apsauga“ bei „tinkamos apsaugos priemonės“ bei paneigė BDAR

[132] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 96 p.

preambulės 107 p. įtvirtintą galimybę remtis BDAR 46 str. perduodant asmens duomenis į trečiąją valstybę, kai ta trečioji valstybė savo teisiniu reguliavimu neužtikrina „tinkamo lygio apsaugos“, kaip ji suprantama pagal BDAR 45 str.

Papildomai atkreiptinas dėmesys į BDAR 46 str. 1 d. vartojamą sąvoką „veiksmingos duomenų subjektų teisių gynimo priemonės“. Kiekviena priežiūros institucija savo teritorijoje privalo nagrinėti skundus, kuriuos pagal BDAR 77 str. 1 d. turi teisę pateikti bet kuris asmuo, kai mano, kad tvarkant jo asmens duomenis pažeistas minėtas reglamentas, ir tinkamu mastu tirti šių skundų dalyką[133]. Priežiūros institucijos privalo ypač kruopščiai išnagrinėti tokius duomenų subjektų skundus[134]. BDAR 78 str. 1 ir 2 d. kiekvienam asmeniui pripažįstama teisė imtis veiksmingų teisminių teisių gynimo priemonių, be kita ko, kai priežiūros institucija neišnagrinėja jo skundo. Atitinkamai, BDAR preambulės 141 p. taip pat įtvirtinta teisė į veiksmingą teisminę teisių gynimo priemonę pagal Europos Sąjungos pagrindinių teisių chartijos 47 straipsnį tuo atveju, jei ši priežiūros institucija nesiima veiksmų, kai tokie veiksmai yra būtini duomenų subjekto teisėms apsaugoti. Todėl BDAR 46 str. 1 d. minima sąvoka „veiksmingos duomenų subjektų teisių gynimo priemonės“ turi būti suprantama kaip asmenų turima teisė kreiptis į nešališką teismą. Šis teisinis klausimas buvo iškilęs Europos Sąjungos Teisingumo Teismui nagrinėjant bylą *Schrems II*, kuomet teismas turėjo nagrinėti *Privacy Shield* susitarimo pagrindu JAV įsteigtą ombudsmeno institutą ir nuspręsti, ar Europos Sąjungos duomenų subjektų turima galimybę kreiptis į jį gali būti laikoma „veiksminga duomenų subjektų teisių gynimo priemone“.

Galiausiai, pažymėtina, kad BDAR 47 str. įtvirtintos įmonėms privalomos taisyklių sąlygos, kurias turi patvirtinti kompetentinga priežiūros institucija BDAR 46 str. 2 d. b) p. pagrindu. Šios privalomos sąlygos nukreiptos į tinkamą duomenų subjektų teisių užtikrinimą ir jų informavimą apie turimas vykdytinas teises, susijusias su jų asmens duomenų tvarkymu, kaip antai taikomus bendruosius duomenų apsaugos principus, skundų nagrinėjimo taisykles, bendradarbiavimo su priežiūros institucija mechanizmą etc.

Apibendrinant pateiktus išaiškinimus, nurodytina, kad BDAR 46 str. 1 d. įtvirtinta antroji prioritetinė pagal hierarchiją (lyginant su BDAR 45 str. 3 d.) galimybė

---

[133] „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)“, *supra note,* 60: 57 str. 1 d. f) p.

[134] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note*, 7: 63 p.

perduoti asmens duomenis į trečiąją valstybę, teritoriją arba tarptautinei organizacijai. Duomenų valdytojams arba duomenų tvarkytojams suteikiama teisė perduoti asmens duomenis į trečiąją valstybę, teritoriją arba tarptautinei organizacijai tik tuo atveju, jeigu jie yra nustatę ir užtikrina tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis. Šios tinkamos apsaugos priemonės gali būti įtvirtinamos vienu iš šešių skirtingų būdų, įtvirtintų BDAR 46 str. 2 d.

### 2.1.3. Asmens duomenų perdavimas taikant nukrypti leidžiančias nuostatas.

BDAR 49 str. 1 d. įtvirtinta trečioji prioritetinė pagal hierarchiją (lyginant su BDAR 45 str. 3 d. bei BDAR 46 str. 1 d.) galimybė perduoti asmens duomenis į trečiąją valstybę, teritoriją arba tarptautinei organizacijai. Jame nustatyta, kad nesant sprendimo dėl tinkamumo pagal BDAR 45 str. 3 d. arba nesant nustatytų tinkamų apsaugos priemonių pagal 46 str., asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai gali būti atliekamas tik viena iš šių sąlygų:

„a) duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu po to, kai buvo informuotas apie galimus tokių perdavimų pavojus duomenų subjektui dėl to, kad nepriimtas sprendimas dėl tinkamumo ir nenustatytos tinkamos apsaugos priemonės;

b) duomenų perdavimas yra būtinas duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti arba ikisutartinėms priemonėms, kurių imtasi duomenų subjekto prašymu, įgyvendinti;

c) duomenų perdavimas yra būtinas, kad būtų sudaryta arba įvykdyta duomenų subjekto interesais sudaroma duomenų valdytojo ir kito fizinio ar juridinio asmens sutartis;

d) duomenų perdavimas yra būtinas dėl svarbių viešojo intereso priežasčių;

e) duomenų perdavimas yra būtinas siekiant pareikšti, vykdyti ar ginti teisinius reikalavimus;

f) duomenų perdavimas yra būtinas, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kitų asmenų interesai, jeigu duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo;

g) duomenys perduodami iš registro, pagal Sąjungos arba valstybės narės teisę skirto teikti informaciją visuomenei, su kuria gali susipažinti plačioji visuomenė arba bet kuris asmuo, galintis įrodyti teisėtą interesą, tačiau tik tiek, kiek konkrečiu atveju laikomasi pagal Sąjungos arba valstybės narės teisę nustatytų susipažinimo su tokiame

registre esančia informacija sąlygų.“[135]

Atkreiptinas dėmesys, kad doktrinoje pateikiamu vertinimu, atsižvelgiant į tai, kad aukščiau nurodyti duomenų perdavimo atvejai yra išimtiniai, jie turi būti aiškinami griežtai (siaurai)[136].

BDAR 49 str. 1 d. paskutinėje pastraipoje yra numatytas dar vienas asmens duomenų perdavimo pagrindas, kuris gali būti taikomas net tuo atveju, kai nėra tenkinama nė viena iš aukščiau numatytų nukrypti leidžiančių nuostatų: „perdavimas nėra kartojamas, yra susijęs tik su ribotu duomenų subjektų skaičiumi, yra būtinas įtikinamų duomenų valdytojo ginamų teisėtų interesų, kai nėra už juos viršesnių duomenų subjekto interesų ar teisių ir laisvių, tikslais, jeigu duomenų valdytojas yra įvertinęs visas su duomenų perdavimu susijusias aplinkybes ir, remdamasis tuo vertinimu, yra nustatęs tinkamas su asmens duomenų apsauga susijusias apsaugos priemones“.

Pažymėtina, kad nors BDAR 49 str. 1 d. paskutinėje pastraipoje *expressis verbis* ir nėra suformuluotas leidimas duomenų valdytojui ar tvarkytojui perduoti asmens duomenis į trečiąją šalį (yra išvardintos tik „perdavimo sąlygos“), tai laikytina formalia BDAR vertimo klaida, nes BDAR tekste anglų kalba šioje nuostatoje yra aiškiai įtvirtinta, kad asmenes duomenų perdavimas „gali įvykti“ (angl. *may take place*) kai tenkinamos toliau išvardintos sąlygos.

Taip pat atkreiptinas dėmesys, kad šis BDAR 49 str. 1 d. paskutinėje pastraipoje įtvirtintas teisinis asmens duomenų perdavimo pagrindas turi būti laikomas „paskutine priemone“ (angl. *last resort*), suteikiančia pagrindą asmens duomenų perdavimui, nes pasinaudojimas ja yra apsunkintas – jis ne tik siejamas su vienkartiniu perdavimo pobūdžiu, turi būti atliekamas duomenų valdytojo ginamais interesais (nesant viršesnių duomenų subjekto interesų ar teisių ir laisvių), tačiau apie pasinaudojimą šiuo duomenų perdavimo pagrindu duomenų valdytojas privalo pranešti priežiūros institucijai ir duomenų subjektui.

BDAR preambulė atskleidžia, kad 49 str. įtvirtintos nukrypti leidžiančios nuostatos gali būti taikomos išimtiniais atvejais, susijusiais su duomenų subjekto ar viešuoju interesu, pavyzdžiui galimybė perduoti duomenis, kai tai reikalinga dėl svarbių Europos Sąjungos ar valstybės narės teisėje įtvirtintų viešojo intereso priežasčių, arba kai

---

[135] „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)“, *supra note,* 60: 49 str. 1 d.

[136] Ioannis Ntouvas, „Exporting Personal Data to EU-based International Organizations under the GDPR” *International Data Privacy Law* 9, 4 (2019): 281.

duomenys perduodami iš teisės aktu įsteigto registro, kuris skirtas naudoti visuomenei ar teisėtų interesų turintiems asmenims (tačiau neturėtų būti perduodama registre sukauptų asmens duomenų visuma arba ištisos jų kategorijos)[137], tarptautinio keitimosi duomenimis tarp konkurencijos institucijų, mokesčių arba muitų administracijų, tarp finansų priežiūros institucijų, tarp kompetentingų socialinės apsaugos ar visuomenės sveikatos tarnybų atvejais, pavyzdžiui, kontakto atveju siekiant atsekti užkrečiamas ligas arba siekiant sumažinti ir (arba) panaikinti dopingą sporte[138] etc.

Autoriaus vertinimu, vien 49 str. 1 d. a) p. įtvirtintu pagrindu perduoti asmens duomenis į trečiąsias šalis turint duomenų subjekto sutikimą atveria *de facto* neribotas galimybes duomenų valdytojams ir tvarkytojams duomenų subjektų asmens duomenis naudoti bet kokiais jiems priimtinais ir pageidaujamais būdais. Nors doktrinoje sutinkamos nuomonės, kad asmens duomenų valdytojai ar tvarkytojai, renkantys duomenis, gali jaustis nepatogiai, informuodami duomenų subjektus apie duomenų eksportavimo riziką, o duomenų subjektai gali atsisakyti duoti sutikimą dėl asmens duomenų tvarkymą, kai apie tai bus informuoti[139], autoriaus vertinimu, dabartinis asmens duomenų apsaugos teisinis reguliavimas pažodžiui nedraudžia skaitmeninių paslaugų teikėjams primesti „priimk arba išeik“ (angl. *take it or leave it*) pasirinkimus paslaugų naudotojams, iš esmės nepalikdamas galimybės naudotis teikiama paslauga be teisės į asmens duomenų apsaugą paaukojimo paslaugos teikėjui priimtinu lygiu. Analogiškai autoriaus vertinimui, 29 straipsnio darbo grupė (angl. *Article 29 Working Party*) apie tokį prieigos prie paslaugų mechanizmą atsiliepė kritiškai, tačiau nekonstatavo, kad toks elgesys būtų draudžiamas[140].

Apibendrinant pateiktus argumentus, darytina išvada, kad BDAR 49 str. įtvirtintas itin platus sąrašas atvejų, įgalinančių asmens duomenų tvarkytojus ar valdytojus suteikti teisinį pagrindą asmens duomenų perdavimui į trečiąsias šalis, net kai nėra Europos Komisija nėra priėmusi sprendimo dėl tinkamumo (BDAR 45 str. 3 d. pagrindu) ar nėra užtikrinamos tinkamos apsaugos priemonės (BDAR 46 str. pagrindu). Autoriaus vertinimu, BDAR 49 str. reguliavimas įgalina duomenų valdytojus ir tvarkytojus

[137] „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)“, *supra note,* 60: preambulės 111 p.

[138] *Ibid*, preambulės 112 p.

[139] Ntouvas, *supra note*, 158.

[140] „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2013 m. spalio 2 d. darbinis dokumentas Nr. 02/2013 nustatantis gaires gaunant sutikimą dėl slapukų (angl. *cookies*) naudojimo“, European Commission, žiūrėta 2021 m. rugpjūčio 2 d., http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf, 5.

perduoti asmens duomenis į trečiąsias šalis nevienareikšmiškai vertintinamais atvejais, kritikuojamais tiek doktrinoje, tiek priežiūros institucijų, keliant pavojų asmens duomenų apsaugai.

### 2.1.4. Asmens duomenų perdavimo į trečiąsias šalis teisinių pagrindų tarpusavio santykis ir priklausomybė

Kaip minėta aukščiau, BDAR asmens duomenų perdavimui į trečiąsias valstybes arba tarptautinėms organizacijoms reglamentuoti yra skirtas V-asis BDAR skyrius, kuriame įtvirtinti savarankiški asmens duomenų perdavimo įteisinimo būdai. Jiems būdinga hierarchinė struktūra ir paskesnis asmens duomenų perdavimo teisinis pagrindas gali būti taikomas tik tuomet, kai aukštesnis pagal hierarchiją teisinis pagrindas neegzistuoja.

Autoriaus vertinimu, vienas pagrindinių teisinių klausimų, susijusių su šių skirtingų duomenų perdavimo į trečiąsias šalis, teritorijas ar organizacijas teisinių pagrindų galiojimu, yra tas, ar panaikinus vieną iš jų (pvz., Europos Sąjungos Teisingumo Teismui panaikinus *Privacy Shield* susitarimą sprendimu byloje *Schrems II*), duomenų perdavimas į tą pačią teritoriją yra galimas kitu teisiniu pagrindu (pvz., taikant tinkamas apsaugos priemones BDAR 46 str. pagrindu)?

Kaip minėta aukščiau, BDAR preambulės 107 p. nurodyta, kad jeigu „trečioji valstybė, teritorija arba nurodytas sektorius trečiojoje valstybėje <…> nebeužtikrina tinkamo lygio duomenų apsaugos[,] <…> perduoti asmens duomenis tai trečiajai šaliai <…> turėtų būti draudžiama, išskyrus atvejus, kai įvykdomi šiame reglamente nustatyti reikalavimai, susiję su perdavimu taikant tinkamas apsaugos priemones“. Taigi, darytina išvada, kad Europos Komisijos sprendimui dėl tinkamumo (pvz. *Privacy Shield* susitarimui) nebegaliojant, asmens duomenų perdavimas į tą pačią teritoriją kitu teisiniu pagrindu (pvz., BDAR 46 str. pagrindu) yra įmanomas – tai *expressis verbis* paminėta BDAR preambulėje.

Atitinkamai, analogišką išvadą iš pirmo žvilgsnio padarė ir Europos Sąjungos Teisingumo Teismas byloje *Schrems II* konstatuodamas, kad panaikinus *Privacy Shield* susitarimą teisinis vakuumas dėl asmens duomenų perdavimo teisinio pagrindo nebus sukuriamas: „bet kuriuo atveju, atsižvelgiant į BDAR 49 straipsnį, panaikinus sprendimą dėl tinkamumo, kaip antai „Privatumo skydo“ sprendimą, negali atsirasti tokia teisės spraga. Iš tiesų šiame straipsnyje išsamiai nustatytos sąlygos, kuriomis asmens duomenys gali būti perduodami į trečiąsias šalis nepriėmus sprendimo dėl tinkamumo

pagal minėto reglamento 45 straipsnio 3 dalį arba tinkamų apsaugos priemonių pagal to paties reglamento 46 straipsnį.“[141].

Tačiau pabrėžtina, kad tokia Europos Sąjungos Teisingumo Teismo padaryta išvada yra mažų mažiausiai kvescionuotina. Teismas toje pačioje byloje nurodė, kad BDAR V skyriuje įtvirtinti skirtingi asmens duomenų perdavimo į trečiąją šalį teisinių pagrindų reguliavimas yra vienijamas vieno tikslo – asmenims, kurių asmens duomenys perduodami į trečiąją šalį, turi būti suteikiamas iš esmės lygiavertis apsaugos lygis, koks garantuojamas Europos Sąjungoje[142].

Pats teismas konstatavo, kad JAV valdžios institucijos turi prieigą prie į JAV perduodamų duomenų; šiai prieigai netaikoma jokia teismų kontrolė; nėra pakankamai aiškiai ir tiksliai nustatytos tokio masinio asmens duomenų rinkimo apimties ribos[143]. Autoriaus vertinimu, tai buvo vieni pagrindinių argumentų, dėl kurių *Privacy Shield* susitarimas apskritai ir buvo panaikintas.

Todėl duomenų valdytojai ar tvarkytojai, pageidaujantys perduoti duomenis į trečiąją šalį, kai Europos Sąjungos Teisingumo Teismas panaikino *Privacy Shield* susitarimą, negali patys suteikti duomenų subjektams „iš esmės lygiaverčio apsaugos lygio, koks garantuojamas Europos Sąjungoje“, nes jie negali suteikti jokių teisių ar garantijų duomenų subjektams, kurios galėtų „pagerinti“ duomenų subjektų padėtį ryšium su JAV teisiniu reguliavimu suteikiamomis galimybėmis valdžios institucijoms neribotai prieiti prie Europos Sąjunugos duomenų subjektų asmens duomenų ir masinio asmens duomenų rinkimo.

Lietuvos teisės doktrinoje yra atliktas aktualus tyrimas, kuriame detaliai atskleistas asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas JAV ir iš kurio analizės darytina neabejotina išvada, kad įmonės, tvarkančios duomenis JAV, privalo paklusti JAV teisėsaugos ar žvalgybos institucijų reikalavimams juos teikti[144].

Todėl atsižvelgiant į nurodytus argumentus, autoriaus vertinimu, Europos Sąjungos Teisingumo Teismui panaikinus *Privacy Shield* susitarimą dėl to, kad JAV neužtikrina tinkamo asmens duomenų apsaugos lygio, asmens duomenų perdavimas į JAV

---

141 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 202 p.

142 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 96 p.

143 *Ibid*,183 p.

144 Stankevičiūtė, *supra not*e, 6: 2 skyrius.

ir kitais pagrindais yra negalimas, nes bet kuriam asmens duomenų perdavimo į JAV teisiniam pagrindui (t. y. BDAR 45, 46 ar 49 str. įtvirtintiems mechanizmams) yra keliamas tas pats BDAR 44 str. įtvirtintas bendrinis tikslas – neturi būti pakenkta BDAR garantuojamam fizinių asmenų apsaugos lygiui.

Taigi, kalbant apie aukščiau minėtą pavyzdį, duomenų valdytojai ir tvarkytojai objektyviai negali užtikrinti „tinkamų apsaugos priemonių" taikymo, nes tai nėra jų valioje – jie negali pakeisti JAV įstatymų ir atsisakyti suteikti JAV teisėsaugos ir žvalgybos institucijoms prieigą prie jų tvarkomų Europos Sąjungos subjektų asmens duomenų. Todėl bet kuriuo atveju, tikslas, kurio siekiant šios priemonės yra nustatomos – užtikrinti asmens duomenų apsaugos lygį, kuris yra iš esmės lygiavertis tam, kuris garantuojamas Europos Sąjungoje BDAR[145] – negalės būti pasiektas.

Apibendrinant nurodytus argumentus, autoriaus vertinimu, dėl prieštaringo BDAR preambulės 107 p. ir 44 str. reguliavimo, teisėtai perduoti asmens duomenis iš Europos Sąjungos į trečią šalį, teritoriją ar tarptautinę organizaciją bus neįmanoma tais atvejais, kai teisinis pagrindas, nustatytas BDAR 45 str. 3 d. pagrindu (pvz., *Privacy Shield* susitarimą) bus panaikintas dėl priežasčių, kurių ištaisymas nepriklauso nuo duomenų valdytojo ar tvarkytojo. Tokiu atveju, pastarieji faktiškai negalės užtikrinti „tinkamų apsaugos priemonių" duomenų subjektams BDAR 46 str. prasme, todėl asmens duomenų perdavimas į tokią trečiąją šalį (kurios atžvilgiu priimtas sprendimas dėl tinkamumo pagal BDAR 45 str. 3 d. panaikintas) bus neteisėtas.

## 2.2. Europos Sąjungos ir Jungtinių Amerikos Valstijų duomenų perdavimo susitarimai.

Nepaisant galiojančio teisinio reguliavimo, pagrindinis iššūkis dėl asmens duomenų apsaugos juos perduodant tarp Europos Sąjungos ir JAV išlieka aktualus pastarąjį dešimtmetį. Tai tiesiogiai liudija Europos Sąjungos Teisingumo Teismo sprendimai bylose *Schrems*[146] ir *Schrems II*[147], kurių pagrindu buvo panaikinti duomenų perdavimą iš Europos Sąjungos į JAV sankcionavę teisės aktai (*Safe Harbour* susitarimas – *Schrems* sprendimu, *Privacy Shield* susitarimas – *Schrems II* sprendimu).

---

[145] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II")", *supra note,* 8: 94 p.

[146] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", *supra note,* 7.

[147] Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II")*, op. cit.,* 42 p.

Tarptautinio duomenų perdavimo sistema grindžiama duomenų, kaip vieno ir bendro (pasaulinio) resurso, teritorinio suvereniteto ir žmogaus teisių pusiausvyra. Nėra universalių tarptautinį duomenų perdavimą reguliuojančių susitarimų, tačiau yra keletas minkštosios teisės priemonių. Reguliavimo dilema ir pasirinkimai tarp laisvo duomenų, informacijos ir žinių srauto, žodžio laisvės, privatumo ir duomenų apsaugos, teritorinio suvereniteto su teisėsauga ir nacionalinio saugumo tikslų, dar nėra išspręsta ir kiekvienas ginčas atspindi šį sudėtingą balanso paieškos iššūkį.

JAV mokslininkų vertinimu, Europos Sąjungos teismai nepagrįstai bando išlaikyti savo teisinės sistemos grynumą ir nėra atviri tarptautinei teisei ar orientuoti į veikiančio susitarimo tarp JAV ir Europos Sąjungos pasiekimą. Pavyzdžiui, J. Weiler, komentuodamas Europos Sąjungos Teisingumo Teismo sprendimą *Kadi* byloje[148], apibūdino Europos Sąjungos Teisingumo Teismo poziciją kaip „įsitvirtinimą į savo konstituciniame kokone, tarptautinio konteksto ignoravimą ir bylos sprendimą tik išimtinai atsižvelgiant į vidinį konstitucinį supratimą“[149]. Nors šis vertinimas pateiktas 2008 m. spręstai Europos Sąjungos Teisingumo Teismo bylai, tarp garsiausių privatumo srities JAV mokslininkų toks Europos Sąjungos Teisingumo Teismo pozicijų vertinimas gajus ir pasisakant apie *Schrems II* bylą[150].

Duomenų perdavimas tarp JAV ir Europos Sąjungos yra tik dar vienas šio sudėtingo tarptautinio susitarimo pasiekimo ir reguliavimo dilemos pavyzdys, tačiau, tikėtina vienas akivaizdžiausių ir svarbiausių. *Safe Harbour* ir *Privacy Shield* susitarimai iš tikrųjų yra sudėtingų derybų tarp Europos Komisijos ir JAV institucijų rezultatas. Visam derybų procesui bei sėkmingo susitarimo pasiekimui buvo būtinas dviejų ekonominių supervalstybių, stiprios teisinės sistemos ir galingų teismų pusiausvyros balansas.

### 2.2.1. *Safe Harbour* ir *Privacy Shield* susitarimų sudarymo istoriniai aspektai

2000-ųjų metų *Safe Harbour* susitarimas buvo pirmasis bandymas pasiekti veikiantį susitarimą dėl duomenų perdavimo tarp Europos Sąjungos ir JAV. Susitarime

---

148 „Europos Sąjungos Teisingumo Teismo 2008 m. rugsėjo 3 d. sprendimas byloje Nr. C-402/05 P ir C-415/05 P Kadi ir Al Barakaat International Foundation prieš Tarybą ir Komisiją“, InfoCuria, žiūrėta 2021 m. rugpjūčio 3 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=67611&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3395010.

149 Joseph Weiler, „Vedamasis straipsnis“, EJIL Talk 19, 5 (2009), žiūrėta 2021 m. kovo 16 d., https://www.ejiltalk.org/letters-to-the-editor-respond-to-ejil-editorials-vol-195/.

150 „Schrems II: Initial Reactions – Solove, Antonipillai, Zanfir-Fortuna, Sauer, Litt“, žiūrėta 2021 m. kovo 16 d., https://www.youtube.com/watch?v=irZHx7CI5K0.

buvo įtvirtintos duomenų perdavimo tvarkymo taisyklės, kurios turėjo būti taikomos praktikoje. Susitarimo įgyvendinimas iš JAV pusės neturėjo realių užtikrinimo mechanizmų, todėl iš esmės priklausė nuo susitariančių šalių geranoriškumo bei duomenų apsaugos institucijų turimų stebėsenos ir susitarimo priežiūros tinkamo įgyvendinimo priemonių evoliucijos ir taikymo. *Safe Harbour* susitarimo turinys buvo aktyviai analizuojamas jo galiojimo metu, nustatant kritikuotiną reguliavimą ir tobulintinas (ypač aktualios yra 2004 m.[151] bei 2008[152] m. analizės).

Jau *Safe Harbour* susitarimo galiojimo metu tapo aišku, kad nors jame nustatytos taisyklės teoriškai galėtų ir turėtų veikti, tačiau praktikoje jos neveikė – į nustatytas taisykles rimtai nežiūrėjo nei JAV bendrovės, nei Europos Sąjungos duomenų apsaugos institucijos, kurios nesinaudojo joms suteiktomis galiomis[153][154]. *Safe Harbour* susitarime nebuvo nustatyti teisėsaugos institucijų prieigos prie duomenų apribojimai ir Europos Sąjungos duomenų apsaugos taisyklių taikymas daugeliu atveju buvo negalimas. JAV institucijoms prieiga prie duomenų galėdavo būti suteikta „tiek, kiek reikia nacionalinio saugumo, viešojo intereso ar teisėsaugos reikalavimams patenkinti“ ir remiantis „įstatymais, Vyriausybės nutarimais arba precedentine teise, dėl kurių atsiranda prieštaringų įsipareigojimų ar aiškių įgaliojimų“[155]. Akivaizdu, kad šios nuostatos buvo pernelyg plačios ir negalėjo būti veiksmingos asmens duomenų apsaugos tikslu.

Atsižvelgiant į šias nuostatas ir į vėlesnius vertinimus, detalizuotus dviejuose

---

[151] „Europos Komisijos personalo 2010 m. spalio 4 d. darbinis dokumentas „Komisijos sprendimo 520/2000/EB įgyvendinimas dėl tinkamos asmens duomenų apsaugos, kurią teikia „Safe Harbor“ susitarimo privatumo principai ir su jais susiję JAV komercijos departamento dažnai užduodami klausimai“, European Commission, žiūrėta 2021 m. kovo 16 d., https://ec.europa.eu/transparency/documents-register/detail?ref=SEC(2004)1323&lang=en.

[152] Chris Connolly, „The US Safe Harbor – Fact or Fiction?“, *Galexia* (2008), žiūrėta 2021 m. rugpjūčio 3 d., https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

[153] *Ibid.*

[154] Pelez Asinari, María Verónica Pérez ir Yves Poullet. „Privacy, Personal Data Protection and the *Safe Harbour* Decision“, *The Future of Transatlantic Economic Relations: Continuity Amid Discord* 101 (2005): 888.

[155] „2000 m. liepos 26 d. Europos Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „Safe Harbor“ susitarimo privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų “Dažnai užduodamų klausimų”, priedo Nr. 1 pastr. Nr. 4., EUR-lex, žiūrėta 2021 m. kovo 16 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX-%3A32000D0520.

Europos Komisijos komunikatuose[156], Europos Sąjungos Teisingumo Teismas nesunkiai galėjo konstatuoti[157] Europos Sąjungos duomenų apsaugos taisyklių nesilaikymą ir paskelbti *Safe Harbour* susitarimą negaliojančiu. Taigi, *Safe Harbour* buvo praktikoje asmens duomenų apsaugos atžvilgiu neveikusiu susitarimu, kuris galiojo net 16 metų, iki Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje.

Naujasis *Privacy Shield* susitarimas tarp Europos Sąjungos ir JAV buvo pasiektas 2016 m. liepos 12 d. – tai yra dokumentas, kuriame tėra šeši straipsniai, tačiau net 155 preambulės punktai ir 7 priedai. *Privacy Shield* susitarimo projektas buvo kritiškai sutiktas su privatumo apsauga susijusių institucijų ir darbo grupių. 29 straipsnio darbo grupės nuomonėje[158] ir 2016 m. gegužės 30 d. Europos duomenų apsaugos priežiūros pareigūno nuomonėje[159] buvo pripažintos reguliavimo tobulinimo pastangos iš JAV pusės, susijusios su policijos ir saugumo agentūrų, žvalgybos ir slaptųjų tarnybų prieiga prie duomenų (*Privacy Shield* susitarime aiškiau įtvirtinamas duomenų panaudojimo tikslo ribojimo principas, pvz. sudaromas nusikalstamumo prevencijos, rizikos prevencijos ir nacionalinio saugumo užduočių sąrašas, įgalinantis teisėsaugos institucijas susipažinti su šiais duomenimis tik nustatytais atvejais[160]), tačiau konstatuota, kad *Privacy Shield* susitarimo projekte nebuvo visų esminių procesinių garantijų (būtinumo, proporcingumo, nepriklausomo sankcionavimo ir kt.), esmingai kritikuojamas numatyto

---

156 „Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU–US Data Flows, COM(2013) 846 fin“, EUR-lex, žiūrėta 2021 m. rugpjūčio 3 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0846.; „Communication from the Commission to the European Parliament and the Council on the Functioning of the *Safe Harbour* from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 fin“, EUR-lex, žiūrėta 2021 m. rugpjūčio 3 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013DC0847.

157 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7.

158 „29 straipsnio darbo grupės 2016 m. balandžio 13 d. nuomonė Nr. 01/2016 dėl EU – JAV privatumo skydo projekto“, European Commission, žiūrėta 2021 m. liepos 20 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

159 „Europos duomenų apsaugos priežiūros pareigūno 2016 m. gegužės 30 d. nuomonė Nr. 4/2016 dėl EU – JAV privatumo skydo projekto“, European Data Protection Supervisor, žiūrėta 2021 m. liepos 20 d., https://edps.europa.eu/sites/default/files/publication/16-05-30_privacy_shield_en.pdf .

160 „2016 m. liepos 12 d. Europos Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl Europos Sąjungos ir JAV „Privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB“, EUR-lex, žiūrėta 2021 m. liepos 20 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX%3A32016D1250, preambulės 74 p.

savireguliacijos principo efektyvumas[161].

Taigi, nuo pat *Privacy Shield* susitarimo priėmimo, jo teikiama apsauga buvo kvescionuojama teisės į privatumą apsauga suinteresuotų asmenų grupių. Neilgai trukus, kilo ginčas dėl jo teisėtumo pagal Austrijos piliečio Maximilian Schrems inicijuotą skundą Airijos duomenų apsaugos institucijai. Ginčo nagrinėjimo metu Airijos Aukščiausiajame Teisme, pastarasis bylos nagrinėjimą sustabdė ir kreipėsi į Europos Sąjungos Teisingumo Teismą su prašymu priimti prejudicinį sprendimą byloje. Airijos Aukščiausiasis Teismas prašyme Europos Sąjungos Teisingumo Teismui inter alia uždavė klausimą, susijusį su *Privacy Shield* susitarimo adekvatumu: „Ar, atsižvelgiant į [Direktyvos 95/46] 25 straipsnio 6 dalį, [„Privatumo skydo“ sprendimas] yra visuotinai taikoma išvada, privaloma valstybių narių duomenų apsaugos institucijoms ir teismams, kiek jame numatyta, kad JAV savo šalies įstatymais arba prisiimtais tarptautiniais įsipareigojimais užtikrina adekvatų apsaugos lygį, kaip tai suprantama pagal [Direktyvos 95/46] 25 straipsnio 2 dalį?“[162].

Europos Sąjungos Teisingumo Teismas, išnagrinėjęs bylą, konstatavo, kad *Privacy Shield* susitarimo 1 straipsnio 1 dalyje konstatavusi, kad JAV užtikrina tinkamą asmens duomenų perdavimą iš Europos Sąjungos šioje trečiojoje šalyje įsteigtoms organizacijoms pagal Europos Sąjungos ir Jungtinių Amerikos Valstijų sudarytą *Privacy Shield* susitarimą, Europos Komisija nesilaikė reikalavimų, kylančių iš BDAR 45 straipsnio 1 dalies, siejamos su Chartijos 7, 8 ir 47 straipsniais, todėl padarė išvadą, kad *Privacy Shield* susitarimo 1 straipsnis nesuderinamas su BDAR 45 straipsnio 1 dalimi, siejama su Chartijos 7, 8 ir 47 straipsniais, todėl negalioja[163].

Tokiu būdu, Europos Sąjungos Teisingumo Teismas, praėjus vos keturiems metams nuo priėmimo, panaikino *Privacy Shield* susitarimą – duomenų perdavimo tarp Europos Sąjungos ir JAV bendrovių teisinį pagrindą. Europos Sąjungos Teisingumo Teismo kritika *Privacy Shield* susitarimo turiniui išsamiau detalizuojama šio tyrimo 4.3.4 skirsnyje.

---

[161] Tam, kad bendrovė taptų *Privacy Shield* sistemos dalyve, ji turėjo atitinkamai pakoreguoti savo privatumo politiką, kad ši atitiktų susitarime numatytus privatumo principus. Bendrovės privalėjo kasmet peržiūrėti savo privatumo politiką bei atnaujinti narystę *Privacy Shield* sistemoje – to nepadariusios JAV organizacijos nebegalėjo gauti ir tvarkyti duomenų, gautų iš Europos Sąjungos pagal *Privacy Shield* sistemą. Plačiau apie tai – žr. „Europos Sąjungos ir JAV „Privatumo skydo“ gairės“, European Commission, žiūrėta 2021 m. kovo 16 d., http://ec.europa.eu/newsroom/document.cfm?doc_id=47770.

[162] Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note*, 8*:* 9 p.

[163] *Ibid*, 198 – 199 p.

### 2.2.2. Tarptautinė sutartis kaip geresnis reguliavimo mechanizmas

Kaip pristatyta aukščiau, Europos Sąjungos Teisingumo Teismas savo sprendimais panaikino ankstesnes Europos Sąjungos ir JAV pastangas įteisinti duomenų perdavimą – *Safe Harbour* ir *Privacy Shield* susitarimus[164].

Europos Sąjungos Teisingumo Teismas *Schrems* byloje konstatavo, kad trečiosios šalies privatumo apsaugos efektyvumas turi būti detalizuotas ir, autoriaus vertinimu, pagrįstas (įrodytas), kai šios trečiosios šalies teisinės sistemos teikiamą privatumo apsaugą siekiama laikyti lygiaverte Europos Sąjungos teikiamai apsaugai[165]. Nors JAV vykdomoms plačioms masinio asmens duomenų rinkimo ir duomenų išsaugojimo programoms (pvz. PRISM) yra taikoma griežtesnė teisinė priežiūra pagal JAV laisvės įstatymo (angl. *USA Freedom Act*) 2015 m. pakeitimus [166], tačiau Europos Sąjungos Teisingumo Teismas analizavo šių programų keliamą grėsmę bei konstatavo, kad reglamentavimas, leidžiantis valstybės institucijoms susipažinti su elektroninės komunikacijos turiniu, turi būti laikomas keliančiu pavojų Europos sąjungos pagrindinių teisių chartijos 7 straipsnyje garantuotos pagrindinės teisės į privatų gyvenimą esmei[167]. Europos Sąjungos Teisingumo Teismas taip pat įvertino JAV žvalgybos bendruomenės priežiūros ir žalos atlyginimo procedūras bei nurodė, kad reglamentavimu, nenumatančiu asmeniui jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti, nepaisoma Europos sąjungos pagrindinių teisių chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės[168].

Šiuos ir kitus *Safe Harbour* trūkumus Europos Sąjunga ir JAV mėgino išspręsti sudarydamos *Privacy Shield* susitarimą. Įvairias ir sudėtingas žalos atlyginimo procedūras *Safe Harbour* susitarime[169] siekta palengvinti, *Privacy Shield* susitarime įsteigiant

---

[164] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7; Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *op. cit,* 42 p.

[165] *Ibid* „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *op.cit.*, 74 p.

[166] „2015 USA Freedom Act“, U. S. Congress, žiūrėta 2021 m. kovo 16 d., https://www.congress.gov/bill/114th-368 congress/house-bill/2048/text.

[167] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note*, 7: 94 p.

[168] *Ibid*, 95 p.

[169] „2000 m. liepos 26 d. Europos Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „Safe Harbor“ susitarimo privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų “Dažnai užduodamų klausimų”“, *supra note,* 177: IV priedas.

ombudsmeno instituciją JAV teisinėje sistemoje[170] ir sustiprinus Europos Sąjungos valstybių narių duomenų apsaugos institucijų kontrolės teises[171]. Palyginti su *Safe Harbour* susitarimu, *Privacy Shield* susitarime numatytos išsamios (dažniausiai) administracinės leidimų suteikimo ir žalos atlyginimo procedūros[172].

Šiuo aspektu paminėtini keli naujojo *Privacy Shield* susitarimo teisinio reguliavimo trūkumai. Pirma, žalos atlyginimo ir kt. teisių pažeidimo atstatymo (angl. *redress*) procedūros nustatomos administracine tvarka ir jas gali lengvai pakeisti kita JAV vykdomoji valdžia. Antra, net po to, kai nustatomos atitikties vertinimo ir asmenų teisių užtikrinimo priemonės, taikomų procedūrų veiksmingumas gali būti įvertintas tik *ad hoc* atvejais atliekant kruopščią analizę. Todėl galutinis *Privacy Shield* susitarimo adekvatumo Europos Sąjungos garantuojamam teisių apsaugos lygiui vertinimas priklauso nuo individualių JAV pusėje veikiančių institucijų sprendimų ir nėra garantuojamas pačiu susitarimo tekstu.

Žvelgiant retrospektyviai, atrodo akivaizdu, kad Europos Sąjungos Teisingumo Teismas *Schrems II* byloje negalėjo pritarti tokiam Europos Sąjungos ir JAV pasiektam konsensusui, jame esant tvarių ilgalaikės asmenų teisių apsaugos sistemos garantijų trūkumui. Šiuo aspektu Europos Sąjungos Teisingumo Teismas konstatavo, kad nors *Privacy Shield* susitarimo 120 preambulės punkte pabrėžtas JAV Vyriausybės įsipareigojimas, kad atitinkamas žvalgybos tarnybų padalinys turės ištaisyti kiekvieną *Privacy Shield* susitarimo ombudsmeno nustatytą taikytinų normų pažeidimą, tame sprendime visiškai nenurodyta, jog šis ombudsmenas būtų įgaliotas priimti šioms tarnyboms privalomus sprendimus, taip pat nekalbama apie jokias teisines garantijas, kurios būtų siejamos su šiuo įsipareigojimu ir kuriomis galėtų remtis duomenų subjektai[173]. Todėl Europos Sąjungos Teisingumo Teismas padarė išvadą, kad nurodytu ombudsmeno mechanizmu nesuteikiama teisių gynimo priemonė institucijoje, kurioje asmenims, kurių duomenys perduodami į JAV, būtų suteiktos garantijos, iš esmės lygiavertės toms, kurios reikalaujamos Chartijos 47 straipsnyje[174].

Atsižvelgiant į tai, kad Europos Sąjungos Teisingumo Teismas panaikino abu Europos Sąjungos ir JAV mėginimus įteisinti duomenų mainų tarp Europos Sąjungos ir JAV taisykles, manytina, kad tikėtinai tvaresnis sprendimas būtų tarptautinė sutartis.

[170] „2016 m. liepos 12 d. Europos Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl Europos Sąjungos ir JAV „Privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB“, *supra note,* 182: preambulės 116 p.

[171] *Ibid*, preambulės 40 – 44 p.

[172] *Ibid*, II priedo 7 skyrius.

[173] Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 196 p.

[174] *Ibid*, 197 p.

Šią poziciją patvirtina tiek BDAR[175], tiek iki jo galiojusi direktyva 95/46[176], kuriuose nurodoma, kad Europos Komisija trečiosios šalies garantuojamo apsaugos lygio adekvatumu gali įsitikinti, kai pastarąjį trečioji šalis užtikrina savo šalies įstatymais arba tarptautiniais įsipareigojimais.

Tarptautinė JAV ir Europos Sąjungos sutartis, tikėtinai, suteiktų daug daugiau lankstumo tarp skirtingų reguliavimo metodų ir teisinių sistemų, nes parlamentai turi daug daugiau įgaliojimų kištis į žmogaus teises. Tarptautinė sutartis gali išspręsti daugumą *Safe Harbour* bei *Privacy Shield* susitarimais neišspręstų klausimų: koncepcinius skirtumus dėl asmens duomenų sampratos, skirtingų reguliavimo principų, duomenų apsaugos taisyklių, procedūrinių garantijų ir JAV žvalgybos tarnybų prieigos prie duomenų teisėtumo. Europos Sąjungos duomenų apsaugos įstatymai ir JAV privatumo taisyklės, pastarosios žvalgybos institucijų interesai bei skirtingas jų įgyvendinimas būtų pripažinti tame pačiame teisiniame lygmenyje (t. y. tarptautinėje sutartyje, o ne skirtinguose vykdomosios valdžios sprendimuose). Kaip minėta aukščiau, JAV Vyriausybė nenorėjo keisti savo įstatymų ir *Privacy Shield* susitarime įgyvendino tik administracines garantijas. Kita vertus, Europos Sąjunga gali būti lanksti, tačiau turi įvertinti, ar JAV asmens teisės privatumą apsaugos padėtis objektyviai yra priimtina. Šią dilemą galima išspręsti tarptautine sutartimi.

Šio darbo rengimo metu, diskusijų apie galimo susitarimo pasiekimą tarptautinės sutarties forma, nėra. Autoriaus vertinimu, pritartina anksčiau išsakytai JAV mokslininkų kritikai Europos Sąjungos pozicijos nelankstumo atžvilgiu, kad ji gali būti lyginama su „įsitvirtinimu į savo konstitucinį kokoną, tarptautinio konteksto ignoravimą ir bylos sprendimą tik išimtinai atsižvelgiant į vidinį konstitucinį supratimą“[177]. Šiuolaikiniame pasaulyje, kai itin socialiai reikšmingos virštinklinės paslaugos (pvz., *Facebook*, *Gmail* etc.) yra teikiamos JAV bendrovių ir, šiuo metu, visi duomenys yra perduodami *inter alia* į JAV veikiančias paslaugų teikėjų tarnybines stotis, dėl Europos Sąjungos užimamos pozicijos nelankstumo, vartotojams egzistuoja rizika netekti prieigos prie visuotinai būtinomis laikomų virštinklinių paslaugų[178].

---

[175] „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)“, *supra note,* 60: 45 str. 2 d. c) p.

[176] „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“, 25 str. 6 d., EUR-lex, žiūrėta 2021 m. liepos 22 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

[177] Weiler, *supra note*, 171.

[178] Natasha Lomas, „Max Schrems on the EU court ruling that could cut Facebook in two“, Techcrunch, žiūrėta 2021 m. kovo 16 d., https://techcrunch.com/2020/08/25/max-*Schrems*-on-the-eu-court-ruling-that-could-cut-facebook-in-two/.

## 3. Privatumo apsaugos problemos perduodant asmens duomenis tarp skirtingų teisinių sistemų pagal Europos Sąjungos Teisingumo Teismo praktiką

Ankstesnėje šio tyrimo dalyje atskleista, kad Europos Sąjungos Teisingumo Teismas savo sprendimais panaikino ankstesnes Europos Sąjungos ir JAV pastangas įteisinti duomenų perdavimą – *Safe Harbour* ir *Privacy Shield* susitarimus[179]. Todėl siekiant tinkamai suprasti, kokie teisės į privatų gyvenimą apsaugos aspektai yra svarbiausi ir, atitinkamai, problematiškiausi, mėginant užtikrinti pakankamą teisės į privatų gyvenimą apsaugą reglamentuojant duomenų perdavimą tarp Europos Sąjungos ir JAV, būtina išanalizuoti Europos Sąjungos Teisingumo Teismo praktiką (kuria ankstesni susitarimai tarp Europos Sąjungos ir JAV buvo panaikinti) bei nustatyti Europos Sąjungos Teisingumo Teismo keliamus pakankamus teisės į privatumą apsaugos kriterijus.

Autoriaus vertinimu, svarbiausi Europos Sąjungos Teisingumo Teismo sprendimai, turintys esminės įtakos teisės į privatumą apsaugos užtikrinimui, yra sprendimai *Digital Rights Ireland*[180], *Schrems*[181] bei *Schrems II*[182] bylose, kuriais buvo panaikinta atitinkamai Direktyva 2006/24/EB[183], *Safe Harbour* susitarimas bei *Privacy Shield* susitarimas. Todėl toliau siekiama pateikti Europos Sąjungos Teisingumo Teismo šiose bylose užimtas pozicijas, pateiktus išaiškinimus bei identifikuoti teisės į privatumą apsaugos kryptį, kuria Europos Sąjungos Teisingumo Teismas mėgina nukreipti visuomenę, JAV bei Europos Sąjungos institucijas savo formuojamos praktikos pagalba.

---

179 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7; Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8.

180 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.*“,* InfoCuria, *žiūrėta 2021 m. liepos 30 d.,* https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3541738.

181 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7.

182 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“*, op.cit., 42*.

183 „2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB“, EUR-lex, žiūrėta 2021 m. liepos 30 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:32006L0024.

## 3.1. Europos Sąjungos Teisingumo Teismo išaiškinimai *Digital Rights Ireland* byloje

Europos Sąjungos Teisingumo Teismas sprendimu *Digital Rights Ireland* byloje Direktyvą 2006/24 pripažino negaliojančia. Byloje kilo ginčas dėl Vokietijos ir Airijos nacionaliniuose įstatymuose įtvirtintos elektroninių ryšių paslaugų teikėjų pareigos numatytą laikotarpį (*Digital Rights Ireland* bylos atveju – 6 – 24 mėn.) saugoti turimus srauto ir vietos nustatymo duomenis nusikaltimų prevencijos, atskleidimo, tyrimo arba patraukimo už juos atsakomybėn, taip pat valstybės saugumo užtikrinimo tikslais.

Europos Sąjungos Teisingumo Teismas sprendimas *Digital Rights Ireland* byloje sukėlė didelį atgarsį tiek visuomenėje, tiek tarp teisės mokslininkų[184]. Atsižvelgdamas į tai, kad šį sprendimą savo moksliniame darbe *inter alia* jau analizavo ir Lietuvos mokslininkė[185], autorius toliau atskleis tik esminius teismo sprendimo motyvus bei atskleis proporcingumo principo reikšmę.

Europos Sąjungos Teisingumo Teismas sprendimas *Digital Rights Ireland* bylą nagrinėjo Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių į privatų ir šeimos gyvenimą ir į asmens duomenų apsaugą kontekste. Europos Sąjungos Teisingumo Teismas sprendimo motyvacinėje dalyje pirmiausiai pagrindė išvadą, kad Direktyvoje 2006/24 reikalaujant saugoti jos 5 straipsnio 1 dalyje išvardytus duomenis ir suteikiant kompetentingoms nacionalinėms institucijoms prieigą prie jų, *inter alia* riboja Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose įtvirtintas pagrindines teises[186].

Tuomet Europos Sąjungos Teisingumo Teismas analizavo, ar šios bylos atveju, Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniais įtvirtintų teisių apribojimai yra pateisinami. Šiuo aspektu, aukščiau minėtame Dalios Misiūnaitės Kamarauskienės straipsnyje yra abstrakčiai teigiama, kad „Dėl minėto apribojimo proporcingumo Teisingumo Teismas konstatavo, kad nagrinėjamas duomenų saugojimas yra

---

184 Andrew Roberts, „Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications", *Modern Law Review* 78, 3 (2015): 535-48; Rubin S. Waranch, „*Digital Rights Ireland* Deja Vu? Why The Bulk Acquisition Warrant Provisions Of The Investigatory Powers Act 2016 Are Incompatible With The Charter Of Fundamental Rights Of European Union", *The George Washington International Law Review* 50, 1 (2017): 209.

185 Dalia Misiūnaitė-Kamarauskienė, „Europos Sąjungos Teisingumo Teismo praktikos aktualijos pagrindinių teisių į privatų ir šeimos gyvenimą bei asmens duomenų apsaugą srityje ", *Jurisprudencija* 21, 4 (2014): 1233.

186 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.", *supra note,* 202: 32 – 37 p.

tinkama priemonė šios direktyvos tikslui pasiekti, tačiau nurodė, kad tokios priemonės būtinumo negali pateisinti vien kovos su sunkiais nusikaltimais tikslas, kadangi direktyva 2006/24 „<...> taikoma visoms žmonių kasdieniame gyvenime labai plačiai naudojamoms ir vis svarbesnėmis tampančioms elektroninio ryšio priemonėms [ir] <...> visiems abonentams ir registruotiems naudotojams. Taigi, ja ribojamos beveik visų Europos gyventojų pagrindinės teisės““[187].

Tuo tarpu autoriaus vertinimu, būtent proporcingumo principo taikymas ir atliko esminę reikšmę Europos Sąjungos Teisingumo Teismui priimant sprendimą šioje byloje. Nors teismas nusprendė, kad Direktyvoje 2006/24 numatyta duomenų saugojimo pareiga ir nepaneigė Europos Sąjungos pagrindinių teisių chartijoje įtvirtintos teisės į privatumą esmės[188] (nes ji nebuvo susijusi su ryšių turinio išsaugojimu ar prieiga prie jo, o terorizmo ir nusikalstamumo prevencija buvo teisėti bendro intereso tikslai), lemtingas klausimas byloje tapo tas, ar šie teisės į privatumą ribojimai buvo proporcingi.

Kalbėdamas apie proporcingumo principo esminio reikalavimo, keliamo Europos Sąjungos institucijų aktams (būti tinkamais reglamentavimo teisėtiems tikslams pasiekti ir neviršyti to, kas tinkama ir būtina jiems įgyvendinti) laikymosi teisminę kontrolę, teismas pažymėjo, kad atsižvelgiant į tai, jog ribojama teisė į privatumą yra pagrindinė, Europos Sąjungos teisės aktų leidėjo vertinimo diskrecija gali būti apribota pagal kelis kriterijus, įskaitant, be kita ko, atitinkamą sritį, Europos Sąjungos pagrindinių teisių chartija užtikrintos atitinkamos teisės pobūdį, apribojimo pobūdį, dydį ir tikslą[189].

Atsižvelgdamas į šioje byloje taikomą itin plačios apimties (turinio bei subjektų prasme) teisės į privatumą apribojimą, teismas padarė išvadą, kad Europos Sąjungos teisės aktų leidėjo vertinimo diskrecija yra nedidelė, todėl reikia taikyti griežtą kontrolę[190]. O ją taikant, dėl Direktyvos 2006/24 universalaus (t. y. neselektyvaus) taikymo visų rūšių susižinojimui visų asmenų atžvilgiu (net kai nėra jokių įrodymų apie net netiesioginį ryšį su sunkiu nusikaltimu ar grėsme nacionaliniam saugumui), Direktyvoje 2006/24 numatyti teisės į privatumą ribojimai pripažinti neproporcingais[191]. Galiausiai,

---

187 Misiūnaitė-Kamarauskienė, *supra note,* 207*:* 1240

188 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 39 p.

189 *Ibid*, 46 p.

190 *Ibid,* 48 p.

191 *Ibid*, 59 p.

efektyvių procedūrinių saugiklių nebuvimas taip pat buvo įvertintas ir su tuo susiję ribojimai pripažinti griežtesniais nei yra būtina demokratinėje visuomenėje.

Kaip patvirtina šis Europos Sąjungos Teisingumo Teismo sprendimas, vertinant pagrindinių teisių (tame tarpe ir teisės į privatumą) pažeidimus, teismas užima griežtą poziciją, taikant proporcingumo principą ribojamų teisių atžvilgiu, ypač su tuo susijusiam ribojimo būtinumo (neišvengiamumo) aspektui. Tokiu būdu, Europos Sąjungos teisės aktams, kuriais siekiama nukrypti nuo pagrindinių teisių apsaugos, taikoma itin aukšta kartelė, reikalaujanti padidinto dėmesio pagrindinių teisių ribojimams ir, iš tiesų, kuo mažesnio nukrypimo nuo teisės aktais garantuojamo pagrindinių teisių apsaugos lygio[192].

Europos Sąjungos Teisingumo Teismo sprendimo *Digital Rights Ireland* byloje motyvai nurodo, kad teismas yra linkęs prioritetizuoti teisės į privatumą, kaip vienos pagrindinių žmogaus teisių, apsaugą. Pagal sprendimo logiką ir jame pateiktus motyvus, galima daryti prielaidą, kad kuo didesnės apimties ir reikšmingesnis bus teisės į privatumą ribojimas, tuo didesnė tikimybė, kad jis bus pripažintas neproporcingu.

Primintina, kad šios bylos atveju, Europos Sąjungos Teisingumo Teismo atskirai pažymėjo ir pritarė, kad Direktyvoje 2006/24 įtvirtinti teisės į privatumą ribojimai yra nustatyti siekiant bendrojo gėrio – kovos su sunkiais nusikaltimais bei visuomenės saugumo[193], tačiau vien ši aplinkybė, teismo vertinimu, nepateisino tokio plataus masto teisės į privatumą ribojimų. Taigi, net tais atvejais, kai teisės į privatumą ribojimai nustatomi išimtinai dėl visuomenės saugumo, teisės aktų leidėjai negali būti užtikrinti, kad nustatomi teisės į privatumą ribojimai bus laikomi proporcingais.

Šiuo aspektu atkreiptinas dėmesys į doktrinoje sutinkamas nuomones, kad tokie Europos Sąjungos Teisingumo Teismo pasitelkiami standartai – t. y. bendrojo proporcingumo ir mažiausiai varžančių priemonių, yra taikomi selektyviai[194]. Kiti teisės mokslininkai identifikuoja net 8 galimas skirtingas proporcingumo principo taikymo variacijas, be aiškaus jų atskyrimo ar taikymo gairių[195]. Autoriaus vertinimu, tokia kritika Europos Sąjungos Teisingumo Teismo praktikai nėra pagrįsta. Nors Europos

[192] Marrie-Pierre Granger ir Kristina Irion, „The Court of Justice and the Data Retention Directive in *Digital Rights Ireland*: telling off the EU legislator and teaching a lesson in privacy and data protection“, *European Law Review* 39, 6 (2014): 845.

[193] „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 42 p.

[194] Wolf Sauter, „Proportionality in EU Law: A Balancing Act?“, *TILEC Discussion Paper No. 2013-003* (2013): 12.

[195] Jurgem Schwartze, *European administrative law: Revised First edition* (London: Sweet&Maxwell, 2006), 664-665.

Sąjungos Teisingumo Teismo sprendimuose ir nėra metodiškai atskleidžiama, kokios „apimties“ proporcingumo testą taikyti (pvz. bendrąjį proporcingumo vertinimą, ar griežtesnį mažiausiai varžančios priemonės testą (angl. *last resort measure*)) nustatant konkretaus teisės ribojimo netinkamumą, bet minėti mokslininkai neatsižvelgia į tai, kad teismai ir neturi kurti naujų teisės normų ar metodinių pagalbos taisyklių teisėkūros institucijoms, o turi aiškinti ir vertinti konkuruojančias ar kolizines teisės normas. Galiausiai, kritikuojant Europos Sąjungos Teisingumo Teismo praktiką neatsižvelgiama į tai, kad prejudicinių sprendimų atvejais precedentai taikomi, kai konkrečioje byloje keliami klausimai yra identiški užduotiems anksčiau spręstoje byloje ir jokios naujos aplinkybės teismui nėra nurodomos[196], t. y. kaip ir Lietuvos teisėje, teismų precedentų taikymo sąlygos yra griežtos.

Apibendrinant pateiktus argumentus, darytina išvada, kad Europos Sąjungos Teisingumo Teismui priimant sprendimą *Digital Rights Ireland* byloje esminę reikšmę turėjo būtent proporcingumo principo taikymas. Teismas, atsižvelgdamas į byloje keltą klausimą dėl taikomo itin plačios apimties (turinio bei subjektų prasme) teisės į privatumą apribojimo, jį įvertino neproporcingu ir todėl neteisėtu. Tokiu būdu Europos Sąjungos Teisingumo Teismas ne tik panaikino Direktyvą 2006/24, tačiau ir padėjo proporcingumo principo taikymo pamatus kitiems reikšmingiems sprendimams teisės į privatumą apsaugos bylose, o ypač – *Schrems* bei *Schrems II* bylose.

## 3.2. Europos Sąjungos Teisingumo Teismo išaiškinimai *Schrems* byloje

Europos Sąjungos Teisingumo Teismas sprendimu *Schrems* byloje pripažino negaliojančiu *Safe Harbour* susitarimą. Šis sprendimas yra ypač reikšmingas, kadangi juo pirmąsyk buvo panaikino teisinį pagrindą asmens duomenų perdavimui tarp Europos Sąjungos ir JAV suteikiantį susitarimą.

Šioje byloje ginčas kilo pagal Austrijos piliečio Maximilian Schrems skundą Airijos duomenų apsaugos komisarui, kuriuo buvo ginčijamas masinis asmens duomenų perdavimas iš „Facebook Ireland“ savo motininei kompanijai, esančiai JAV – „Facebook Inc.“. Europoje Facebook vartotojai privalo sudaryti sutartis su „Facebook Ireland“,

---

[196] „Europos Sąjungos Teisingumo Teismo 1963 m. kovo 27 d. sprendimas sujungtose bylose Nr. 28 iki 30-62 Da Costa en Schaake NV ir kt. prieš Administratie der Belastingen“, InfoCuria, žiūrėta 2021 m. liepos 30 d., https://curia.europa.eu/juris/showPdf.jsf?text=&docid=87133&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3549379.

kuri saugo duomenis tarnybinėse stotyse Airijoje ir perduoda duomenis į tarnybines stotis JAV. Kadangi „Facebook Inc.“ yra JAV įmonė, pagal JAV teisinį reguliavimą prieigą prie jos duomenų gali gauti ir JAV Nacionalinio saugumo agentūra (angl. *National Security Agency*). Būdamas Facebook vartotoju, *Schrems* teigė, kad „Facebook Ireland“ suteikia JAV žvalgybos agentūroms plačią prieigą prie jo asmens duomenų ir atitinkamai, kad Airijos duomenų apsaugos komisaras turėtų nurodyti „Facebook Ireland“ nutraukti asmens duomenų perdavimą JAV.

Airijos duomenų apsaugos komisaras atmetė *Schrems* skundą iš esmės remdamasis aplinkybe, kad kadangi perduoti duomenis teisę suteikia *Safe Harbour* susitarimas, o Airijos duomenų apsaugos komisaras negalėjo tirti skundo.

Atmetus jo skundą, *Schrems* kreipėsi į Airijos Aukščiausiąjį Teismą dėl teisminio Airijos duomenų apsaugos komisaro sprendimo peržiūros. Pagrindinis Airijos Aukščiausiojo Teismo klausimas buvo, ar galiojant *Safe Harbour* susitarimui, kuriuo leidžiamas duomenų perdavimas tarp Europos Sąjungos ir JAV (šiuo atveju – „Facebook Ireland“ ir „Facebook Inc.“) ir konstatuota, kad JAV suteikia adekvatų privatumo apsaugos lygį, visiškai užkirto kelią skundams dėl tokio duomenų perdavimo. Airijos Aukščiausiasis Teismas, besikreipdamas į Europos Sąjungos Teisingumo Teismą, neatskleisdamas detalios skirtingų JAV veikiančių Nacionalinės saugumo agentūrai prieinamų skaitmeninių duomenų kaupimo ir analizės sistemų (pvz. PRISM), padarė išvadą, kad asmens duomenims patekus į JAV, Nacionalinė saugumo agentūra turėjo neribotą ir kontroliuojamą prieigą prie Facebook duomenų[197].

Kadangi byloje buvo keliamas klausimas dėl *Safe Harbour* susitarimo teisėtumo pagal Direktyvą 95/46, Airijos duomenų apsaugos komisaro sprendimo peržiūrai esminę reikšmę turėjo Europos Sąjungos teisės aiškinimas, ypač atsižvelgiant į pagrindines teises, kurias garantuoja Europos Sąjungos pagrindinių teisių chartija, o Airijos nacionalinė teisė užkirto kelią *Safe Harbour* susitarimo peržiūrai, Airijos Aukščiausiasis Teismas kreipėsi į Europos Sąjungos Teisingumo Teismą iš esmės klausdamas, ar (i) nacionalinis duomenų apsaugos komisaras, nagrinėdamas skundą, susijusį su asmens duomenų perdavimu trečiajai šaliai (šiuo atveju – JAV), kurios įstatymuose ir praktikoje, pareiškėjo teigimu, nenumatyta adekvačių atitinkamo asmens teisės į privatumą apsaugos priemonių, yra absoliučiai saistomas *Safe Harbour* susitarimo, o jei taip nėra – (ii) ar jis gali ir (arba) privalo pats ištirti šį klausimą, atsižvelgdamas į per laikotarpį

[197] „Airijos Aukščiausiojo Teismo 2014 m. birželio 18 d. sprendimas byloje Nr. IEHC 310“, Bailii, žiūrėta 2021 m. liepos 30 d., https://www.bailii.org/ie/cases/IEHC/2014/H310.html.

nuo tada, kai *Safe Harbour* susitarimo buvo pirmą kartą paskelbtas, pasikeitusias faktines aplinkybes?

Europos Sąjungos Teisingumo Teismas sprendimu *Schrems* byloje pripažino, kad, pirma, *Safe Harbour* susitarimo teisėtumas gali būti tiriamas nacionalinės priežiūros institucijos (kaip Airijos duomenų apsaugos komisaras), ar trečioji šalis užtikrina tinkamą apsaugos lygį, ir, antra, kad *Safe Harbour* susitarimas, yra negaliojantis.

Vertindamas nacionalinių duomenų priežiūros institucijų įgaliojimus, Europos Sąjungos Teisingumo Teismas daug dėmesio skyrė teisiniams reikalavimams, taikomiems nacionalinėms duomenų priežiūros institucijoms, kad jos veiktų savarankiškai, kaip nustatyta Europos Sąjungos pagrindinių teisių chartijoje ir Direktyvoje 95/46. Europos Sąjungos pagrindinių teisių chartijos atžvilgiu, teismas akcentavo, kad jos 8 str. 3 d. reikalaujama, kad teisę į privatumą saugančios nuostatos būtų kontroliuojamos būtent nepriklausomos institucijos. Be to, Direktyvos 95/46 28 str. 1 d., kuri turi būti aiškinama atsižvelgiant į Europos Sąjungos pagrindinių teisių chartiją, aiškiai nurodoma, kad nacionalinės priežiūros institucijos „veiktų visiškai nepriklausomai".

Atitinkamai, *Safe Harbour* susitarimas, nors ir galiojantis, buvo privalomas Europos Sąjungos valstybėms narėms ir jų nacionalinėms duomenų priežiūros institucijoms, teismas nurodė, kad tai pastarosioms negali sudaryti kliūčų savarankiškai nagrinėti asmenų skundus (dėl duomenų perdavimo trečiosioms šalims teisėtumo) pagal Direktyvos 95/46 28 str. Šiuo aspektu teismas nurodė, kad net jei Europos Komisija yra priėmusi sprendimą pagal šios direktyvos 25 straipsnio 6 dalį (šiuo atveju – *Safe Harbour* susitarimą), nacionalinės duomenų priežiūros institucijos, kurioms asmuo yra pateikęs prašymą dėl jo teisių ir laisvių apsaugos tvarkant asmens duomenis, turi turėti galimybę visiškai nepriklausomai išnagrinėti, ar šių duomenų perdavimas atitinka Direktyvos 95/46 reikalavimus[198].

Teismas priminė, kad pagal nusistovėjusią Europos Sąjungos Teisingumo Teismo praktiką, Europos Sąjunga yra teisės sąjunga, kurioje jos institucijoms taikoma jų aktų atitikties kontrolė, būtent sutartims, bendriesiems teisės principams ir pagrindinėmis teisėms[199], todėl atitinkamai ir Europos Komisijos sprendimai, priimti pagal

---

[198] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", *supra note,* 7: 57 p.

[199] Europos Sąjungos Teisingumo Teismo 2013 m. liepos 18 d. sprendimas sujungtose bylose Nr. C-584/10 P, C-593/10 P ir C-595/10 P Komisija ir kt. prieš Kadi", InfoCuria, žiūrėta 2021 m. liepos 10 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3551313.

Direktyvos 95/46 25 str. 6 d. (*inter alia Safe Harbour* susitarimas), neturi išvengti tokios kontrolės. Tokiomis aplinkybėmis tik Europos Sąjungos Teisingumo Teismas yra kompetentingas pripažinti Europos Sąjungos teisės aktą (pavyzdžiui, pagal Direktyvos 95/46 25 str. 6 d. priimtą *Safe Harbour* susitarimą), negaliojančiu ir šia kompetencija siekiama garantuoti teisinį saugumą užtikrinant vienodą Europos Sąjungos teisės taikymą[200].

Europos Sąjungos Teisingumo Teismas pabrėžė, kad jei nacionaliniai teismai manytų, jog vienas ar keli besikreipiančio asmens skunde arba jų iniciatyva nurodyti pagrindai dėl Europos Sąjungos akto neteisėtumo yra pagrįsti (kaip buvo *Schrems* bylos atveju), jie privalo sustabdyti bylos nagrinėjimą ir kreiptis į Europos Sąjungos Teisingumo Teismą su prašymu priimti prejudicinį sprendimą dėl teisės akto (*Schrems* bylos atveju – dėl *Safe Harbour* susitarimo). galiojimo vertinimo[201].

Tokiu būdu Europos Sąjungos Teisingumo Teismas padarė išvadą, kad nors nacionalinės duomenų priežiūros institucijos pačios ir neturi teisės panaikinti jų analizuojamo Europos Komisijos sprendimo, valstybių narių nacionaliniai teisės aktai turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis nacionaliniuose teismuose kaltinimais, kurie, jos nuomone, yra pagrįsti, tam, kad šie teismai, vertindami Europos Komisijos sprendimo galiojimą, pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir ši institucija, nacionaliniai teismai turėtų abejonių dėl šio sprendimo teisėtumo[202].

Europos Sąjungos Teisingumo Teismui išnagrinėjus, kad nacionalinės duomenų priežiūros institucijos, nors pačios ir negali panaikinti konkretaus Europos Komisijos sprendimo, tačiau turi teisę kreiptis į Europos Sąjungos Teisingumo Teismą, analizė nukrypo dėl paties *Safe Harbour* susitarimo teisėtumo.

Šiuo aspektu svarbu atkreipti dėmesį, kad Europos Sąjungos Teisingumo Teismas *Schrems* sprendimo priėmimo metu (t. y. 2015 metais) turėjo vertinti *Safe Harbour* susitarimo, kuris buvo sudarytas dar 2000 m., įgyvendinimo aspektus. Ši aplinkybė sukuria ne tik faktinį neužtikrintumą (ar pagrįsta vertinti prieš daugiau nei 15 metų priimto teisės akto proporcingumą pagal šių laikų standartus), tačiau ir su tuo susijusį

---

200 „Europos Sąjungos Teisingumo Teismo 2010 m. birželio 22 d. sprendimas sujungtose byloje Nr. C-188/10 ir C-189/10 Melki ir Abdeli“, InfoCuria, žiūrėta 2021 m. liepos 10 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=80748&pageIndex=0&doclang=LT&mode=lst&dir=&occ=-first&part=1&cid=3551700.

201 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7: 64 p.

202 *Ibid*, 65 – 66 p.

teisinį neaiškumą.

Atsakymas į šį klausimą gali būti kildinamas iš Europos Sąjungos Teisingumo Teismo išaiškinimų *Jippes* byloje, kurioje teismas konstatavo, kad „Bendrijos teisės akto teisėtumas negali priklausyti nuo retrospektyvaus jo veiksmingumo įvertinimo. Kai Europos Sąjungos įstatymų leidėjas yra įpareigotas įvertinti ateityje numatomų priimti taisyklių poveikį ir tų padarinių negalima tiksliai numatyti, jo vertinimas gali būti kritikuojamas tik tuo atveju, jei jis akivaizdžiai neteisingas, atsižvelgiant į informaciją, kurią jis turėjo kvestionuojamo teisės akto rengimo metu“[203]. Todėl remiantis šia suformuota praktika, atrodytų, kad paskesni įvykiai, susiklostę po kvestionuojamo teisės akto priėmimo, neturėtų turėti lemiamos reikšmės svarstant dėl teisės akto teisėtumo.

Tačiau vėlesnėje savo praktikoje Europos Sąjungos Teisingumo Teismas atvėrė kelią aplinkybių, susiklosčiusių po kvestionuojamo teisės akto priėmimo, vertinimui, nurodydamas, kad „akto galiojimas tam tikrais atvejais gali būti vertinamas atsižvelgiant į naujas aplinkybes, atsiradusias po šio akto priėmimo“[204]. Atkreiptinas dėmesys, kad nei cituojamoje *Gaz de France – Berliner Investissement* byloje, nei ankstesn**ėje** praktikoje[205], kuria Europos Sąjungos Teisingumo Teismas rėmėsi *Gaz de France – Berliner Investissement* byloje, nors pažodžiui ir buvo paminėta galimybė remtis po teisės akto priėmimo susiklosčiusiomis aplinkybėmis, nė vienos bylos atveju situacija nebuvo pripažinta tokia išskirtine, kad pateisintų tokius išimtinius veiksmus (retrospektyvinį teisės akto vertinimą atsižvelgiant į vėlesnius įvykius).

Europos Sąjungos Teisingumo Teismas *Schrems* byloje tiesiogiai nesirėmė aukščiau nurodytomis *Jippes* ar *Gaz de France – Berliner Investissement* bylomis ar joje pateiktais išaiškinimais, tačiau konstatavo, kad svarstant *Safe Harbour* susitarimo galiojimo klausimą, taip pat reikia atsižvelgti į aplinkybes, kurios susiklostė po šio sprendimo priėmimo[206]. Nors Europos Sąjungos Teisingumo Teismas šio savo nukrypimo nuo bendros taisyklės, suformuotos ankstesnėje praktikoje *Jippes* ir *Gaz de France – Berliner*

[203] „Europos Sąjungos Teisingumo Teismo 2001 m. liepos 12 d. sprendimas byloje Nr. C-189/01 Jippes ir kt.“, *supra note*, 148: 84 p.

[204] „Europos Sąjungos Teisingumo Teismo 2009 m. spalio 1 d. sprendimas byloje Nr. C-247/08 Gaz de France – Berliner Investissement“, 50 p., InfoCuria, žiūrėta 2021 m. liepos 30 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=78359&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3552751.

[205] „Europos Sąjungos Teisingumo Teismo 1997 m. liepos 17 d. sprendimas sujungtose bylose Nr. C-248/95 ir C-249/95 SAM Schiffahrt ir Stapf prieš Bundesrepublik Deutschland“, 47 p., InfoCuria, žiūrėta 2021 m. liepos 30 d., https://curia.europa.eu/juris/showPdf.jsf?text=&docid=43712&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3553114.

[206] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7: 77 p.

*Investissement* bylose plačiau nemotyvavo, tačiau atkreiptinas dėmesys, kad generalinis advokatas Y. Bot savo išvadoje, teiktoje *Schrems* byloje, tam skyrė dėmesio. Generalinis advokatas savo išvadoje *Schrems* byloje nurodė, kad kadangi *Safe Harbour* susitarimas dėl JAV teikiamos privatumo apsaugos adekvatumo yra tęstinis, teikiamos privatumo apsaugos adekvatumo vertinimas turi keistis, atsižvelgiant į trečiojoje šalyje (t. y. JAV) vyraujančias faktines ir teisines aplinkybes[207].

Darydamas nuorodą į pateiktus išaiškinimus *Digital Rights Ireland* byloje, Europos Sąjungos Teisingumo Teismas laikė, kad atsižvelgiant, viena vertus, į asmens duomenų apsaugos svarbą pagrindinei teisei į privatų gyvenimą ir, kita vertus, į didelį asmenų, kurių pagrindinės teisės gali būti pažeistos perdavus asmens duomenis į adekvataus apsaugos lygio neužtikrinančią trečiąją šalį, skaičių, Europos Komisijos turima trečiosios šalies užtikrinamo adekvataus apsaugos lygio vertinimo diskrecija yra nedidelė, todėl reikia taikyti griežtą reikalavimų, kylančių iš su Europos Sąjungos pagrindinių Teisių Chartija siejamos Direktyvos 95/46 25 str., kontrolę[208].

Taikydamas šią griežtą kontrolę, Europos Sąjungos Teisingumo Teismas nustatė kelis *Safe Harbour* susitarimu taikomos privatumo teisės apsaugos iš JAV pusės neadekvatumo aspektus, pavyzdžiui, *Safe Harbour* susitarimu savisertifikacijos procedūra taikoma tik JAV „organizacijoms", taigi susitarime įtvirtinti teisės į privatumą apsaugos principai apskritai netaikomi JAV valdžios įstaigoms[209]; pačiame susitarime aiškiai nurodyta, kad kai JAV teisės aktai nustato *Safe Harbour* susitarimui prieštaraujančius įsipareigojimus, tiek susitarimo sistemai priklausančios, tiek nepriklausančios JAV organizacijos privalo laikytis šių teisės aktų[210].

Atsižvelgdamas į šiuos ir kitus *Safe Harbour* susitarimo trūkumus, Europos Sąjungos Teisingumo Teismas padarė išvadą, kad susitarimas nepagrįstai įgalina JAV nustatyti asmenų, kurių asmens duomenis yra arba gali būti perduodami iš Europos Sąjungos į JAV, pagrindinių teisių apribojimus, grindžiamus reikalavimais, susijusiais

---

[207] „Generalinio advokato Yves Bot išvada, pateikta 2015 m. rugsėjo 23 d. byloje Nr. C-362/14 Schrems", InfoCuria, žiūrėta 2021 m. liepos 30 d., https://curia.europa.eu/juris/document/document.jsf?-text=&docid=168421&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3553683.

[208] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", *supra note*, 7: 78 p.

[209] „2000 m. liepos 26 d. Europos Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „Safe Harbor" susitarimo privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų "Dažnai užduodamų klausimų", *supra note,* 177: priedo Nr. I pastr. Nr. 2

[210] *Ibid*, priedo Nr. IV B antraštinė dalis

su nacionaliniu saugumu, viešuoju interesu ir JAV teisės aktų laikymusi[211].

Analizuojant proporcingumo principo reikšmę Europos Sąjungos Teisingumo Teismui sprendžiant *Schrems* bylą, paminėtina, kad teismas vertindamas *Safe Harbour* susitarimą taikė ne tik bendrąjį proporcingumo principą, tačiau ir mažiausiai varžančios priemonės testą bei šiuo aspektu padarė svarbią išvadą, kad „Nėra ribojamas tuo, kas yra griežtai būtina toks reglamentavimas, kuris apskritai leidžia saugoti visų asmenų, kurių duomenys buvo perduoti iš Sąjungos į Jungtines Amerikos Valstijas, visus asmens duomenis nediferencijuojant, nenustatant jokių apribojimų arba išimčių pagal siekiamą tikslą ir nenumatant objektyvių kriterijų, leidžiančių nubrėžti ribas valstybės institucijų prieigai prie duomenų ir jų vėlesniam naudojimui konkrečiais, griežtai ribojamais ir galinčiais pateisinti apribojimą, taikomą tiek prieigai prie šių duomenų, tiek jų naudojimui, tikslais“[212].

Apibendrindamas aukščiau nurodytas išvadas, teismas nurodė, kad *Safe Harbour* susitarimo reglamentavimas, leidžiantis valstybės institucijoms susipažinti su elektroninės komunikacijos turiniu, turi būti laikomas keliančiu pavojų Europos Sąjungos pagrindinių teisių chartijos 7 straipsnyje garantuotos pagrindinės teisės į privatų gyvenimą esmei. Autoriaus vertinimu, čia slypi vienos reikšmingiausių faktinių aplinkybių skirtumų tarp *Digital Rights Ireland* ir *Schrems* bylų: *Digital Rights Ireland* bylos atveju ginčas kilo dėl Direktyvos 2006/24 pagrindu nustatytos pareigos saugoti vartotojų metaduomenis[213], tuo tarpu *Schrems* bylos atveju, (i) net ne Europos Sąjungos, o JAV institucijos turėjo prieigą (ii) ne tik prie Europos Sąjungos vartotojų metaduomenų, tačiau ir prie paties susižinojimo turinio[214]. Dėl šios aplinkybės, teisės į privatumą ribojimai *Schrems* bylos atveju laikytini žymiai reikšmingesniais, nei tie, dėl kurių ginčas kilo *Digital Rights Ireland* byloje. Atsižvelgiant į šią aplinkybę, buvo nepagrįsta iš Europos Sąjungos Teisingumo Teismo tikėtis palankesnio *Safe Harbour* susitarimo vertinimo, kai *Digital Rights Ireland* bylos atveju Direktyva 2006/24 buvo panaikinta net ne dėl tokių reikšmingų teisės į privatumą ribojimų.

Galiausiai, teismas konstatavo, kad *Safe Harbour* susitarimas turi būti supran-

---

211 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *op. cit.,* 87 p.

212 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7: 93 p.

213 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 28 p.

214 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *op. cit.*, 94 p.

tamas kaip atimantis iš nacionalinių priežiūros institucijų Direktyvos 95/46 28 str. numatytus įgaliojimus tuo atveju, kai asmuo, pateikęs pagal šią nuostatą prašymą, nurodo aplinkybes, galinčias sukelti abejonių dėl *Safe Harbour* susitarimo, kuriame remiantis šios Direktyvos 95/46 25 str. 6 d. konstatuota, jog trečioji šalis užtikrina adekvatų apsaugos lygį, suderinamumo su privataus gyvenimo ir asmens pagrindinių laisvių ir teisių apsauga, nors pati Direktyvos 95/46 25 str. 6 d., nesuteikia teisės Europos Komisijai kompetencijos riboti nacionalinių priežiūros institucijų įgaliojimų[215].

Atsižvelgiant į aukščiau pateiktus Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje motyvus dėl *Safe Harbour* susitarimo negaliojimo, iš pirmo žvilgsnio galima susidaryti nuomonę, kad sprendimas yra iš esmės grindžiamas *Safe Harbour* susitarimo teikiamos apsaugos adekvatumo vertinimu pagal Direktyvos 95/46 25 str. 1 d. Tačiau autoriaus vertinimu, kaip ir *Digital Rights Ireland* bylos atveju, šis teismo sprendimas išties yra grindžiamas proporcingumo principo taikymu trečios šalies vykdomo plataus masto duomenų rinkimo praktikai.

Nagrinėdamas šią bylą, Europos Sąjungos Teisingumo Teismas remiasi ankstesne savo praktika (įskaitant sprendimą *Digital Rights Ireland* byloje), analizuodamas ar *Schrems* bylos atveju, Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 str. įtvirtintos teisės į privatumą ribojimai yra proporcingi, griežtai būtini bei ar taikomos priemonės yra mažiausiai varžančios užsibrėžtam tikslui pasiekti. Šią poziciją autorius grindžia šiais argumentais: aukštas teisės į privatumą apsaugos lygis reiškia, kad „pakankama" trečios šalies teikiama privatumo apsauga turi būti aiškinama kaip „iš esmės lygiavertė" apsaugai, teikiamai Europos Sąjungos teisės aktais; todėl proporcingumo analizė, taikyta Europos Sąjungos teisei (pavyzdžiui, Direktyvos 2006/24 atžvilgiu *Digital Rights Ireland* byloje), turi būti analogiškai taikoma ir trečiųjų šalių (JAV – *Schrems* bylos atveju) įstatymams vertinant, ar ta jurisdikcija suteikia tinkamą apsaugą.

Šiuo aspektu paminėtina, kad Europos Sąjungos Teisingumo Teismas *Schrems* byloje tiesiogiai beveik nesirėmė ir netaikė proporcingumo principo turinio reikalavimais. Kita vertus, proporcingumo principo ir *Digital Rights Ireland* byloje suformuoti išaiškinimai, jų aktualumas bei tiesioginis pritaikomumas *Schrems* bylos atveju aiškiau atskleisti ir generalinio advokato Y. Bot išvadoje šioje byloje[216]. Neatsižvelgiant į neproporcingumą, kurį teismas konstatavo dėl nediferencijuotos universalios prieigos prie

[215] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", *supra note,* 7: 102 - 103 p.

[216] „Generalinio advokato Yves Bot išvada, pateikta 2015 m. rugsėjo 23 d. byloje Nr. C-362/14 Schrems", *supra note,* 229: 171, 177, 198 p.

asmens duomenų, autoriaus nuomone, teismo sprendimui dėl *Safe Harbour* susitarimo negaliojimo itin didelę įtaką turėjo tai, kad Europos Sąjungos duomenų subjektams nebuvo suteikta jokių veiksmingų procesinių garantijų, užtikrinančių jų teisių apsaugą pagal JAV teisinį reguliavimą, nes remiantis Europos Sąjungos Teisingumo Teismo jurisprudencija[217] ir ja aiškinančia teisės doktrina, proporcingumo nustatymui reikšmingą įtaką gali turėti procesinių garantijų buvimas – pavyzdžiui, būtent dėl procedūrinių garantijų gali būti nustatyta, kad kitu atveju vertintinas kaip reikšmingas ir esminis kišimasis į subjekto teises, yra proporcingas[218].

Apibendrinant nurodytus argumentus, Europos Sąjungos Teisingumo Teismas *Schrems* byloje priėmė neabejotinai reikšmingą sprendimą, kuris ne tik panaikino tuometinį duomenų perdavimo tarp Europos Sąjungos ir JAV teisinį pagrindą (*Safe Harbour* susitarimą) bet ir atskleidė, kokie yra galimi naujo susitarimo dėl duomenų perdavimo tarp Europos Sąjungos ir JAV kontūrai. Kita vertus, autoriaus vertinimu, sprendimas *Schrems* byloje neišsprendė ypač sudėtingų klausimų, susijusių su tuo, ar žvalgybos institucijų masinis, nediferencijuotas asmens duomenų rinkimas apskritai gali būti pateisinamas, nors šis klausimas liko neatsakytas dar nuo Europos Sąjungos Teisingumo Teismo sprendimo *Digital Rights Ireland* byloje. Net ir po *Schrems* byloje pateiktų išaiškinimų, Europos Komisija negalėjo būti užtikrinta, ar valstybių narių taikomi privatumo apribojimai, susiję su valstybių narių nacionaliniu saugumu, gali būti taikomi trečiai šaliai bei ar prieinamesnės (ar paprastesnės) teisės į privatumą gynimo priemonės trečiojoje šalyje, gali atsverti trečiosios šalies taikomus teisės į privatumą ribojimus. Todėl po teismo sprendimo *Schrems* byloje, tarp Europos Sąjungos ir JAV buvo sudarytas *Privacy Shield* susitarimas, kuris ir vėl atsidūrė ant Europos Sąjungos Teisingumo Teismo darbo stalo.

## 3.3. Europos Sąjungos Teisingumo Teismo išaiškinimai *Schrems II* byloje

Europos Sąjungos Teisingumo Teismui sprendimu *Schrems* byloje panaikinus *Safe Harbour* susitarimą, Europos Komisija priėmė *Privacy Shield* susitarimą. Pagal šį naują asemns duomenų perdavimą tarp Europos Sąjungos ir JAV reglamentuojantį

[217] „Europos Sąjungos Teisingumo Teismo 2005 m. liepos 12 d. sprendimas sujungtose bylose C154/04 ir C155/04 Alliance for Natural Health ir kt.“, InfoCuria, žiūrėta 2021 m. liepos 5 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=60405&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3555378.

[218] Sauter, *supra note*, 216: 14.

susitarimą, JAV buvo sukurtas nepriklausomas *Privacy Shield* ombudsmenas, kuriam buvo pavesta prižiūrėti įsikišimus į duomenų mainų procedūrą dėl nacionalinio saugumo intereso užtikrinimo taikomų ribojimų. *Privacy Shield* susitarime JAV atžvilgiu taip pat buvo numatyti išsamūs įsipareigojimai dėl teisės į privatumą ribojimų ir apsaugos priemonių, susijusių su prieiga prie duomenų nacionalinio saugumo tikslais.

Nors šio tyrimo rengimo metu, Lietuvos doktrinoje Europos Sąjungos Teisingumo Teismo sprendimas *Schrems II* byloje dar nėra išsamiai analizuotas, tačiau užsienio mokslininkų darbuose[219] jau yra pateikiama *Schrems II* sprendimo analizė. Atsižvelgdamas į tai, autorius toliau išsamiai nedetalizuos Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje motyvų, o tik pateiks bendrą jų apžvalgą ir akcentuos pagrindinę teisinę problemą, kuri, autoriaus vertinimu, kelia didžiausią iššūkį sėkmingo susitarimo tarp Europos Sąjungos ir JAV dėl duomenų perdavimo pasiekimui.

Prieš pasisakant dėl teismo išaiškinimų apie *Privacy Shield* susitarimo esmę bei byloje keliamų aplinkybių atitiktį BDAR reikalavimams, atkreiptinas dėmesys, kad „Facebook Ireland", Vokietijos ir Jungtinės Karalystės Vyriausybės bylos nagrinėjimo metu užėmė pozicijas, kad prašymas priimti prejudicinį sprendimą šioje byloje apskritai yra nepriimtinas, nes prašymą priimti prejudicinį sprendimą pateikęs teismas formulavo prejudicinius klausimus, remdamasis tik Direktyvos 95/46 nuostatomis (kuri bylos nagrinėjimo metu jau nebegaliojo ir ją pakeitė BDAR) bei prejudiciniai klausimai yra hipotetiniai (nes besikreipiantis teismas nekonstatavo, kad asmens duomenys iš tikrųjų buvo perduoti Europos Komisijos įgyvendinimo sprendimo (ES) 2016/2297[220] pagrindu). Teismas su šiais argumentais nesutiko ir nurodė, kad šiuo atveju prašymas priimti prejudicinį sprendimą yra priimtinas, nes jame nurodytos faktinės ir teisinės aplinkybės, kurių pakanka, kad būtų galima suprasti prejudicinių klausimų turinį ir Europos Sąjungos Teisingumo Teismo turimoje bylos medžiagoje nėra jokių duomenų, kuriais remiantis būtų galima konstatuoti, jog prašomas Europos Sąjungos teisės išaiškinimas

---

[219] Žr. pvz., Ursula Sury, „Die Auswirkungen Des EuGH-Urteils C-311/18 "*Schrems*-II" Auf Den Datenaustausch Mit Den USA", *Informatik-Spektrum* 43, 5 (2020): 354; Marc Rotenberg, „*Schrems II*, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection", *European Law Journal: Review of European Law in Context* 26, 1-2 (2020): 141-152; Xavier Tracol, „*Schrems II*": The Return of the Privacy Shield", *The Computer Law and Security Report 39 (2020): The Computer Law and Security Report* 39 (2020).

[220] „2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimas (ES) 2016/2297 kuriuo iš dalies keičiami sprendimai 2001/497/EB ir 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosioms šalims ir tokiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas", EUR-lex, žiūrėta 2021 birželio 20 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016D2297.

yra nesusijęs su ginčo pagrindinėje byloje aplinkybėmis arba hipotetinis, be kita ko, dėl to, kad pagrindinėje byloje nagrinėjamas asmens duomenų perdavimas grindžiamas aiškiu duomenų subjekto sutikimu su šiuo perdavimu, o ne Europos Komisijos įgyvendinimo sprendimu Nr. 2016/2297[221].

Nustatęs, kad prašymas priimti prejudicinį sprendimą yra priimtinas, Europos Sąjungos Teisingumo Teismas perėjo prie prejudicinių klausimų analizės. Pirma, teismas konstatavo, kad BDAR 2 straipsnio 1 ir 2 dalys turi būti aiškinamos taip, kad į šio reglamento taikymo sritį patenka asmens duomenų perdavimas, atliktas komerciniais tikslais valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, nepaisant to, ar atliekant šį perdavimą arba po jo atitinkamos trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais[222].

Tuomet teismas nurodė, kad vertinant perduodamų duomenų į trečiąją šalį teisėtumą, reikia atsižvelgti ir į duomenų valdytojo ar jo duomenų tvarkytojo, įsteigtų Europos Sąjungoje, ir perduodamų duomenų gavėjo, įsteigto atitinkamoje trečiojoje šalyje, sudarytų sutarčių sąlygas, ir, kiek tai susiję su galima šios trečiosios šalies valdžios institucijų prieiga prie taip perduotų asmens duomenų, į atitinkamus šios šalies teisinės sistemos aspektus, be kita ko, nurodytus BDAR 45 str. 2 d.[223].

Pasisakydamas dėl nacionalinių duomenų priežiūros institucijų reikšmės ir turimų įgaliojimų, Europos Sąjungos Teisingumo Teismas pabrėžė, kad Europos Komisijai pagal BDAR 46 str. 2 d. c) p. pripažintais įgyvendinimo įgaliojimais priimti standartines duomenų apsaugos sąlygas nėra suteikiama kompetencija apriboti priežiūros institucijų pagal šio reglamento 58 str. 2 d. turimus įgaliojimus, todėl nebent Europos Komisija yra teisėtai priėmusi sprendimą dėl tinkamumo, kompetentinga priežiūros institucija turi sustabdyti arba uždrausti duomenų perdavimą į trečiąją šalį, grindžiamą Europos Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis, jei, atsižvelgdama į visas konkrečias šio perdavimo aplinkybes, mano, kad šioje trečiojoje šalyje šių sąlygų nesilaikoma arba jų negalima laikytis ir kad kitomis priemonėmis negalima užtikrinti pagal Sąjungos teisę, visų pirma pagal BDAR 45 bei 46 str. ir Europos Sąjungos pagrindinių teisių chartiją, reikalaujamos perduodamų duomenų apsaugos[224].

---

221 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8*:* 74 p.

222 *Ibid*, 89 p.

223 *Ibid*, 105 p.

224 *Ibid*, 121 p.

Pasisakydamas dėl *Privacy Shield* susitarimo galiojimo, Europos Sąjungos Teisingumo Teismas, kaip ir anksčiau analizuotų bylų atveju (t. y. *Digital Rights Ireland*, *Schrems* bylos) rėmėsi proporcingumo principu ir nustatė, kad JAV taikomi duomenų apsaugos apribojimai pažeidžia proporcingumo principą[225]. Teismas pažymėjo, kad siekiant įvykdyti proporcingumo reikalavimą, kad nukrypti nuo asmens duomenų apsaugos leidžiančios nuostatos ir šios apsaugos apribojimai neviršytų to, kas yra griežtai būtina, nagrinėjamame suvaržymą nustatančiame teisės akte turi būti numatytos aiškios ir tikslios taisyklės, kuriomis būtų reglamentuojama atitinkamos priemonės apimtis ir taikymas bei nustatomi minimalūs reikalavimai, kad asmenims, kurių duomenys perduodami, būtų suteikta pakankamai garantijų, leidžiančių veiksmingai apsaugoti jų asmens duomenis nuo piktnaudžiavimo pavojų, o visi teisės aktai, pažeidžiantys Europos Sąjungos duomenų subjekto teises į duomenų privatumą, turi būti apriboti tik tuo, kas būtinai būtina[226].

Atsižvelgdamas į šiuos argumentus, Europos Sąjungos Teisingumo Teismas pirmiausia konstatavo, kad JAV nacionalinis saugumas, viešasis interesas, teisėsaugos interesai pagal *Privacy Shield* susitarimą turi viršenybę ir gali riboti pagrindines Europos Sąjungos subjektų teises (t. y. jas pažeisti), tačiau JAV teisės aktai nėra pakankamai apibrėžti, kad Europos Sąjungos subjektų privatumo apsauga būtų iš esmės lygiavertė tokiai, kurią užtikrinta Europos Sąjungos Pagrindinių Teisių Chartija[227]. Todėl teismas padarė išvadą, kad JAV duomenų apsaugos apribojimai pažeidžia proporcingumo principą, nes JAV vykdomos asmens duomenų rinkimo ir analizės programos (pvz. PRISM, UPSTREAM) nenustato „minimalių apsaugos priemonių" ir nėra „apribotos tuo, kas griežtai būtina".

Galiausiai, Europos Sąjungos Teisingumo Teismas pabrėžė, kad JAV įstatymai nenumato veiksmingų teisių gynimo būdų Europos Sąjungos subjektams, kurių duomenų privatumas buvo pažeistas ir tai galutinai patvirtino *Privacy Shield* susitarimo neproporcingumą[228].

Šiais pagrindiniais argumentais Europos Sąjungos Teisingumo Teismas padarė išvadą, kad ir antrasis Europos Sąjungos ir JAV bandymas supaprastinti duomenų perdavimą (sudarant *Privacy Shield* susitarimą) yra neproporcingas galimiems teisės į privatumą ribojimams JAV ir todėl yra negaliojantis.

---

225 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II")", *supra note,* 8*:* 184 p.

226 *Ibid*, 176 p.

227 *Ibid*, 185 p.

228 *Ibid*, 190 p.

## 4. Skirtingas nacionalinio saugumo teisinis reglamentavimas - esminė privatumo apsaugos elektroninėje erdvėje teisinių sistemų sąveikos problema: samprata, esminiai principai, turinys, teismų praktikos tendencijos

Kaip rodo Europos Sąjungos Teisingumo Teismo praktika, teisėkūra duomenų apsaugos srityje tobulėja ir aktualios asmens duomenų perdavimo tarp Europos Sąjungos ir JAV problemos kinta – panaikinus *Safe Harbour* susitarimą, jį pakeitęs *Privacy Shield* susitarimas doktrinoje buvo vertinamas žymiai palankiau[229]. Tačiau nepaisant to, Europos Sąjungos Teisingumo Teismo sprendimu *Schrems II* byloje panaikinus *Privacy Shield* susitarimą, akivaizdu, kad ne visos grėsmės teisės į privatumą apsaugai (kokias jas identifikuoja Europos Sąjungos Teisingumo Teismas) yra pašalintos arba suvaldytos.

Autoriaus vertinimu, kai kurie Europos Sąjungos Teisingumo Teismo *Schrems II* sprendime įvardinti *Privacy Shield* susitarimo trūkumai yra, neabejotinai, pataisomi. Nors teismo pateikta kritika *Privacy Shield* susitarime įtvirtintam ombudsmenui (kad jis negali būti prilygintas teismui, kaip jis suprantamas pagal Europos Sąjungos Pagrindinių Teisių Chartijos 47 straipsnį[230]), JAV teisės doktrinoje sutinkama ypač kritiškai, nes teigiama, kad teismas neatsižvelgė į tai, kad jei kuris nors ombudsmenui pateiktas skundas patvirtina JAV įstatymų pažeidimą, neteisėtai surinkti duomenys pašalinami iš JAV vyriausybės duomenų bazių ir pašalinami iš JAV žvalgybos institucijų ataskaitų[231]. Atsižvelgiant į Europos Sąjungos Teisingumo Teismo motyvus bei į JAV teisės doktrinoje pateikiamus argumentus apie *Privacy Shield* susitarime įtvirtinto ombudsmeno įgaliojimus, šią problemą neabejotinai galima išspręsti, kaip netiesiogiai *Schrems II* sprendime siūlo pats teismas, suteikiant ombudsmenui ypatingas garantijas, kurios pašalintų abejones dėl ombudsmeno nepriklausomumo nuo vykdomosios valdžios[232].

Tačiau ne visi Europos Sąjungos Teisingumo Teismo *Schrems II* sprendime pa-

---

229 Rotenberg, *supra note*, 241.

230 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 168 p.

231 „National Security Law - Surveillance - Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield – Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.,* ECLI:EU:C:2020:559 (July 16, 2020)”, *Harvard Law Review* 134, 4 (2021): 1571, žiūrėta 2021 m. rugpjūčio 2 d., https://harvardlawreview.org/2021/02/data-protection-commissioner-v-facebook-ireland-ltd/.

232 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *op. cit.,* 195 p.

teikti privatumo apsaugos iššūkiai JAV teisinėje sistemoje yra tokie paprastai išsprendžiami. Sprendimai *Schrems* ir *Schrems II* bylose tiesiogiai nurodo, kad Europos Sąjungos Teisingumo Teismas tikisi, kad JAV pakeis savo vidaus įstatymus dėl asmens duomenų (ar bent jau gaunamų iš Europos Sąjungos) tvarkymo ir teisėsaugos institucijų prieigos prie jų, tačiau, akivaizdu, JAV iki šiol to nenorėjo daryti ir JAV vyriausybė nesuteikia jokių vilčių dėl galimo pozicijos pasikeitimo[233].

Autoriaus vertinimu, *Schrems II* sprendime, JAV atžvilgiu yra identifikuotas privatumo apsaugos trūkumas, kuris gali būti laikomas kertiniu, keliančiu rimtą abejonę dėl galimybės ateityje pasiekti sėkmingą susitarimą dėl asmens duomenų perdavimo iš Europos Sąjungos į JAV. Vienas pirmųjų teismo šioje byloje nagrinėtų (ir mažiausiai motyvuotas) klausimų – ar BDAR yra taikomas asmens duomenų perdavimui, atliktam valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, jei atliekant šį perdavimą ar po jo, šios trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais.

Teismas padarė išvadą, kad priešingai nei Europos Sąjungos valstybei narei, trečiajai šaliai tvarkant duomenis, gautus iš Europos Sąjungos, BDAR yra taikomas net tuomet, kai jie yra tvarkomi trečiosios šalies nacionalinio saugumo tikslais. Todėl prieš pasisakant dėl šios teismo pozicijos pagrįstumo ir svarbos, yra reikšminga išanalizuoti nacionalinio saugumo sampratą.

## 4.1. Nacionalinio saugumo samprata

Atkreiptinas dėmesys, kad nacionalinio saugumo samprata Lietuvos teisės doktrinoje išsamiai nebuvo analizuota. Viename šiam tyrimui aktualiame darbe, yra detaliai atskleistas asmens duomenų rinkimas elektroninėje erdvėje žvalgybos tikslais[234], tačiau dėmesio pačiai nacionalinio saugumo sampratai, ką ji apima ir kokios problemos asmens duomenų apsaugai dėl to gali kilti – minėtame darbe nebuvo atskleista. Todėl toliau autorius pateiks nacionalinio saugumo sampratos analizę, jos teisinį reguliavimą Lietuvoje, tačiau nedetalizuos kitų mokslininkų tyrimuose jau aptarto reglamentavimo, kokie žvalgybos subjektai nacionalinį saugumą gina bei kokiais teisiniais pagrindais jie veikia.

Šiandien Europos Sąjunugos teisiniame reguliavime ir tarptautinėse sutartyse

---

233 Tracol, *supra note*, 241: 6.1.3 p.
234 Stankevičiūtė, *supra note*, 6: 4.2 skyrius

nėra vieno visuotinai priimtino apibrėžimo, ką apima sąvoka nacionalinis saugumas[235]. Kai kurios šalys pateikia savo teisinius apibrėžimus, tačiau jie taikomi tik toje konkrečioje teritorijoje, pavyzdžiui nacionalinio saugumo samprata yra įtvirtinta Vengrijos saugumo tarnybų įstatyme, kuriame nacionalinis saugumas apibrėžiamas kaip suverenumo ir saugumo užtikrinimo interesas[236], o Lietuvoje yra įtvirtintas nacionalinio saugumo objektų sąrašas[237].

Nacionalinio saugumo samprata įprastai yra siejama su žvalgybos tarnybų vykdoma stebėjimo veikla ir glaudžiai susijusi su informacijos rinkimu ir tvarkymu. Pirmoji iškylanti problema yra ta, kad ne visada lengva (ar apskritai įmanoma) nustatyti, ar konkretūs duomenys buvo tvarkomi teisėsaugos tikslais, ar nacionalinio saugumo užtikrinimo tikslais, kaip žvalgybos tarnybų veiklos dalis, nors skirtumas tarp teisėsaugos institucijų veiklos bei tikslų ir nacionalinio saugumo užtikrinimo yra pripažįstamas.

Pavyzdžiui, JAV žvalgybos institucijų atliekami tyrimai dėl nacionalinio saugumo identifikuojami kaip įprastai susiję su trijų rūšių grėsmėmis: tarptautiniu terorizmu, šnipinėjimu ir kita žvalgybos veikla, sabotažu ar nužudymu, kuris atliekamas užsienio valstybių, organizacijų ar asmenų vardu ir užsienio šalių įsilaužimai į kompiuterines sistemas[238]. Tuo tarpu teisėsaugos institucijų tikslas visuomet yra baudžiamasis persekiojimas; nors tyrimų metu ir gali būti fakultatyvių uždavinių, pavyzdžiui, sulaikyti ar sunaikinti narkotikus, grąžinti pavogtą turtą ir pan., tačiau pats baudžiamasis persekiojimas yra neatsiejamas ir visuomet siekiama nuo kaltųjų nuteisimo[239]. Papildomi teisiniai ir politiniai klausimai, pvz., diplomatinės neliečiamybės taikymas užsienio agentams, teroristinių veiklų organizatorių faktinis buvimas užsienyje stabdo ar net užkardo baudžiamąjį persekiojimą šių asmenų atžvilgiu nacionalinio saugumo tyrimų atvejais. Galiausiai, ilgalaikiai nacionalinių saugumo tyrimų bei jį vykdančių subjektų tikslai taip pat turi įtakos nereikšti kaltinimų konkretiems asmenims ar vengti viešo

[235] „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2014 m. gruodžio 5 d. darbinis dokumentas Nr. WP228 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais“, European Commission, žiūrėta balandžio 20 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf, 2.

[236] „Vengrijos saugumo tarnybų įstatymas“, 74 str. a) p., žiūrėta 2021 m. liepos 10 d., https://www.legislationline.org/download/id/4443/file/Act_National_Security_Service_1995_en.pdf.

[237] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, priedėlio 2 skyriaus I skirsnis., LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

[238] „Generalinio advokato nacionalinių FTB operacijų gairės“, Jungtinių Amerikos Valstijų Teisingumo departamentas, žiūrėta 2021 m. rugpjūčio 2 d., https://www.justice.gov/archive/opa/docs/guidelines.pdf, 7.

[239] L. Rush. Atkinson, „The Fourth Amendment's National Security Exception: Its History and Limits”, *Vanderbilt Law Review* 66, 5 (2013): 1349.

proceso, nes, pavyzdžiui, bendradarbiavimas su demaskuotu šnipu gali būti naudingesnis nei jo įkalinimas, arba inicijuojant viešą procesą kyla didelė rizika dėl taikytų slaptų priemonių ir resursų (įskaitant asmenis) atskleidimo[240]. Su tokiomis problemomis ir klausimais nėra susiduriama teisėsaugos veikloje, tačiau jie kyla vykdant tyrimus nacionalinio saugumo klausimais. Apskritai, nacionalinio saugumo tyrimuose nusikalstamos veikos nebūtinai yra jų epicentre, nes nacionalinio saugumo veikla teikia kritinę informaciją, reikalingą platesnei analizei ir žvalgybos tikslams (prieš tuos, kurie gali pakenkti valstybės interesams)[241], o ne siekia patraukti konkrečius asmenis baudžiamojon atsakomybėn. Todėl vien dėl šių priežasčių nacionalinio saugumo veikla laikytina pakankamai unikalia, kad visuomenė plačiąja prasme (t. y. teismai, teisėkūros subjektai ir vykdomoji valdžia) šias veiklas traktuotų kitaip, nei klasikines teisėsaugos operacijas.

Taigi, nors egzistuoja žinomi teisiniai skirtumai tarp žvalgybos tarnybų tvarkomų ir teisėsaugos institucijų tvarkomų duomenų ir jie reguliuojami skirtingais teisės aktais[242], teisės mokslininkai sutaria, kad riba tarp žvalgybos veiklos (kuria saugomas nacionalinis saugumas) ir kriminalinės žvalgybos (kurios pagrindu kovojama su nusikalstamumu) riba yra ne tik nėra aiški, bet ir laikytina nykstančia[243]. Autoriaus vertinimu, pagrindinė to priežastis yra būtent griežtos ir vieningos nacionalinio saugumo sampratos nebuvimas.

Atkreiptinas dėmesys, kad Europos Sąjungos teisės mokslininkų vertinimu, taip buvo ne visuomet, tačiau link didesnio tarnybų bendradarbiavimo, o kartu – ir tų pačių asmens duomenų naudojimo, daugelyje pasaulio šalių yra kryptingai judama. Pavyzdžiui, Vokietijoje vis dar galioja išsiskyrimo įstatymas, kuris paskirsto vaidmenis tarp žvalgybos ir teisėsaugos institucijų[244]. Kita vertus, JAV atskyrimas tarp kriminalinės ir nacionalinės žvalgybos institucijų veiklos nyksta po *Patriot Act* įstatymo priėmimo,

240 Serrin Turner ir Stephen J. Schulhofer, *The Secrecy Problem in Terrorism Trials. Brennan Center for Justice* (2005), žiūrėta 2021 m. kovo 30 d., https://www.brennancenter.org/sites/default/files/legacy/publications/20050000.TheSecrecyProbleminTerrorismTrials.pdf.

241 Atkinson, *supra note,* 261.

242 Pavyzdžiui, Lietuvoje kriminalinės žvalgybos veikla reguliuojama „Lietuvos Respublikos kriminalinės žvalgybos įstatymu“, LRS, žiūrėta rugpjūčio 3 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.434526/asr.; žvalgybos veikla – „Lietuvos Respublikos žvalgybos įstatymu“, LRS, žiūrėta rugpjūčio 3 d., https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167549.

243 „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2014 m. gruodžio 5 d. darbinis dokumentas Nr. WP228 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais“, *supra note,* 194;

Brittany Adams, „Striking A Balance: Privacy And National Security In Section 702 U.S. Person Queries”, *Washington Law Review* 94, 1 (2019): 404.

244 Claudia Hillebrand, „Counter-Terrorism Networks in the European Union: Maintaining Democratic Legitimacy After 9/11“, *Terrorism and Political Violence* 26, 4 (2014): 727-28.

kai teisėsaugos institucijoms tampa prieinamos priemonės, kuriomis anksčiau galėjo naudotis tik nacionalinį saugumą užtikrinančios žvalgybos institucijos[245]. Atitinkamai, bendradarbiavimas tarp nacionalinių žvalgybos institucijų yra skatinamas tarptautiniu lygiu visoje Europos Sąjungoje[246], o Lietuvoje – ir bendradarbiavimas tarp žvalgybos institucijų ir kriminalinės žvalgybos institucijų[247].

Taigi, nepaisant aiškios nacionalinio saugumo sampratos nebuvimo, bendradarbiavimas tarp nacionalinį saugumą užtikrinančių žvalgybos institucijų tarpusavyje bei su kriminalinę žvalgybą atliekančiomis institucijomis stiprėja tiek nacionaliniu, tiek tarptautiniu lygmeniu. Kartu pabrėžtina, kad nors nacionalinio saugumo sąvoka ir nėra įtvirtinta, tačiau ji minima įvairiuose Europos Sąjungos teisės aktuose bei vartojama kartu su kitomis sąvokomis, kurias sunku atskirti nuo nacionalinio saugumo.

Pavyzdžiui, Sutartyje dėl Europos Sąjungos veikimo įtvirtintas atskiras skyrius, skirtas laisvės, saugumo ir teisingumo erdvei. Šiame skyriuje *inter alia* įtvirtinta Europos Sąjungos kompetencija nustatyti teisinių priemonių sistemą, skirtą kovai su terorizmu ir su juo susijusiais nusikaltimais[248]. Teisės doktrinoje teigiama, kad terorizmas ir teroristiniai nusikaltimai yra laikomi nusikaltimais keliančiais pavojų nacionaliniam saugumui[249]. Analogiškai, pagal 29 straipsnį įkurtos darbo grupės vertinimą, atskirti nacionalinį saugumą ir kovą su terorizmu vargiai įmanoma[250]. Papildomai atkreiptinas dėmesys, kad Europos Sąjungos ir valstybės narės glaudžiai bendradarbiauja su JAV kovodamos su terorizmu (pavyzdžiui, dalydamosi finansinių sandorių informacija, kuri bus analizuojama pagal Terorizmo finansavimo sekimo programą (TFSP)). Pagrindinio TFSP susitarimo taikymo sritis apima prevenciją veiksmų, kurie rimtai destabilizuotų ar sunaikintų pagrindines politines, konstitucines, ekonomines ar socialines šalies ar tarptautinės organizacijos struktūras[251]. Be to, pagal Sutarties dėl Euro-

[245] Els De Busser, „EU Data Protection in Transatlantic Cooperation in Criminal Matters Will the EU Be Serving Its Citizens an American Meal?", *Utrecht Law Review* 6, 1 (2010): 98.

[246] *Surveillance by Intelligence Services: fundamental rights safeguards and remedies in the EU* (Luxembourg: Publications Office, 2017), 101, žiūrėta 2021 rugpjūčio 3 d., https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

[247] „Lietuvos Respublikos kriminalinės žvalgybos įstatymas", *supra note,* 264: 18 str. 2 d. 3 p.

[248] „Sutartis dėl Europos Sąjungos veikimo", *supra note*, 54: 75 str.

[249] Stankevičiūtė, *supra note,* 6: 176.

[250] „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2014 m. gruodžio 5 d. darbinis dokumentas Nr. WP228 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais", *supra note,* 257: 23.

[251] „Europos Sąjungos ir Jungtinių Amerikos Valstijų 2010 m. liepos 27 d. susitarimas dėl finansinių mokėjimų pranešimų duomenų tvarkymo ir perdavimo iš Europos Sąjungos į Jungtines Valstijas terorizmo finansavimo sekimo programos tikslais", 2 str. iii p., EUR-lex, žiūrėta rugpjūčio 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32010D0412.

pos Sąjungos veikimo 2 str. 4 d., Europos Sąjungos kompetencijai priklauso apibrėžti ir įgyvendinti bendrą užsienio ir saugumo politiką. Taigi, priešingai nei „nacionalinis saugumas“ (vadovaujantis Sutarties dėl Europos Sąjungos veikimo 4 str. 2 d.), „ES saugumas“, „kova su terorizmu“ vis dėlto patenka į Europos Sąjungos kompetenciją ir gali būti reguliuojami Europos Sąjungos teisės aktais.

Atsižvelgiant į nurodytus argumentus, pritartina pagal 29 straipsnį įkurtos darbo grupės vertinimui, kad asmens duomenų tvarkymas tokiais tikslais (pvz., Europos Sąjungos vidinio saugumo užtikrinimo, kovos su terorizmu) jei ne tapatus, tai bent itin artimas tokiam, kuris paprastai būtų suprantamas kaip atliekamas nacionalinio saugumo tikslais ir, matyt, jam vis dėlto galėtų būti taikomos Europos Sąjungos sutartos taisyklės, kaip jos taikomos kovos su terorizmu bei Europos Sąjungos saugumo užtikrinimo priemonėms[252].

Nacionalinio saugumo sampratos taip pat negalima kildinti ir iš Europos Sąjungos Teisingumo Teismo praktikos. Bylose, formuojamose asmens teisės į privatumą ir kt. pagrindinių teisių apsaugos ginčuose, teismas nors ir mini „nacionalinį saugumą“, tačiau jo turinio neidentifikuoja ir nedetalizuoja – jokių indikacijų apie nacionalinio saugumo sampratą nebuvo pateikta nei *Schrems*[253], nei *Schrems II*[254], nei *Digital Rights Ireland*[255], nei *Promusicae*[256] bylose. Nors toks nacionalinio saugumo sampratos vakuumas gali pasirodyti ir logiškas (nes Europos Sąjungos teisė negali reguliuoti valstybių narių nacionalinio saugumo[257], o Europos Sąjungos Teisingumo Teismo jurisdikcijai nepriklauso prižiūrėti kaip valstybės narės užtikrina „vidaus saugumą“[258]), autoriaus vertinimu, tai laikytina nepriimtina teisinio vakuumo situacija, nes Europos Sąjungos teisė yra taikoma visai eilei kitų Europos Sąjungos bendrai ir valstybių narių atskirai atliekamų funkcijų, susijusių su saugumo užtikrinimu, kriminaline žvalgyba, etc.

---

252 „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2014 m. gruodžio 5 d. darbinis dokumentas Nr. WP228 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais“, *supra note,* 257: 22.

253 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7.

254 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8.

255 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202.

256 „Europos Sąjungos Teisingumo Teismo 2008 m. sausio 29 d. sprendimas byloje Nr. C-275/06 Promusicae“, InfoCuria, žiūrėta 2021 m. rugpjūčio 5 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=1623552.

257 „Europos Sąjungos sutartis“, *supra note*, 78: 4 str. 2 d.

258 „Sutartis dėl Europos Sąjungos veikimo“, *supra note*, 54: 276 str.

Atsižvelgiant į tai, kad nei Europos Sąjungos teisės aktuose, nei Europos Sąjungos Teisingumo Teismo praktikoje negalima rasti nacionalinio saugumo sampratos ar apibrėžimo, vienintele institucija, galinčia suteikti daugiau teisinio tikrumo ir nubrėžti, ką nacionalinio saugumo samprata gali apimti, o ko – ne, yra Europos Sąjungos Teisingumo Teismas, nes tik jis pagal Europos Sąjungos teisės aktus turi išimtinę teisę aiškinti Europos Sąjungos teisinį reguliavimą[259].

### 4.4.1. Nacionalinio saugumo samprata pagal Lietuvos Respublikos teisinį reguliavimą

Lietuvoje su nacionalinio saugumo samprata labiausiai susijęs yra Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas. Šiame įstatyme įtvirtinti nacionalinio saugumo pagrindai, kurie aiškiausiai identifikuoja tai, kas gali patekti į šią savoką. Tuo tarpu žvalgybos institucijų, siekiančių įgyvendinti Nacionalinio saugumo pagrindų įstatymą bei pasiekti jame įtvirtintus tikslus, veiklą reglamentuoja Lietuvos Respublikos žvalgybos įstatymas.

Lietuvos teisės doktrinoje šis nacionalinio saugumo sampratos klausimas iš esmės nebuvo nagrinėtas. Kaip minėta anksčiau, kadangi šio tyrimo rengimo metu aktualiame Lietuvos mokslininkės darbe buvo detaliai paaiškinti žvalgybos veikimo teisinis reguliavimas (ypač asmens duomenų rinkimas elektroninėje erdvėje)[260], apie Žvalgybos įstatymo nuostatas autorius detaliau pasisakys tik nagrinėjant pačią nacionalinio saugumo sampratą, o ne jo įgyvendinimo (užtikrinimo) aspektus. Kitame Lietuvos mokslininkų darbe nacionalinio saugumo samprata nebuvo nagrinėta, tačiau atskleidžiant žvalgybos institucijų veiklos metodų aspektus paminėta, kad nacionalinio saugumo samprata, kaip žvalgybos veiklos objektas, yra neapibrėžta ir nuolatos kintanti, todėl sąlygoja ir žvalgybinės veiklos dilemas[261]. Dar viename Lietuvos mokslininkės darbe buvo analizuoti teisės į privatumą suvaržymai, susiję su finansinėmis transakcijomis ir pinigų plovimo prevencija, atliekami nacionalinio saugumo interesais[262].

---

259 „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2014 m. gruodžio 5 d. darbinis dokumentas Nr. WP228 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais“, *supra note*, 257: 23.

260 Stankevičiūtė, *supra note,* 6: 4.2 skyrius

261 Audronė Petrauskaitė ir Laurynas Šaltenis, „Žvalgybos Veiklos Ir Etikos Sąveika Nacionalinio Saugumo Kontekste: Teorinė Problemos Apžvalga“, *Lietuvos Metinė Strateginė Apžvalga* 16, 2017-2018 (2018): 396.

262 Birutė Pranevičienė, „Limiting of the Right to Privacy in the Context of Protection of National Security“, *Jurisprudencija* 18, 4 (2011).

Lietuvos Respublikos nacionalinio saugumo pagrindų įstatyme nėra aiškiai įtvirtinta nacionalinio saugumo sąvoka. Tačiau įstatymo priedelyje įtvirtinti Lietuvos nacionalinio saugumo užtikrinimo pagrindai. Šio įstatymo priedelio 2 skyriaus I skirsnyje įtvirtinti pagrindiniai nacionalinio saugumo objektai: žmogaus ir piliečio teisės, laisvės bei asmens saugumas; tautos puoselėjamos vertybės, jos teisės ir laisvos raidos sąlygos; valstybės nepriklausomybė; konstitucinė santvarka; valstybės teritorijos vientisumas; aplinka ir kultūros paveldas; visuomenės sveikata. Taigi, nacionalinis saugumo objektai apima ne tik kertinius dalykus valstybės egzistavimui (pvz., konstitucinę santvarką ir valstybės teritorijos vientisumą), tačiau ir kitus visuomenės interesus – aplinką, kultūros paveldą, visuomenės sveikatą bei net tokius vertybinius aspektus, kaip „tautos puoselėjamas vertybes". Todėl sunku identifikuoti sritį, kuri apskritai galėtų būti laikoma nepatenkančią į nacionalinio saugumo sampratą.

Atitinkamai netiesioginių užuominų apie tai, kas gali būti priskiriama prie nacionalinio saugumo sampratos galima nustatyti iš Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo. Jame įtvirtinta nacionalinio saugumo interesų sąvoka: saugomi gyvybiniai ir pirmaeiliai valstybės saugumo interesai, kaip jie suprantami Nacionalinio saugumo strategijoje, transeuropinės infrastruktūros plėtra bei Lietuvos Respublikos įstatymuose įtvirtinti esminiai visuomenės interesai, įskaitant svarbiausių bendrus interesus atitinkančių paslaugų teikimą ir kita[263].

Autoriaus vertinimu, ši sąvoka turi būti laikoma artimiausia nacionalinio saugumo sampratai, nes ji yra blanketinė ir nė kiek nesusiaurina Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymo priedelyje įtvirtintų Lietuvos nacionalinio saugumo užtikrinimo pagrindų. Atitinkamai, Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 1 – 4 prieduose yra išvardintos įmonės, objektai, įrenginiai, kurie laikomi tiesiogiai svarbiais užtikrinant Lietuvos nacionalinį saugumą ir kurie apima įvairiausius objektus, pradedant nuo branduolinės energetikos objektų, suskystintų gamtinių dujų terminalo infrastruktūros ir baigiant valstybinės reikšmės automobilių keliais, polderiais ir jų statiniais Klaipėdos ir Šilutės rajonų bei Pagėgių savivaldybėse bei įmone, teikiančia penktosios kartos judriojo ryšio (5G) paslaugas ar valdančia šioms paslaugoms teikti reikalingą infrastruktūrą[264]. Taigi, kaip ir vadovaujantis Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymu,

---

[263] „Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas", 2 str. 7 d., LRS, žiūrėta 2021 m. rugpjūčio 5 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498/asr.

[264] *Ibid,* I – IV priedai.

Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo analizė neleidžia pagrįstai susiaurinti nacionalinio saugumo sampratos ar bent aiškiai identifikuoti sritį, kuri gali būti laikoma į jį nepatenkančia.

Lietuvos teisės aktuose nesant tikslesnio nurodymo, kas gali būti laikoma nacionaliniu saugumu, šios teisės aktuose minimos sąvokos aiškinimo reikia ieškoti Lietuvos teismų išaiškinimuose. Atlikus Lietuvos teismų praktikos analizę, galima daryti išvadą, kad, deja, nacionalinio saugumo samprata tiesiogiai analizuota nebuvo, tačiau Lietuvos teismai nagrinėjo ne vieną bylą, kurioje ši samprata buvo minima ir iš šių bylų objektų galima spręsti, kokios konkrečios aplinkybės gali būti laikomos patenkančiomis į nacionalinio saugumo sampratą.

Pirmas ir ryškiausias pavyzdys, iš kurio yra atsiradęs ne vienas Lietuvos teismų sprendimas ar nutarimas, kuriame minima nacionalinio saugumo samprata, yra šio darbo rengimo metu vis dar vykstantis teisminis procesas, susijęs su (šiuo metu – tariama) korupcija, verslo struktūrų (kurių epicentre buvo koncernas MG Baltic) įtaka teisėkūros procesams, valstybės vykdomajai valdžiai bei atskiriems sprendimams valstybės valdomose įmonėse. Valstybės saugumo departamentas ne vėliau nei nuo 2007 metų taikė žvalgybos priemones ir nustatė verslo organizacijų atstovų bei aktyvių politikos veikėjų tarpusavio ryšius[265]. 2017 m. ikiteisminio tyrimo institucijos išviešino atliekamą ikiteisminį tyrimą dėl kyšininkavimo, prekybos poveikiu ir kt. nusikaltimų. 2018 m. Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komitetas atliko parlamentinį tyrimą dėl asmenų, verslo subjektų ir kitų interesų grupių galimo neteisėto poveikio valstybės institucijoms priimant sprendimus ir galimos neteisėtos įtakos politiniams procesams.

Autoriaus vertinimu, pirmas paminėtinas su šiuo tyrimu susijęs Lietuvos teismų sprendimas yra Lietuvos Respublikos Konstitucinio Teismo nutarimas[266], kuriuo buvo analizuotos Lietuvos Respublikos Seimo sudarytos Seimo laikinosios tyrimo komisijos dėl galimos neteisėtos įtakos ir (ar) poveikio Lietuvos politikams, valstybės tarnautojams ir politiniams procesams, sudarymo aplinkybės, teisiniai pagrindai bei šios komisijos atlikto tyrimo atitiktis Lietuvos Respublikos Konstitucijos 5 straipsnio

---

[265] „Dėl Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komiteto atlikto parlamentinio tyrimo dėl asmenų, verslo subjektų ir kitų interesų grupių galimo neteisėto poveikio valstybės institucijoms priimant sprendimus ir galimos neteisėtos įtakos politiniams procesams išvados“, LRS, žiūrėta 2021 m. balandžio 20 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3c03fbf26b0611e8b7d2b2d2ca774092.

[266] „Lietuvos Respublikos Konstitucinio Teismo 2020 m. birželio 12 d. nutarimas „Dėl Seimo laikinajai tyrimo komisijai pavedamo tyrimo ribų““, LRKT, žiūrėta 2021 m. balandžio 20 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta2161/content.

1, 2 dalims, 67 straipsniui, konstituciniam teisinės valstybės principui. Šiame nutarime Lietuvos Respublikos Konstitucinis Teismas konstatavo, kad minėtos Seimo laikinojo tyrimo komisijos sudarymas ir jos atliktas tyrimas prieštaravo Lietuvos Respublikos Konstitucijos 67, 76 straipsniams, konstituciniams atsakingo valdymo, teisinės valstybės principams.

Taip pat paminėtinas ir kitas Lietuvos Respublikos Konstitucinio Teismo nutarimas[267], kuriuo buvo analizuotas klausimas susijęs su galimu kriminalinės žvalgybos informacijos priemonių vieno asmens atžvilgiu taikymo metu gautos informacijos naudojimu kitais tikslais ir kito asmens atžvilgiu (bylos atveju – tarnybinės atsakomybės taikymo kitam asmeniui (nei tam, kurio atžvilgiu taikomos kriminalinės žvalgybos priemonės) tikslais). Analizuotoje byloje buvo taikomos kriminalinės žvalgybos priemonės privataus subjekto – verslo atstovo atžvilgiu ir buvo perimtas jo bendravimas kitu asmeniu. Perimtas bendravimas tapo pagrindu Valstybinės mokesčių inspekcijos vadovo atžvilgiu taikyti tarnybinę nuobaudą – atleidimą iš tarnybos. Šioje byloje Lietuvos Respublikos Konstitucinis Teismas nutarė, kad Lietuvos Respublikos kriminalinės žvalgybos įstatymo 19 str. 3 d. įgalinanti kriminalinės žvalgybos taikymo metu gautos informacijos panaudojimą tiriant nusižengimus neprieštarauja Lietuvos Respublikos Konstitucijai[268].

Su minėtu Lietuvos Respublikos Seimo sudarytos Seimo laikinosios komisijos tyrimu yra ir kitų Lietuvos teismų sprendimų, priimtų nagrinėjant ginčus dėl teisės į garbės ir orumą gynimo ir neturtinės žalos atlyginimo[269]. Šio darbo rengimo metu, juose dar nėra priimti galutiniai sprendimai, tačiau jie nėra aktualūs šio tyrimo problematikos prasme (kadangi juos nagrinėjami kiti teisiniai klausimai), todėl dėl jų plačiau nepasisakoma.

---

267 „Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas „Dėl kriminalinės žvalgybos informacijos panaudojimo tiriant korupcinio pobūdžio tarnybinius nusižengimus"", LRKT, žiūrėta 2021 m. balandžio 20 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta1927/content.

268 „Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas „Dėl kriminalinės žvalgybos informacijos panaudojimo tiriant korupcinio pobūdžio tarnybinius nusižengimus"", *supra note*, 289.

269 „Vilniaus apygardos teismo Civilinių bylų skyriaus 2021 m. sausio 19 d. nutartis civilinėje byloje Nr. e2A-165-567/2021", Liteko, žiūrėta 2021 m. balandžio 22 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=c1f3413a-53ad-4655-8852-c90faa5941e6.; „Vilniaus apygardos teismo Civilinių bylų skyriaus 2020 m. vasario 11 d. nutartis civilinėje byloje Nr. 2A-95-340/2020", Liteko, žiūrėta 2021 m. balandžio 21 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=d7c034af-a5a6-4723-bc63-3943e611f86e; „Lietuvos vyriausiojo administracinio teismo 2021 m. balandžio 7 d.nutartis administracinėje byloje Nr. A-749-556/2021", Liteko, žiūrėta 2021 m. balandžio 21 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=5783f33b-8ab1-4b87-9933-1c63b756cf5f.

Kita paminėtina teisinio reguliavimo sritis, susijusi su nacionalinio saugumo samprata, yra susijusi su Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu bei jo taikymu.

Lietuvos Respublikos Konstitucinis teismas nagrinėjo bylą dėl Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 11 straipsnio 4 punkto atitikties Lietuvos Respublikos Konstitucijai, kurioje pagrindinis klausimas buvo kilęs dėl asmens galimo pripažinimo neatitinkančiu nacionalinio saugumo interesų, jeigu jis yra kaltinamas dėl labai sunkaus, sunkaus ar apysunkio nusikaltimo padarymo, tačiau dėl šio asmens nėra įsiteisėjusio apkaltinamojo teismo nuosprendžio[270]. Šioje byloje Konstitucinis teismas padarė išvadą, kad minėta Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo nuostata neprieštaravo Lietuvos Respublikos Konstitucijai ir asmuo gali būti pripažįstamas neatitinkančiu nacionalinio saugumo interesų, net tais atvejais, kai dėl nėra įsiteisėjusio apkaltinamojo teismo nuosprendžio dėl labai sunkaus, sunkaus ar apysunkio nusikaltimo padarymo.

Taip pat, kiek tai susiję su Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo taikymu, Lietuvos administraciniai teismai taip pat yra priėmė eilę sprendimų ir nutarčių[271], kurie iš esmės patvirtina, kad nacionalinio saugumo samprata apima ir investuotojų į Lietuvos Respublikos geležinkelių ir Klaipėdos valstybinio jūrų uosto infrastruktūrą, tikrinimą nacionalinio saugumo interesams. Atkreiptinas dėmesys, kad šiose bylose pagrindinė investuotojų neatitiktis nacionaliniam interesui buvo siejama su asmens pripažinimu kaltu dėl labai sunkaus, sunkaus ar apysunkio nusikaltimo pagal Lietuvos Respublikos baudžiamąjį kodeksą ar dėl nusikaltimo pagal užsienio valstybių baudžiamuosius įstatymus, kuris atitinka Lietuvos Respublikos baudžiamojo kodekso specialiojoje dalyje nurodytus labai sunkaus, sunkaus ar apysunkio nusikaltimo požymius, ar dėl tokio nusikaltimo pa-

---

[270] „Lietuvos Respublikos Konstitucinio Teismo 2021 m. kovo 4 d. nutarimas "Dėl baudžiamojo persekiojimo kaip pagrindo pripažinti asmenį neatitinkančiu nacionalinio saugumo interesų"", LRKT, žiūrėta 2021 m. balandžio 20 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta2379/content.

[271] „Lietuvos vyriausiojo administracinio teismo 2019 m. gruodžio 30 d.nutartis administracinėje byloje Nr. eAS-738-575/2019", Liteko, žiūrėta 2021 m. balandžio 21 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=fcfce450-5b83-4043-8fbd-5e0373281d69; „Lietuvos vyriausiojo administracinio teismo 2018 m. rugsėjo 18 d. nutartis administracinėje byloje Nr. eAS-624-756/2018" , Liteko, žiūrėta 2021 m. balandžio 21 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=79b87395-dc5e-4e3a-92a0-ef57a79a69ac; „Lietuvos vyriausiojo administracinio teismo 2018 m. rugsėjo 6 d. sprendimas administracinėje byloje Nr. eA-5177-602/2018", Liteko, žiūrėta 2021 m. balandžio 21 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=92a0f05a-59d5-4b72-b58e-0226bf4f6de8.

darymo vykdomas šio asmens baudžiamasis persekiojimas ir už padarytą nusikaltimą nėra išnykęs ar panaikintas investuotojo teistumas[272]. Todėl minėtos bylos nepadeda apibrėžti nacionalinio saugumo sampratos, nes su sampratos turiniuu susiję klausimai jose detaliai nagrinėti taip pat nebuvo.

Apibendrinant pateiktą Lietuvos teismų praktikos analizę, darytina išvada, kad nacionalinio saugumo samprata joje taip pat nėra atskleista. Atlikta Lietuvos teismų sprendimų analizė atskleidė, kad nėra jokios indikacijos ar bent vieno pavyzdžio apie galimas nacionalinio saugumo sampratos ribas. Todėl darytina išvada, kad Lietuvos žvalgybos institucijų vykdomos žvalgybos informacijos rinkimo veikla apie grėsmes Lietuvos Respublikos nacionaliniam saugumui gali būti nukreipta į bet kokius visuomeninius interesus ir net neapibrėžtus vertybinius aspektus, tokius kaip „tautos puoselėjamas vertybes“. Šiuo aspektu Lietuvos teisinis reguliavimas nėra tikslesnis už Europos Sąjungos teisinį reguliavimą, kuriame nacionalinio saugumo sąvoka taip pat yra vartojama, tačiau jos ribos nėra nubrėžtos.

### 4.1.2. Nacionalinio saugumo sampratos kilmė Jungtinių Amerikos Valstijų teisiniame reguliavime

Kolonijinės eros metu amerikiečiai protestavo prieš platų, nekontroliuojamą britų vykdytą stebėjimą. „Bendrieji orderiai“ ir „pagalbos raštai“, kuriuos britų kolonijiniai pareigūnai pirmiausia naudojo vykdydami kratas, nukreiptas į kontrabandą, kėlė didžiausią pasipiktinimą[273]. Šios kratos ir jų teisiniai pagrindai buvo bendro pobūdžio – jie nepasižymėjo konkretumu ar apskritai kokiais nors apribojimais[274]. Didelė antipatija šioms plačioms kratoms atsispindėjo ketvirtojoje JAV Konstitucijos pataisoje (angl. *Fourth amendment*), kurioje numatyta, kad „žmonių teisė apsaugoti savo asmenis, namus, dokumentus ir daiktus nuo nepagrįstų kratų ir arešto negali būti pažeista ir jokie orderiai neturi būti išduodami, nebent tik dėl galimos priežasties, paremtos priesaika ar patvirtinimu, ir aprašant kratos vietą bei areštuojamus asmenis ar daiktus“[275]. Kai pareigūnai atlieka tokius veiksmus, jie pirmiausia turėjo gauti neutralaus magistro orderį, nebent paieška patektų į vieną iš kelių ilgalaikių orderio reikalavimo išimčių.

[272] „Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas“, *supra note,* 285: 11 str. 4 p.

[273] Bernard Schwartz, *The Bill of Rights: A Documentary History* 1 (1971): 199.

[274] Michael W. Price, „Rethinking Privacy: Fourth Amendment”Papers”and the Third Party Doctrine“, *J. Nat ’l Security L. & Pol ’Y* 8, 2 (2016): 247, 250 – 58.

[275] „The Bill of Rights: A Transcription“, National Archives, žiūrėta 2021 m. liepos 4 d., https://www.archives.gov/founding-docs/bill-of-rights-transcript.

Nors žodis „privatumas“ ketvirtojoje Konstitucijos pataisoje neminimas, šiandien ji suprantama kaip apsauganti „pagrįstus privatumo lūkesčius“ – būtent tuos subjektyvius lūkesčius, kuriuos visuomenė yra pasirengusi priimti kaip pagrįstus[276].

Nepaisant ketvirtosios JAV Konstitucijos pataisos garantijų, visuomeniniame gyvenime plačios apimties stebėjimo atvejai kartodavosi ir teisiniai pagrindai jiems buvo stiprinami. Pavyzdžiui, Vudrou Vilsono 1917 m. priimtas Šnipinėjimo įstatymas (angl. *Espionage Act*) ir Palmerio reidai (angl. *Palmer Raids*) Vilsono administracijos pabaigoje[277], buvo susiję su padidėjusiomis stebėjimo programomis ir intervencija į asmenų privatų gyvenimą. Pažymėtina, kad XX a. pradžioje pasitaikantys privatumo pažeidimo atvejai buvo žinomi Kongresui, teismams ir visuomenei, todėl bent teoriškai, jei ne visada praktikoje, jie buvo kritikuojami ir ginčijami spaudoje bei plačiojoje visuomenėje.

Slaptai vykdomas išplėstinis stebėjimas yra skiriamasis nacionalinio saugumo užtikrinimo priemonių bruožas. JAV Prezidentas Franklinas D. Ruzveltas žengė du svarbius (ir slaptus) žingsnius tam, kad suteiktų jam teisinį pagrindą: 1938 m. jis išplėtė Federalinio tyrimų biuro (FTB) įgaliojimus, įgalindamas juos atlikti ne tik nusikalstamo elgesio, bet ir „ardomosios veiklos“ tyrimus. Šios sąvokos neapibrėžė nei F. Ruzveltas, nei tuometinis FTB direktorius J. Edgaras Huveris, todėl JAV teisės istorikų vertinimu, FTB iš sąlyginai nedidelės federalinės agentūros virto į klestintį biurokratijos pavyzdį, turintį prieigą prie įvairiausių jų veiklai reikalingų duomenų šaltinių[278]. F. Ruzveltas dėl tokio FTB įgaliojimų išplėtimo nesikonsultavo su Kongresu ir net neinformavo jo apie šių įgaliojimų suteikimą, nes teisėsaugos institucijos matė didelę riziką dėl šių papildomų funkcijų suteikimo tvarumo (t. y. jų išlaikymo plačiajai visuomenei apie tai sužinojus), todėl pageidavo tai laikyti kaip įmanoma konfidencialiau[279].

Antrasis įvykis, įgalinęs platesnį stebėjimo priemonių taikymą piliečių atžvilgiu įvyko 1940 m., kai prezidentas Ruzveltas slapta panaikino tuometinio generalinio prokuroro Roberto Jacksono įsakymą, kuriuo buvo uždraustas FTB atliekamas pokalbių

---

276 „Katz v. United States (1967)“, FindLaw, žiūrėta 2021 m. liepos 4 d., https://caselaw.findlaw.com/us-supreme-court/389/347.html.

277 „Palmer Raids“, FBI, žiūrėta 2021 m. liepos 4 d., https://www.fbi.gov/history/famous-cases/palmer-raids.

278 Kenneth O'Reilly, „A New Deal for the FBI: The Roosevelt Administration, Crime Control, and National Security“, *The Journal of American History* 69, 3 (1982): 639.

279 „Supplementary Detailed Staff Reports on Intilligence Activities and the Rights of Americans“, *Final Report of the U.S. Select Commity to Study Governmental Operations with Respect to Intelligence Activities* Rep. 94 – 755, bk. III (Washington: U.S. Government printing Office, 1976), 398.

pasiklausymas be išankstinių leidimų[280]. Tokiu būdu, FTB pareigūnams buvo suteikta teisė be išankstinių leidimų perimti asmenų, įtariamų „ardomąja veikla“, susižinojimą, nepateikiant jokios motyvacijos, ką tokia tariama „ardomoji veikla” gali apimti[281].

Tačiau didžiausią įtaką nacionalinio saugumo užtikrinimo veiklų įtvirtinimui teisės aktuose padarė 1947 m. priimtas Nacionalinio saugumo įstatymas[282]. Jis iš esmės pertvarkė vyriausybės karines ir žvalgybos agentūras, įsteigė Nacionalinę saugumo tarybą tam, kad būtų koordinuojama nacionalinė saugumo politika vykdomojoje valdžioje ir Centrinėje žvalgybos valdyboje (CŽV), o vėliau Gynybos departamente buvo sukurta Nacionalinio saugumo agentūra (NSA)[283].

Visi šie veiksniai ir nacionalinio saugumo politiką vykdančių bei prižiūrinčių subjektų reorganizacija tik paskatino plačiai taikomą JAV piliečių stebėjimą, kuris pradėjo ryškėti aštuntajame dešimtmetyje. 1972 metais atliktas žurnalistinis tyrimas atskleidė, kad prezidento Niksono administracija šnipinėja ir sabotuoja politinius oponentus – kilo *Watergate* skandalas[284]. Praėjus dvejiems metams, „New York Times“ atliktas žurnalistinis tyrimas atskleidė, kad CŽV prezidento Džonsono įsakymu atliko didžiulę žvalgybos operaciją prieš Vietnamo karo kritikus, kitus vidaus disidentus ir žurnalistus, kuriuos administracija laikė nedraugiškais[285].

Šios ataskaitos paskatino JAV Kongresą atlikti tyrimus, kurių geriausiai žinomas buvo specialiai suburto Senato komiteto, žinomas kaip Church komitetas (angl. *Church Committee*), tyrimas[286]. Per dvejus metus trukusį tyrimą Church komitetas identifikavo daugybę piktnaudžiavimo atvejų, apimančių kiekvieną administraciją – nuo Franklino

---

280 Joseph E. Persico, „Roosevelt‘s Secret War: FDR and World War II Espionage“ 35 (2002); David C. Unger, „The Emergency State: America’s Pursuit of Absolute Security at All Costs“ 41 (2013).

281 Alexander Charns, „Cloak and Gavel: FBI Wiretaps, Bugs, Informers, and the Supreme Court“ 23 (1992); Darren E. Tromblay, „The U.S. Domestic Intelligence Enterprise: History, Development, and Operations“ 15 (2015).

282 „1947 m. Nacionalinio saugumo įstatymas“, U.S. Government, žiūrėta 2021 m. liepos 5 d., https://www.govinfo.gov/content/pkg/COMPS-1493/pdf/COMPS-1493.pdf.

283 Sarah Parsons, „Sources and Methods for Cryptologic History: NSA.gov - a Tour through Its History and Resources“, *Cryptologia* 44, 4 (2020): 372.

284 Carl Bernstein ir Bob Woodward, „FBI Finds Nixon Aides Sabotaged Democrats“, *Washington Post*, 1972 m. spalio 10 d., A01, žiūrėta 2021 m. liepos 5 d., https://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/101072-1.htm.

285 Seymour M. Hersh, „Huge C.I.A. Operation Reported in U.S. against Antiwar Forces, Other Dissidents in Nixon Years“, *The New York Times*, 1974 m. gruodžio 22 d., A1, žiūrėta 2021 m. liepos 5 d., https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html.

286 Vienuolikos narių komitetas, sušauktas tirti vykdomosios valdžios veiklą ryšiuje su žvalgybos veiksmais, buvo vadinamas Church komitetu pagal jo pirmininko senatoriaus Frank Church pavardę.

Ruzvelto iki Ričardo Niksono[287]. Tyrimo metu buvo nustatyta, kad FTB šnipinėjo daugiau nei 500 000 amerikiečių, įskaitant moterų išsivadavimo judėjimo, konservatyvių krikščionių grupių, įvairių universitetų bei bažnyčių grupių, besipriešinančių Vietnamo karui narių, o CŽV tyrė mažiausiai 200 000 asmenų Jungtinėse Valstijose prieštaraujančių karo Vietname politikai; JAV mokesčių administratorius, remdamasi politiniais, o ne mokestiniais kriterijais, rinko duomenis apie daugiau nei 11 000 amerikiečių; FTB ir CŽV pažeidė šimtų tūkstančių laiškų konfidencialumą, įskaitant adresuotus ar siųstus JAV mokslininkų federacijos, daugelio JAV taikos grupių nariams ir t. t.[288].

Kai kurie teisėsaugos institucijų tyrimai buvo vykdomi dešimtmečiais ir net ilgą laiko tarpą po to, kai paaiškėjo, kad stebimi subjektai neturėdavo jokio ryšio su užsienio agentais (pvz. Sovietų sąjunga) ar nusikalstamomis veikomis. Pavyzdžiui, 1941 m. FTB vykdė Nacionalinės spalvotųjų žmonių pažangos asociacijos (angl. *National Association for the Advancement of Colored People*) tyrimą dėl penkiolikos protestų dalyvių, susijusių su rasine diskriminacija kariniame jūrų laivyne. Nors FTB pranešimuose iš pat pradžių buvo aiškiai identifikuota, kad minėtos asociacijos veikla yra visiškai teisėta, tyrimas buvo vykdomas net dvidešimt penkerius metus[289]. Taip pat, FTB dvidešimt šešerius metus tyrė Socialistinę darbininkų partiją (SDP), nors nepaisant pareigūnų pripažinimo, kad nėra jokių neteisėtos veiklos įrodymų, FTB informatoriai ir toliau teikė informaciją dėl SDP pozicijų įvairiais klausimais[290]. FTB kelis dešimtmečius tyrė Bajardą Rustiną, kuris Martiną Liuterį Kingą supažindino su nesmurtiniu Gandi mokymu ir 1963 m. Vašingtone surengė protestą „March on Washington". Tyrimas buvo pradėtas remiantis įtarimu, kad Rustinas turėjo komunistų ryšių. Nors FTB pareigūnai pranešė, kad Rustinas tokių ryšių neturi, FTB direktoriuus E. Huveris nurodė tęsti tyrimą, nes esą nebuvo „esminių įrodymų, kad jis yra antikomunistas"[291].

Sovietų Sąjungos iširimas ir Šaltojo karo pabaiga pareikalavo JAV permąstyti nacionalinio saugumo sampratą. Pagrindinis siekis tebebuvo išsaugoti JAV kaip laisvą, ekonomiškai klestinčią tautą, kurios pagrindinės institucijos ir vertybės nepažeistos,

---

287 David Rudgers, „The Church Committee on Intelligence Activities Investigation, 1975 – 76" , iš *Congress Investigates: A Critical and Documentary History*, Roger A. Burns, David L. Hostetter, Raymond W. Smock, (New York: Facts on File, 2011), 932.

288 „Supplementary Detailed Staff Reports on Intilligence Activities and the Rights of Americans", *supra note*, 301: 733 – 83

289 „Intelligence Activities and the Rights of Americans", *Final Report of the U.S. Select Commity to Study Governmental Operations with Respect to Intelligence Activities* S. Rep. 94 – 755, bk. II (Washington: U.S. Government printing Office, 1976), 179.

290 *Ibid*, 180.

291 *Ibid,* , 182.

tačiau technologijų, ryšių, informacijos ir transporto revoliucijos apsunkino minėto tikslo siekimą, o revoliucijos paskatino globalizaciją, ypač ekonomikos ir aplinkos atžvilgiu[292].

Nacionalinio saugumo sampratos analizė ir rekonstravimas (angl. *redefining, rethinking, reconstructing, revisioning* ir t. t.) tapo populiaria tema tarp mokslininkų po Šaltojo karo pabaigos[293]. Tačiau daugumoje pateiktų pavyzdžių dominuoja subjektyvūs įvairių valstybių politikos pakeitimų pasiūlymai, pateikiami kaip prioritetų perdėliojimas tarp žmogaus teisių, ekonomikos, aplinkos apsaugos, narkotikų prekybos, epidemijų pavojų ir kontrolės, nusikalstamumo ir pan. sričių, be tradicinio susirūpinimo fiziniu saugumu nuo išorinių karinių grėsmių.

Pasibaigus Šaltajam karui, JAV prezidentų administracijos ir toliau strateginiuus nacionalinio saugumo interesus siejo su karinių pajėgų panaudojimu užsienyje. Valdant Klintono administracijai, buvo kuriamos kompleksinės pasaulinės karinės programos, apimančios valstybių kūrimą, pabėgėlių kontrolę ir kt. su karu susijusių reiškinių valdymu[294]. Tuo tarpu Bušo administracija iš pradžių daugiausia dėmesio skyrė gyvybiškai svarbiems JAV interesams užsienyje kylančioms grėsmėms, ypač galimam Rusijos valdžios žlugimui ar Kinijos karinės ir ekonominės galios augimui[295].

Dar iki 2001 m. rugsėjo 11 d. teroro išpuolių buvo aišku, kad JAV turės įgyvendinti nacionalinio saugumo sampratos pakeitimus. 1997 m. gruodžio mėn. Krašto apsaugos grupė perspėjo apie didėjančią terorizmo grėsmę Jungtinėms Valstijoms[296]. Tai buvo pabrėžta 1999 m. rugsėjo mėn. I etapo ir 2000 m. balandžio mėn. II etapo JAV Nacionalinio saugumo komisijos ataskaitose, kuriose terorizmas, nukreiptas prieš

---

292 Condolezza Rice, „Promoting the National Interest“, *Foreign Affairs* 79, 1 (2002): 45-62.

293 Pavyzdžiui, Lester R. Brown, „Redefining National Security“, *Worldwatch Paper* 14 (1977); Jessica Tuchman Matthews, „Redefining Security“, *Foreign Affairs* 68, 2 (1989): 162-77; Richard H. Ullman, „Redefining Security“, *International Security* 81, 1 (1983): 129-53; Joseph J. Romm, *Defining National Security* (New York: Council on Foreign Relations, 1993); J. Ann Tickner, „Re-visioning Security“, iš, *International Relations Theory Today*, Ken Booth ir Steve Smith (Oxford, 1995), 175-97; Ken Booth, „Security and Emancipation“, *Review of International Studies* 17, 4 (1991): 313-26; Martin Shaw, „There Is No Such Thing as Society: Beyond Individualism and Statism in International Security Studies“, *Review of International Studies* 19, 2 (1993): 159-75; John Peterson ir Hugh Ward, „Coalitional Instability and the New Multidimensional Politics of Security: A Rational Choice Argument for US-EU Cooperation“, *European Journal of International Relations* 1 (1995): 131-56; dešimt straipsnių apie saugumą ir saugumo tyrimus „Arms Control“ 13, 3 (1992): 463-544.; ir Graham Allison ir Gregory F. Treverton*, Rethinking America's Security: Beyond Cold War to New World Order* (New York, 1992).

294 Ashton B. Carter, „The Architecture of Government in the Face of Terrorism“, *International Security* 26, 3 (2001/2002): 8.

295 Chris Seiple, „Homeland Security Concepts and Strategy“, *Orbis* 46, 2 (2002): 264.

296 Nacionalinė saugumo komisija, *Transforming Defense: National Security in the 21st Century* (1997), 25-28.

Jungtines Valstijas, įvardintas kaip vis labiau didėjanti grėsmė, o 2001 m. kovo mėn. komisija galutinėje III fazės ataskaitoje pabrėžė būtinybę keisti po Antrojo pasaulinio karo susiklosčiusią nacionalinio saugumo sampratą[297]. JAV Nacionalinio saugumo komisija padarė išvadą, kad į nacionalinį saugumą buvo žiūrėta plačiai, o naujoje eroje žymūs skirtumai tarp „užsienio" ir „vidaus" nebeegzistuoja ir nacionalinis saugumas nebegali būti tapatinamas su „gynyba" siaurąja prasme[298].

Praėjus dešimtmečiui po Šaltojo karo pabaigos, JAV aktyviai gynė savo nacionalinį saugumą aktyviai įsitraukdama į karines ir ekonomines iniciatyvas visame pasaulyje. Net ir neegzistuojant reikšmingai ideologinei ar tiesioginei karinei grėsmei (pavyzdžiui, Sovietų Sąjungos) JAV papildomai įsipareigojo Balkanų, Vidurio Europos ir Persijos įlankos šalims – tokią strategiją kai kurie mokslininkai įvardijo kaip itin rizikingą[299].

Toks kritiškas JAV nacionalinio saugumo užtikrinimo globalaus įsitraukimo strategijos pagalba vertinimas gavo dar didesnį populiaruumą po 2001 m. rugsėjo 11 d. teroristinių išpuolių ir priešiškumas tokiai strategijai reikšmingai augo[300]. Minėti įvykiai parodė, kad JAV vykdoma globalaus įsitraukimo politika gali pakisti į izoliacinės strategijos (t. y. nesikišimo) laikymąsi, nes plačioji visuomenė suprato, kad teroristiniai išpuoliai JAV teritorijoje yra sąlygojami būtent pasaulinio JAV įsitraukimo ir kituose žemynuose dedamų pastangų užtikrinti tarptautinį stabilumą ir „tvarką pasaulyje" (angl. *world order*)[301]. Panašus paradoksas buvo identifikuotas ir Šaltojo karo metu, so-

---

297 „Road Map for National Security: Imperative for Change", *the Phase III Report of the U.S. Commission on National Security/21st Century* (Washington: GPO, 2001), xiii.

298 *Ibid*. Taip pat, žr.: the United States Commission on National Security/21st Century, „New World Coming: American Security in the 21st Century", *The Phase 1 Report on the Emerging Global Security Environment*
*for the First Quarter of the 21st Century* (1999); ir the United States Commission on National Security/21st Century, „Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom", The Phase *II Report on a U.S. National Security Strategy for the 21st Century* (2000). Reaguojant į tokius perspėjmus, 1999 m. Klintono Administracijos nacionalinio saugumo strategija buvo orientuota į kovą su terorizmu, o atskirame skyriuje, pavadinimu „Defending the Homeland", buvo aptariama, kaip valstybė pasiruošusi atremti išpuolius, susijusius su masinio naikinimo ginklų panaudojimu, ir apsaugoti valstybės infrastruktūrą. William Clinton, *A National Security Strategy for a New Century* (1999), 13, 16-18.

299 Barry R. Posen ir Andrew L. Ross, „Competing Visions for U.S. Grand Strategy", *International Security* 21, 3 (1996/97): 5, 52

300 Pavyzdžiui, žr.: Francois Heisbourg, „American Hegemony? Perceptions of the U.S.Abroad", *Survival* 41, 4 (1999-2000): 5-19; Peter W. Rodman, „The World's Resentment: Anti-Americanism as a Global Phenomenon", *National Interest* 60 (2000): 33-41; ir Chalmer A. Johnson, *Blowback: The Costs and Consequences of American Empire* (New York: Metropolitan, 2000).

301 Barry R. Posen, „The Struggle Against Terrorism: Grand Strategy, Strategy, and Tactics", *International Security* 26, 3 (Winter 2001/2002): 54.

vietiniams branduoliniams ginklams, strateginiams bombonešiams ir raketoms artėjant prie JAV teritorijos (pvz. Sovietams dislokuojant savo strateginę ginkluotę Kuboje), t. y. JAV strateginis įsitraukimas į veiklas kituose žemynuose (Europoje, Artimuosiuose Rytuose ir Azijoje) galėjo būti branduolinių išpuolių JAV atžvilgiu (jos pačios teritorijoje) priežastimi[302]. Todėl JAV karinių pajėgų buvimas ir įsitraukimas probleminiuose taškuose visame pasaulyje kėlė priešiškumą visuomenėje.

Taigi, nors JAV teisės sistemoje nacionalinio saugumo samprata nėra įtvirtinta[303], tačiau remiantis anksčiau pateiktais nacionalinio saugumo užtikrinimo iniciatyvų pavyzdžiais, ji yra itin plati ir apima įvairias visuomenės gyvenimo sritis nuo fizinio iki ekonominio saugumo užtikrinimo ir net demokratinės santvarkos puoselėjimo strateginėse užsienio teritorijose. JAV nacionalinio saugumo sampratos raida bei evoliucija pasižymi ne tik šio ginamo intereso neapibrėžtumu ir itin plačiomis teisėmis, susijusiomis su nacionalinio saugumo užtikrinimu, kurios suteikiamos žvalgybos bei teisėsaugos institucijoms, tačiau ir gausiaiis piktnaudžiavimo suteiktomis teisėmis pavyzdžiais.

### 4.1.3. Asmens teisės į privatumą ribojimo teisėtumas nacionalinio saugumo tikslais pagal Europos Žmogaus Teisių Teismo praktiką

Galimybė valstybėms remtis nacionalinio saugumo institutu, siekiant pateisinti žmogaus teisių apsaugos apribojimą, neišvengiamai kelia susirūpinimą, nes žvalgybos institucijų piktnaudžiavimo rizika suteikiamomis teisėmis niekuomet negali būti visiškai atmetama – anksčiau aprašytuose šio tyrimo skirsniuose pateikiami žvalgybos nesėkmių istorijos pavyzdžiai patvirtina, kad piktnaudžiavimas turimais įgaliojiimais yra neatsiejama politinės tikrovės dalis. Dėl to vieningai sutaria tiek teisės mokslininkai[304], tiek tai rodo praktika, pavyzdžiui Edvardui Snoudenui 2013 m. paviešinus JAV žvalgybos institucijų taikomą duomenų rinkimo ir analizės praktiką[305]. Nacionalinis saugumas dažnai minimas terorizmo grėsmės kontekste, o po 2001 m. rugsėjo 11-osios išpuolių visuomenėje juo remiamasi kaip įvairių teisių apribojimų pateisinimu (dažnai, su santykinai dideliu visuomenės pritarimu, pavyzdžiui, kaip 2001 m. Amerikoje buvo

---

302 Stephen M.Walt, „Beyond bin Laden: Reshaping U.S. Foreign Policy“, *International Security* 26, 3 (Winter 2001/2002): 74.

303 Žr. pvz., JAV 1947 m. Nacionalinio saugumo įstatymą, *supra note*, 304, ir „2004 m. Žvalgybos reformos ir terorizmo prevencijos įstatymą“, U.S. Government Printing Office, žiūrėta 2021 m. liepos 2d., https://www.govinfo.gov/content/pkg/PLAW-108publ458/html/PLAW-108publ458.htm.

304 Brittany Adams, „Striking A Balance: Privacy And National Security In Section 702 U.S. Person Queries“, *Washington Law Review* 94, 1 (2019): 403.

305 Rotenberg, *supra note*, 241: 141-52.

priimtas PATRIOT įstatymas, apimantis reikšmingus privatumo suvaržymus)[306]. Dėl labai sudėtingų šnipinėjimo ir terorizmo formų, kurios šiuo metu kelia grėsmę demokratinėms visuomenėms, valstybės taip pat turi imtis inovatyvių gynybos priemonių, tačiau visiška veiksmų laisvė bet kuriuo atveju negali būti pateisinama šioje kovoje[307].

Todėl šiame skyriuje siekiama išanalizuoti Europos Žmogaus Teisių Teismo praktiką, sietiną su nacionalinio saugumo samprata, kuri naudojama kaip pagrindas valstybėms naudotis išimtiniais įgaliojimais, ribojančiais pagrindinių teisių teikiamą apsaugą.

Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau šiame skyriuje – Konvencija) straipsniuose, kuriuose įtvirtinama teisė į privatumą, minčių, susirinkimų laisvę, nacionalinis saugumas minimas kaip pirmasis iš teisėtų tikslų, kurio pagrindu galima šias teises riboti[308]. Tačiau ši sąvoka Konvencijoje apskritai nėra apibrėžta ir teisės doktrinoje pripažįstama, kad ji yra neaiški[309]. Be to, pati Europos žmogaus teisių komisija pateikė vertinimus, kad jos negalima išsamiai apibrėžti, todėl ji yra tam tikra prasme turi būti laikoma tampria ir lanksčia, o tai atsispindi valstybėms šioje srityje suteikiamoje vertinimo laisvėje[310].

Nors jos ribas sunku apibrėžti, Europos Žmogaus Teisių Teismų praktika leidžia nacionalinio saugumo sąvokai priskirti tam tikrą turinį arba brėžti (nors ir netvirtas) jos ribas. Toliau pateikiamoje Europos Žmogaus Teisių Teismų ir Europos žmogaus teisių komisijos praktikos analizėje, daugiausia dėmesio skiriama praktikai, suformuotai bylose, susijusiose su slaptu sekimu, kurios, autoriaus vertinimu, yra vienos iš svarbiausių bylų, kurių motyvai sietini su nacionalinio saugumo samprata.

---

306 Viet D. Dinh ir Wendy J. Keefer, „FISA and the Patriot Act: A Look Back and a Look Forward Note“, *Annual Review of Criminal Procedure* 35 (2006): iii–xxxiv.

307 Autoriaus vertinimu, šią mintį netiesiogiai sustiprina Europos Sąjungos Teisingumo Teismo sprendimai bylose *Digital Rights Ireland, Tele2 Sverige, Schrems* ir *Schrems II*, kuriuose buvo analizuojamos teisėsaugos (sunkių nusikaltimų prevencijos) ir nacionalinio saugumo pagrindu taikomi teisės į privatumą ir asmens duomenų apsaugą ribojimai.

308 „1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, *supra note*, 52: 8, 10, 11 str. 2 d.

309 Romm, *supra note*, 315; Tickner, *supra note*, 315: 175.

310 „Europos žmogaus teisių komisijos 1993 m. balandžio 2 d. sprendimas dėl David Esbester v. Jungtinė Karalystė skundo priimtinumo“: „*Tačiau Komisija mano, kad minėti principai nebūtinai reikalauja išsamiai apibrėžti sąvoką „nacionalinio saugumo interesai*“, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-1537&filename=001-1537.pdf&TID=ihgdqbxnfi.

### 4.1.3.1. Europos Žmogaus Teisių Teismo praktika bylose dėl masinio stebėjimo ir teisių pažeidimo aukos statuso taikymo

Prieš pradedant analizuoti Europos Žmogaus Teisių Teismo praktiką susijusią su nacionalinio saugumo samprata, svarbu atkreipti dėmesį į aplinkybę, kad pagal Konvenciją, nagrinėti gali būti priimamos tik tos peticijos, kuriose fiziniai asmenys, nevyriausybinės organizacijos ar asmenų grupės, teigia, kad jie yra šioje Konvencijoje pripažintų teisių pažeidimo aukos[311]. Autorius atkreipia dėmesį, kad sąvoka „auka" yra vartojama oficialiame Konvencijos vertime lietuvių kalba. Nors ji ir yra neįprasta vartoti šio darbo rengimo metu, apibūdinant asmenis, kurių pagrindinės teisės yra pažeidžiamos, siekiant teisinio tikslumo ir aiškumo, analizuojant Europos Žmogaus Teisių Teismo praktiką dėl Konvencijos taikymo, autorius vartos būtent aukos sąvoką.

Taigi, pagal Konvencijos 25 str. 1 d., laiduojamų pagrindinių teisių pažeidimo aukos statusas gali būti suteikiamas ir asmenų peticijos priimamos, kai (i) jas pateikia fiziniai asmenys, nevyriausybinės organizacijos ar asmenų grupės bei (ii) kai jie teigia, kad jų teisės yra pažeidžiamos. Autoriaus vertinimu, yra aktualu plačiau išanalizuoti šiuos du reikalavimus peticijos pateikimui ir priimtinumui svarbius aspektus, nes, nors jų turinys ir atrodo aiškus ir apibrėžtas, tačiau jų aiškinimas Europos Žmogaus Teisių Teismo praktikoje nėra toks vienareikšmiškas.

Vienas iš pirmųjų klausimų, iškeltų byloje *Klass* ir kiti prieš Vokietiją (kuri buvo pirmoji didelio visuomenės atgarsio susilaukusi byla dėl telefoninių pokalbių pasiklausymo), buvo tas, ar pareiškėjai gali teigti, kad jie yra Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos pažeidimo aukos. Pareiškėjai, kurie buvo Vokietijos teisininkai, skundėsi dėl teisės aktų, kuriuose numatyti pašto, korespondencijos ir telekomunikacijų paslapties apribojimai, t. y. dėl to, kad jais leidžiama taikyti sekimo priemones, neįpareigojant valdžios institucijų kiekvienu atveju po įvykio informuoti atitinkamus asmenis, ir dėl to, kad dėl tokių priemonių skyrimo ir vykdymo negalima kreiptis į teismą (asmenys, manantys, kad yra sekami, galėjo kreiptis į Konstitucinį Teismą, tačiau šia priemone buvo galima pasinaudoti tik retais atvejais)[312].

Pagal Konvenciją, Europos žmogaus teisių komisija gali priimti peticijas tik tokių fizinių asmenų, kurie teigia, jog jie yra aukos Konvencijoje pripažintų teisių pažei-

---

311 „1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija", *supra note*, 52: 25 str. 1 d.

312 „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją", 23 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-57510.

dimo[313]. Todėl Europos Žmogaus Teisių Teismo vertinimu, šioje byloje asmenys neturėjo teisės interpretuoti Konvenciją ir negalėjo *in abstracto* skųstis dėl įstatymo, kurio egzistavimą jie laikė pažeidžiančiu jų teises, kuriomis jie naudojosi pagal Konvenciją, t. y. įstatymas turėjo būti taikomas jų nenaudai[314].

Tačiau Europos Žmogaus Teisių Teismas pažymėjo, kad, jei valstybė pradeda slaptą sekimą, apie kurio egzistavimą kontroliuojami asmenys nežino, su asmenimis gali būti elgiamasi Konvencijos 8 straipsniui prieštaraujančiu būdu, jiems apie tai nežinant ir todėl negalint pasinaudoti teisių gynimo priemonėmis nacionaliniu lygmeniu arba Konvencijos institucijose, todėl nepriimtina, jog galimybė naudotis Konvencijos garantuojama teise gali būti panaikinta vien dėl to, kad atitinkamas asmuo nežinojo apie jos pažeidimą[315]. Remdamasis šiais argumentais Europos Žmogaus Teisių Teismas pripažino, kad, esant tam tikroms sąlygoms, asmuo gali teigti, kad jis tapo pažeidimo auka vien dėl to, kad egzistuoja slaptos priemonės arba teisės aktai, leidžiantys taikyti slaptas priemones, ir jam nebūtina tvirtinti, kad tokios priemonės jam buvo iš tikrųjų pritaikytos. Atitinkamos sąlygos kiekvienu atveju turėjo būti nustatomos atsižvelgiant į tariamai pažeistą Konvencijos teisę ar teises, slaptą ginčijamų priemonių pobūdį ir pareiškėjo ryšį su šiomis priemonėmis[316].

Atsižvelgdamas į šios bylos faktus, Europos Žmogaus Teisių Teismas pažymėjo, kad ginčijamais teisės aktais buvo sukurta sekimo sistema, pagal kurią visi Vokietijos Federacinės Respublikos asmenys galėjo būti stebimi, jiems nežinant, kad jų paštas, korespondencija ir telekomunikacijos yra stebimi[317]. Todėl ginčijami teisės aktai tiesiogiai paveikė visus Vokietijos Federacinės Respublikos pašto ir telekomunikacijų paslaugų naudotojus ar potencialius naudotojus. Atsižvelgdamas į konkrečias šios bylos aplinkybes, teismas padarė išvadą, kad kiekvienas iš pareiškėjų turėjo teisę „(teigti), kad jis yra Konvencijos pažeidimo auka“, nors ir negalėjo pagrįsti savo pareiškimo, kad jam buvo taikyta konkreti sekimo priemonė[318].

Sprendžiant klausimą, ar pareiškėjai iš tikrųjų tapo Konvencijos pažeidimo aukomis, reikėjo nustatyti, ar ginčijami teisės aktai ir jais sukurta asmenų sekimo sistema

[313] „1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, *supra note,* 52: 25 str. 1 d.
[314] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *op. cit*., 33 p.
[315] *Ibid*, 36 p.
[316] *Ibid*, 34 p.
[317] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *supra note*, 334: 37 p.
[318] *Ibid,* 38 p.

patys savaime buvo suderinami su Konvencijos nuostatomis. Atlikęs bylos aplinkybių ir aktualių teisės aktų analizę, Europos Žmogaus Teisių Teismas pripažino, kad Vokietijos teisės aktais nustatyti asmens teisės į privatų gyvenimą ribojimai (leidžiama taikyti sekimo priemones, neįpareigojant valdžios institucijų kiekvienu atveju po įvykio informuoti atitinkamus asmenis, ir dėl tokių priemonių skyrimo ir vykdymo negalima kreiptis į teismą) buvo pagrįsti ir proporcingi[319].

Byloje *Weber ir Saravia* prieš Vokietiją Europos Žmogaus Teisių Teismas priminė savo išaiškinimsu *Klass* prieš Vokietiją byloje ir pažymėjo, kad teisės aktai, kurie jau vien dėl savo egzistavimo sukelia sekimo grėsmę visiems, kuriems jie gali būti taikomi, neišvengiamai pažeidžia telekomunikacijų paslaugų vartotojų bendravimo laisvę, todėl savaime reiškia kišimąsi į pareiškėjų naudojimąsi 8 straipsnyje įtvirtintomis teisėmis, neatsižvelgiant į priemones, kurių iš tikrųjų buvo imtasi jų atžvilgiu[320]. Šis principas taip pat taikytas sprendime *Kennedy* prieš Jungtinę Karalystę, kuriame buvo nurodyta, kad siekdamas įvertinti, ar asmuo gali reikalauti pripažinti jo teisių pažeidimą vien dėl to, kad egzistuoja teisės aktai, leidžiantys taikyti slapto sekimo priemones, Europos Žmogaus Teisių Teismas turi atsižvelgti į bet kokių teisių gynimo priemonių prieinamumą nacionaliniu lygmeniu ir riziką, kad atitinkamam asmeniui bus taikomos slapto sekimo priemonės[321]. Kai nebuvo galimybės užginčyti tariamo slapto sekimo priemonių taikymo nacionaliniu lygmeniu, negalima teigti, kad visuomenėje plačiai paplitę įtarimai ir susirūpinimas, kad slapto sekimo įgaliojimais piktnaudžiaujama, buvo nepagrįsti ir tokiais atvejais teismai itin atidžiai nagrinėja bylos faktines aplinkybes, ką tiesiogiai patvirtina Europos Žmogaus Teisių Teismo sprendimo byloje *Weber ir Saravia* prieš Vokietiją išsamumas[322].

Dėl subjekto kvalifikavimo pagrindinių teisių ribojimo auka, taip pat aktuali Europos Žmogaus Teisių Teismo praktiką byloje, kurioje vienas iš pareiškėjų buvo juridinis asmuo, konkrečiai byloje *Ekimdzhiev* prieš Bulgariją. Pareiškėjai, kurie buvo

319 *Ibid*, *60 p.*

320 „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją“*,* 78 p., Hudoc*,* žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/fre?i=001-76586.

321 „Europos Žmogaus Teisių Teismo 2010 m. gegužės 18 d. nutarimas byloje Nr. 26839/05 Kennedy prieš Jungtinę Karalystę“*,* Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf,.

322 Pavyzdžiui, Europos Žmogaus Teisių Teismas sprendime *Weber ir Saravia prieš Vokietiją* kaip savarankiškus argumentus nagrinėjo (i) ar Vokietijos teisėsaugos institucijoms suteiktais įgaliojimais pažeidžiama teisė į privatumą, (ii) ar Vokietijos nacionalinė teisėje įtvirtintas pagrindas tokiems teisės į privatumą pažeidimams, (iii) ar šie nacionaliniai teisės aktai yra pakankamai kokybiški, (iv) ar nustatyti ribojimai yra tikslingi ir būtini.

pelno nesiekianti asociacija ir pareiškėjų asociacijai Teisme atstovaujantis advokatas, teigė, kad pagal 1997 m. Specialiųjų stebėjimo priemonių įstatymą jiems galėjo būti bet kada ir be jokio įspėjimo taikomos stebėjimo priemonės[323]. Teismas konstatavo, kad jie taip pat gali teigti, jog šis įstatymas juos paveikė tiesiogiai ir pripažino jų aukos statusą, nepaisant to, kad jie kreipėsi ne kaip fiziniai asmenys, bet kaip juridiniai asmenys ir komercine veikla užsiimantis advokatas[324]. Atitinkamai ir kitose bylose, kuriose pareiškėjai buvo susiję su organizacijomis, dirbančiomis pilietinių laisvių srityje arba atstovaujančiomis pareiškėjams Europos Žmogaus Teisių Teisme, teismas laikėsi tos pačios argumentacijos ir nustatė, kad buvo kišamasi į šių organizacijų ar jų narių teises pagal Konvencijos 8 straipsnį[325].

Apibendrinant pateiktą Europos Žmogaus Teisių Teismo praktikos analizę, darytina išvada, kad teismas yra linkęs plačiai taikyti pagrindinių teisių apsaugos mechanizmus, įtvirtintus Konvencijoje ir sudaryti sąlygas efektyviai įgyvendinti teisę į pagrindinių teisių gynybą plačiam ratui asmenų. Tai daroma nepriklausomai nuo Konvencijos 25 str. 1 d. keliamo reikalavimo subjektams – ar pareiškėjai yra fiziniai, ar juridiniai asmenys (nors juridiniai asmenys įprastai laikomi neturinčiais teisės į privatumą) ir ar jie objektyviai gali pagrįsti, kad jų atžvilgiu apskritai buvo taikytos konkrečios sekimo priemonės.

### 4.1.3.2. Europos Žmogaus Teisių Teismo praktika dėl teisės į privatumą ribojimų nacionalinio saugumo tikslais

Konvencijos 8 str. įtvirtinta, kad kiekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas, o valdžios pareigūnai neturi teisės kištis į naudojimąsi šia teise, išskyrus įstatymo numatytus atvejus ir kai tai būtina demokratinėje visuomenėje valstybės saugumo interesams [...] apsaugoti. Taigi, bet koks kišimasis į privatų gyvenimą (net ir dėl nacionalinio saugumo tikslų) turi atitikti įstatymus, būti pateisinamas vienu iš išvardytų teisėtų tikslų ir

---

323 „Europos Žmogaus Teisių Teismo 2007 m. birželio 28 d. sprendimas byloje Nr. 62540/00 Ekimdzhiev prieš Bulgariją“, Bailii, žiūrėta 2021 m. rugpjūčio 2 d., https://www.bailii.org/eu/cases/ECHR/2007/533.html.

324 *Ibid*, 60 p.

325 „Europos Žmogaus Teisių Teismo 2008 m. liepos 1 d. sprendimas byloje Nr. 58243/00 Liberty ir kiti prieš Jungtinę Karalystę“, Bailii, žiūrėta 2021 m. rugpjūčio 2 d., https://www.bailii.org/eu/cases/ECHR/2008/568.html,; „Europos Žmogaus Teisių Teismo 2009 m. vasario 10 d. sprendimas byloje Nr. 25198/02 Iordachi ir kiti prieš Moldovą“, Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/fre?i=002-1661.

būtinas demokratinėje visuomenėje.

Todėl toliau pateikiama Europos Žmogaus Teisių Teismo praktikos analizė dėl šių trijų teisės į privatumo apribojimą nacionalinio saugumo pagrindais teisėtumo sąlygų.

#### *4.1.3.2.1. Teisės į privatumą pažeidimo nustatymas*

Taikant žmogaus stebėjimo priemones, paprastai nėra ginčijama, kad buvo kišamasi į privatų gyvenimą. Vis dėlto, kai kuriais atvejais, kai duomenys apie fizinius asmenis buvo tiesiog saugomi (o ne naudojami žvalgybos veikloje), Europos Žmogaus Teisių Teismo praktikoje buvo pateikti įdomūs paaiškinimai šiuo klausimu.

Byloje *Rotaru* prieš Rumuniją Europos Žmogaus Teisių Teismas nurodė, kad net ir vieša informacija gali patekti į privataus gyvenimo sritį, jei ji sistemingai renkama ir saugoma valdžios institucijų turimose bylose[326]. Pažymėtina, kad byloje *Uzun* prieš Vokietiją teismas laikėsi nuomonės, kad judėjimo viešoje vietoje stebėjimas naudojant GPS turėtų būti atskirtas nuo kitų vizualinio ar akustinio stebėjimo metodų, nes jie atskleidžia mažiau informacijos apie atitinkamo asmens elgesį, nuomones ir jausmus, taigi mažiau kišasi į jo privatų gyvenimą – todėl teismas nemanė, kad reikia taikyti tokias pat griežtas apsaugos priemones, kokias jis buvo nustatęs savo praktikoje dėl telekomunikacijų stebėjimo, kaip antai stebėjimo trukmės apribojimas arba gautų duomenų nagrinėjimo, naudojimo ir saugojimo tvarka[327].

Byla *Amman* prieš Šveicariją taip pat buvo susijusi informacijos saugojimu – skambučiu pareiškėjui iš Sovietų Sąjungos ambasados buvo užsakoma depiliacijos priemonė, kurią pareiškėjas platino Šveicarijoje. Šveicarijos prokuratūra klausėsi skambučio ir sudarė pareiškėjo bylą, kurioje buvo nurodyta, kad pareiškėjas yra „kontaktinis asmuo Rusijos ambasadoje“ ir „vykdo įvairaus pobūdžio veiklą su [A.] įmone“[328]. Teismas sprendė, kad pareiškėjui pakanka nustatyti, jog valdžios institucija saugojo duomenis, susijusius su asmens privačiu gyvenimu, kad būtų galima daryti išvadą, jog šiuo

---

[326] Šioje byloje buvo renkama ir saugoma informacija apie pareiškėjo studijas, politinę veiklą ir teistumą, o kai kurie iš duomenų buvo surinkti daugiau nei prieš penkiasdešimt metų. „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 28341/95 Rotaru prieš Rumuniją“, 44 p., Bailii, žiūrėta 2021 m. rugpjūčio 2 d., https://www.bailii.org/eu/cases/ECHR/2000/192.html.

[327] „Europos Žmogaus Teisių Teismo 2010 m. rugsėjo 2 d. sprendimas byloje Nr. 35623/05 Uzun prieš Vokietiją“, 35 p., Bailii, žiūrėta 2021 m. rugpjūčio 2 d., https://www.bailii.org/eu/cases/ECHR/2010/2263.html.

[328] „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 27798/95 Amman prieš Šveicariją“, 15 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-58497.

atveju ginčijamos bylos sukūrimas ir saugojimas prilygo kišimuisi į pareiškėjo teisę į privataus gyvenimo gerbimą Konvencijos 8 straipsnio prasme, neatsižvelgiant į tolesnį saugomos informacijos panaudojimą ir į tai, ar surinkta informacija buvo jautri, ar pareiškėjas patyrė kokių nors nepatogumų[329].

Nors Konvencijos 8 straipsniu iš esmės siekiama apsaugoti asmenį nuo savavališko valdžios institucijų kišimosi, jis įpareigoja valstybę ne tik susilaikyti nuo tokio kišimosi. Be šio visų pirma negatyvaus įsipareigojimo, Europos Žmogaus Teisių Teismo praktika rodo, kad gali būti ir pozityvių įsipareigojimų, susijusių su veiksminga pagarba privačiam ar šeimos gyvenimui. Byloje *McGinley ir Egan* prieš Jungtinę Karalystę pareiškėjams kilo abejonių, ar dalyvaudami branduoliniuose bandymuose jie patyrė pavojingą radiacijos poveikį ir jie prašė pateikti su tuo susijusią informaciją, tačiau Jungtinės Karalystės valdžios institucijos atsisakė suteikti informaciją, susijusią su pareiškėjų sveikata. Atsižvelgdamas į pareiškėjų siekį susipažinti su aptariama medžiaga ir į tai, kad nebuvo jokio svarbaus viešojo intereso ją išsaugoti, Europos Žmogaus Teisių Teismo sprendė, kad tais atvejais, kai Vyriausybė vykdė pavojingą veiklą, kaip šioje byloje, kuri galėjo turėti paslėptų neigiamų pasekmių tokioje veikloje dalyvaujančių asmenų sveikatai, pagarba privačiam ir šeimos gyvenimui pagal 8 straipsnį reikalavo, kad būtų nustatyta veiksminga ir prieinama procedūra, leidžianti tokiems asmenims gauti visą svarbią ir reikalingą informaciją, todėl Vyriausybei kilo atitinkama prievolė pateikti informaciją pagal 8 straipsnį[330].

Taigi, pagal Europos Žmogaus Teisių Teismo praktiką, kišimasis į asmens privatų gyvenimą yra pripažįstamas plačiai, nereikalaujant įrodyti surinktos informacijos panaudojimo tikslais, kuriais ji buvo rinkta bei neatsižvelgiant į tai, ar surinkta informacija buvo jautri; ar pareiškėjas dėl jos naudojimo patyrė kokių nors nepatogumų. Pabrėžtina, kad kišimasis į asmens privatų gyvenimą gali būti pripažįstamas net ir valstybių neveikimo atveju, kai jos nesuteikia **jų turimos** ir pareiškėjams objektyviai būtinos informacijos, kuri gali turėti didelės reikšmės asmenų privačiam gyvenimui (pavyzdžiui, tinkamai jų sveikatos apsaugai).

#### *4.1.3.2.2. Teisės į privatumą ribojimo įtvirtinimo įstatymuose reikalavimas*

Pagal nusistovėjusią Europos Žmogaus Teisių Teismo praktiką reikalavimas,

329 *Ibid*, 70 p.

330 „Europos Žmogaus Teisių Teismo 1998 m. birželio 9 d. sprendimas byloje Nr. 10/1997/794/995-996 McGinley ir Egan prieš Jungtinę Karalystę“, 101 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-58175.

kad bet kokiam įsikišimui į privatų gyvenimą būti „suderinamam su teise“ įvykdomas tik tada, kai tenkinamos trys sąlygos: ginčijamas įsikišimas turi turėti tam tikrą pagrindą vidaus teisėje, ji turi būti prieinama atitinkamam asmeniui ir turėti numatomas pasekmes[331].

Sprendime *Malone* prieš Jungtinę Karalystę Europos Žmogaus Teisių Teismo praktikoje pirmą kartą nustatytas pažeidimas šioje srityje. Didžiosios Britanijos teisės aktuose tiesiog užsimenama apie ministrų teisę leisti klausytis telefoninių pokalbių, tačiau ji iš tikrųjų nebuvo aiškiai įtvirtinta (t. y. suteikta), o administracinė tokios praktikos naudojiimosi tvarka nebuvo tiksliai apibrėžta[332]. Teismas pripažino, kad Konvencijos reikalavimai, ypač dėl numatomumo, negali būti visiškai vienodi specialiame ryšių perėmimo policijos tyrimų tikslais kontekste; būtent numatomumo reikalavimas negali reikšti, kad asmuo turėtų turėti galimybę numatyti, ar valdžios institucijos gali klausytis jo pranešimų ir kada tai gali padaryti, kad jis galėtų atitinkamai pakoreguoti savo elgesį, nes slaptumas yra viena iš taikomų priemonių efektyvumo prielaidų[333]. Vis dėlto įstatymas turėtų būti pakankamai aiškus, kad piliečiai galėtų tinkamai suprasti, kokiomis aplinkybėmis ir kokiomis sąlygomis valdžios institucijos galėjo imtis šio slapto ir potencialiai pavojingo kišimosi į asmens teisę į privataus gyvenimo ir susirašinėjimo gerbimą[334]. Kadangi slaptos ryšių kontrolės priemonių įgyvendinimo praktiškai negalėjo tikrinti nei atitinkami asmenys, nei visuomenė, teisinės valstybės principui prieštarautų tai, kad vykdomajai valdžiai suteikta teisinė diskrecija išreikšta kaip neribota galia, todėl įstatyme turėtų būti pakankamai aiškiai nurodyta kompetentingoms institucijoms suteiktos diskrecijos apimtis ir jos įgyvendinimo būdas, atsižvelgiant į atitinkamos priemonės teisėtą tikslą, kad asmuo būtų tinkamai apsaugotas nuo sava-

---

331 „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 28341/95 Rotaru prieš Rumuniją“, *supra note*, 348: 52 p.*;* „Europos Žmogaus Teisių Teismo 2010 m. gegužės 18 d. nutarimas byloje Nr. 26839/05 Kennedy prieš Jungtinę Karalystę“, *supra note*, 343: 151 p.; „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 27798/95 Amman prieš Šveicariją“, *supra note*, 350: 50 p.; „Europos Žmogaus Teisių Teismo 1990 m. balandžio 24 d. sprendimas byloje Nr. 11801/85 Kruslin prieš Prancūziją“, 27 p.*,* Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf.

332 „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Nr. 8691/79 Malone prieš Jungtinę Karalystę“, 68 p.*,* Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf.

333 *Ibid*, 67 p.

334 „Europos Žmogaus Teisių Teismo 1983 m. kovo 25 d. sprendimas byloje Nr. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 Silver ir kt. prieš Jungtinę Karalystę“, 88 p.*,* Hudoc*,* žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf.

vališko kišimosi[335].

Panašių argumentų Europos Žmogaus Teisių Teismas laikėsi ir byloje *Leander* prieš Švediją, nagrinėdamas konkretų su nacionaliniam saugumui įtaką darančių sektorių darbuotojų slaptos kontrolės kontekstą. Nors šioje srityje numatomumo reikalavimas ir negali būti toks pat kaip daugelyje kitų sričių, tai negali reikšti, kad asmenys gali tiksliai numatyti, kokius patikrinimus jų atžvilgiu atliks specialioji policija, vis dėlto įstatymas turėjo būti pakankamai aiškus, kad leistų tinkamai suprasti, kokiomis aplinkybėmis ir kokiomis sąlygomis valdžios institucijos gali imtis tokio slapto ir potencialiai pavojingo kišimosi į privatų gyvenimą[336]. Byloje *Amman* prieš Šveicariją teismas nustatė, kad teisės aktų reikalavimai, kuriuose nenumatytos taisyklės dėl sąlygų, kuriomis gali būti pradedamos bylos (turėjo būti nurodytos sąlygos, kuriomis gali būti sukurtos bylos, procedūros, kurių reikia laikytis, informacija, kuri gali būti saugoma), negali būti laikomos pakankamai aiškiomis ir detalizuotomis, kad užtikrintų adekvačią apsaugą nuo teisės į privatumą ribojimų[337].

Byla *Shimovolos* prieš Rusiją buvo susijusi su žmogaus teisių gynėjo vardo įregistravimu stebėjimo duomenų bazėje ir jo judėjimo stebėjimu. Europos Žmogaus Teisių Teismas šios bylos atveju taip pat nustatė Konvencijos 8 straipsnio pažeidimą *inter alia* dėl to, kad pagrindinė teisė buvo ribojama ne pagal įstatymą, nes duomenų bazė, kurioje buvo saugomas pareiškėjo vardas ir pavardė, nebuvo sukurta ministro įsakymu, nebuvo paskelbta ar kitaip padaryta viešai prieinama ir piliečiai negalėjo sužinoti, kodėl asmuo buvo užregistruotas šioje duomenų bazėje, kiek laiko buvo saugoma informacija apie jį, kokio pobūdžio informacija buvo įrašyta, kaip informacija buvo saugoma ir naudojama ir kas už ją buvo atsakingas[338].

Byloje *Kruslin* prieš Prancūziją Europos Žmogaus Teisių Teismo laikėsi nuomonės, kad telefoninių pokalbių pasiklausymas ir kitų formų telefoninių pokalbių perėmimas yra rimtas kišimasis į privatų gyvenimą ir susirašinėjimą, todėl jis turi būti grindžiamas ypač tiksliu įstatymu, o naudojamoms technologijoms nuolat tobulėjant, todėl yra būtina parengti aiškias ir išsamias taisykles šio teisės apribojimo taikymo at-

[335] „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Nr. 8691/79 Malone prieš Jungtinę Karalystę“, *supra note,* 354: 68 p.

[336] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Nr. 9248/81 Leander prieš Švediją“, 51 p., Bailii, žiūrėta 2021 m. rugpjūčio 2 d., https://www.bailii.org/eu/cases/ECHR/1987/4.html.

[337] „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 27798/95 Amman prieš Šveicariją“, *supra note*, 350: 76 p.

[338] „Europos Žmogaus Teisių Teismo 2011 m. birželio 21 d. sprendimas byloje Nr. 30194/09 Shimovolos prieš Rusiją“, 69 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., https://www.refworld.org/cases,ECHR,4e26e4d32.html.

žvilgiu[339]. Teismas atkreipė dėmesį, Prancūzijos sistema nesuteikė tinkamų apsaugos priemonių nuo įvairių galimų pažeidimų, pavyzdžiui, niekur nebuvo apibrėžtos asmenų, kurių telefonų gali būti klausomasi teismo nutartimi, kategorijos ir nusikaltimų, dėl kurių gali būti priimta tokia nutartis, pobūdis; niekas neįpareigojo teisėjo nustatyti telefonų pasiklausymo trukmės apribojimo; niekur nebuvo nurodyta, kokia tvarka turi būti rengiamos suvestinės su pasiklausytų pokalbių įrašais arba kokių atsargumo priemonių reikia imtis, kad įrašai būtų perduoti nepažeisti ir ištisi, kad juos galėtų patikrinti teisėjas (kuris vargu ar galėtų vietoje patikrinti originalių juostų skaičių ir ilgį) ir gynyba; niekur nebuvo nurodyta, kokiomis aplinkybėmis įrašai gali ar turi būti ištrinami arba juostos sunaikinamos, ypač tais atvejais, kai kaltinamasis tyrimo teisėjo buvo atleistas nuo baudžiamosios atsakomybės arba teismo išteisintas[340]. Dėl šių aplinkybių minimoje byloje įstatymas, suteikęs teisę klausytis asmenų pokalbių Prancūzijoje buvo pripažintas nepakankamai aiškiu ir išsamiu.

Byla *Kopp* prieš Šveicariją buvo susijusi su pareiškėjo advokatų telefoninių pokalbių pasiklausymu. Reikšminga faktinė aplinkybė šioje byloje yra ta, kad pareiškėjo asmeniniai ir verslo (advokato kontoros) telefonai buvo pasiklausomi, tačiau pareiškėjas vykdomame tyrime nebuvo įtariamasis (jo buvo pasiklausoma kaip „trečiojo asmens“) ir leidime pasiklausyti jo pokalbių buvo aiškiai nurodyta „teisininko pokalbių negalima imti domėn“[341]. Siekiant išvengti nepriimtino profesinės paslapties pažeidimo ir pareiškėjo kaip advokato pokalbių netinkamo panaudojimo, pagal galiojusią pasiklausymo praktiką, pareiškėjo pokalbiai buvo perklausomi Pašto tarnybos teisės departamento pareigūno, siekiant atskirti klausimus, susijusius su advokato darbu, nuo klausimų, susijusių su kita nei advokato veikla[342]. Teismas buvo ypač nustebęs dėl tokios situacijos ir dėl to, kad nepriklausomas teisėjas nevykdė jokios priežiūros, ypač jautrioje srityje, susijusioje su konfidencialiais advokato ir jo klientų santykiais, kurie tiesiogiai susiję su teise į gynybą, o ši funkcija buvo faktiškai patikėta Pašto tarnybos teisės departamento atstovui. Europos Žmogaus Teisių Teismas padarė išvadą, kad rašytinėje ar nerašytinėje Šveicarijos teisėje nebuvo pakankamai aiškiai nurodyta valdžios institucijų diskrecijos šiuo klausimu apimtis ir įgyvendinimo būdas ir kad pareiškėjas, kaip advokatas, tapo

---

339 „Europos Žmogaus Teisių Teismo 1990 m. balandžio 24 d. sprendimas byloje Nr. 11801/85 Kruslin prieš Prancūziją“, *supra note*, 353: 33 p.

340 *Ibid*, 35 p.

341 „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendimas byloje Nr. 30194/09 Kopp prieš Šveicariją“, 18 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-58144.

342 *Ibid*, 71 p.

Konvencijos 8 straipsnyje garantuojamų teisių pažeidimo auka[343].

Galiausiai reikėtų pažymėti, kad Europos Žmogaus Teisių Teismas, nagrinėdamas ginčus, nevertina išimtinai tik nacionalinės teisės aktų nuostatų, nustatydamas jų atitiktį kokybės, prieinamumo asmeniui ir aiškumo kriterijams. Teismo praktikoje pripažįstama, kad tinkamos pagrindinių teisių ribojimų taikymo sąlygos nebūtinai turi būti numatytos įstatymuose *per se*, tačiau jos taip pat gali būti nustatytos remiantis nacionalinių teismų praktika ir Europos Žmogaus Teisių Teismo praktika[344] bei akademinių autorių nuomone[345]. Taigi, pagal Europos Žmogaus Teisių Teismo praktiką, galimu teisės į privatumą ribojimo teisės šaltiniu pripažįstamas ne vien tik įstatymas, tačiau ir kiti teisės šaltiniai – teismų precedentai ir teisės doktrina.

Apibendrinant pateiktą Europos Žmogaus Teisių Teismo praktiką dėl galimybės riboti teisę į privatumą, atkreiptinas dėmesys, kad būtent privatumo ribojimo atvejai perimant pokalbius turi būti vertinami išskirtinai skrupulingai („specialiame kontekste“) dėl itin reikšmingo pagrindinės asmens teisės į privatumą ribojimo pobūdžio. Teisės aktai ne tik turi būti pakankamai aiškūs, kad piliečiai galėtų tinkamai suprasti, kokiomis aplinkybėmis ir kokiomis sąlygomis valdžios institucijos gali imtis slapto ir potencialiai pavojingo kišimosi į asmens teisę į privataus gyvenimo ir susirašinėjimo gerbimą, tačiau ir turi būti pakankamai detalūs ir aiškūs – juose turėtų būti pakankamai aiškiai nurodyta kompetentingoms institucijoms suteiktos diskrecijos apimtis ir jos įgyvendinimo būdas (pavyzdžiui, tvarka kaip ir kokiais atvejais turi būti užvedamos bylos dėl subjektų, kurių atžvilgiu taikomos priemonės; apibrėžtos asmenų, kurių telefonų gali būti klausomasi teismo nutartimi, kategorijos ir nusikaltimų, dėl kurių gali būti priimta tokia nutartis, pobūdis; įpareigojimas nustatyti telefonų pasiklausymo trukmės apribojimą; kokia tvarka turi būti rengiamos suvestinės su pasiklausytų pokalbių įrašais etc.).

#### *4.1.3.2.3. Teisės į privatumo ribojimo būtinumas demokratinėje visuomenėje, atsižvelgiant į siekiamą teisėtą tikslą*

Dažniausiai Europos Žmogaus Teisių Teismas nesudėtingai pripažįsta siekiamo

[343] „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendimas byloje Nr. 30194/09 Kopp prieš Šveicariją“, *supra note*, 363: 75 p.

[344] „Europos Žmogaus Teisių Teismo 1998 m. liepos 30 d.sprendimas byloje Nr. 58/1997/842/1048 Valenzuela Contreras prieš Ispaniją“, 34 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-58208&filename=001-58208.pdf.

[345] „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendimas byloje Nr. 30194/09 Kopp prieš Šveicariją)“, *op. cit.*, 60 p.

tikslo (pvz. nacionalinio saugumo apsaugos) teisėtumą ir savo praktikoje retai abejoja valstybės vertinimu dėl konkretaus teisės ribojimo tikslo. Dėl to valstybės turi plačią vertinimo laisvę nustatyti, ar egzistuouja konkretus pavojus nacionaliniam saugumui, todėl pagrindinis jo teisinės analizės objektas yra būtinumo demokratinėje visuomenėje klausimas. Vis dėlto, nors teismas pažymi, kad bet kuriuo konkrečiu atveju jis negali užginčyti nacionalinių valdžios institucijų sprendimo, susijusio su nacionalinio saugumo apsaugos tikslais, tačiau kompetentinga nepriklausoma institucija vis dėlto turi peržiūrėti sprendimo motyvus ir atitinkamus įrodymus, taikydama tam tikrą rungimosi principą[346]. Ši institucija turi įsitikinti, ar išvada, kad išslaptinimas keltų pavojų nacionaliniam saugumui, turi pagrįstą faktinį pagrindą[347].

Seniausiame ir svarbiausiu laikytiname sprendime šiuo klausimu byloje *Klass* ir kiti prieš Vokietiją Europos Žmogaus Teisių Teismas rėmėsi prielaida, kad demokratinėms visuomenėms grėsmę kelia itin sudėtingos šnipinėjimo ir terorizmo formos, dėl to valstybė, siekdama veiksmingai kovoti su tokiomis grėsmėmis, turi turėti galimybę vykdyti slaptą jos jurisdikcijoje veikiančių ardomųjų elementų stebėjimą[348]. Todėl teismas pripažino, kad kai kurie teisės aktai, suteikiantys įgaliojimus slapta sekti paštą, korespondenciją ir telekomunikacijas, išimtinėmis sąlygomis yra būtini demokratinėje visuomenėje nacionalinio saugumo interesais ir (arba) siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams[349]. Panašiai byloje *Leander* prieš Švediją teismas pripažino, kad negali kilti abejonių dėl būtinybės nacionalinio saugumo apsaugos tikslais susitariančiosiose valstybėse priimti įstatymus, suteikiančius kompetentingoms nacionalinėms institucijoms įgaliojimus, pirma, rinkti ir saugoti viešai neprieinamuose registruose informaciją apie asmenis ir, antra, naudoti šią informaciją vertinant kandidatų tinkamumą įsidarbinti nacionaliniam saugumui svarbiose pareigose[350].

Vertindamas naudojimąsi teisės į privatumą ribojimo galimybe nacionalinio saugumo pagrindais, Europos Žmogaus Teisių Teismas pažymėjo, kad negali pakeisti nacionalinių valdžios institucijų vertinimo bet kokiu kitu vertinimu, kuris būtų tinkamiausias šioje srityje ir todėl nacionalinis įstatymų leidėjas šiuo aspektu turi tam tikrą

[346] „Europos Žmogaus Teisių Teismo 2013 m. spalio 21 d. sprendimas byloje Nr. 55508/07 ir 29520/09 Janowiec ir kiti prieš Rusiją“, 213 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-127684&filename=001-127684.pdf.

[347] *Ibid*, 214 p.

[348] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *supra note*, 334: 48 p.

[349] *Ibid*, 49 p.

[350] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Nr. 9248/81 Leander prieš Švediją“, *supra note,* 358: 59 p.

diskreciją[351]. Byloje *Leander* prieš Švediją teismas detalizavo, kad valstybės turima diskrecija pasirenkant nacionalinio saugumo apsaugos priemones yra plati ir valstybė turi įvertinti, ar neatidėliotinas poreikis tikrai egzistuoja[352].

Tačiau, kaip suponuoja Konvencijos 8 str. 2 d. nuostatos, dėl tokio to, kad ribojamos pagrindinės asmenų teisės ir tokiu būdu keliamas pavojus demokratijai, teismas pabrėžė, kad valstybių diskrecija (nors ir plati, kaip minėta aukščiau) nėra neribota asmenims taikyti slaptas sekimo priemones, net ir kovoje su šnipinėjimu ir terorizmu[353]. Kadangi slaptas piliečių sekimas yra policinės valstybės požymis, jis toleruotinas tik tiek, kiek teisės aktuose numatytos priemonės tokiems tikslams pasiekti neviršija demokratinėje visuomenėje būtinų ribų[354] ir valstybės interesas saugoti savo nacionalinį saugumą turi būti suderintas su kišimosi į pareiškėjo teisę į privataus gyvenimo gerbimu[355].

Atkreiptinas dėmesys, kad Europos Žmogaus Teisių Teismas atliko ir šiam teisinių pagrindų nustatymui aktualių Konvencijos sąvokų lingvistinę analizę. Teismas nurodė, kad būdvardis „būtinas“ įtvirtintas Konvencijos 8 str. 2 d., 10 str. 2 dalyje, 11 str. 2 d. nėra sąvokų „privalomas“ (angl. *indispensable*) ar „griežtai būtinas“ (angl. *strictly necessary*) sinonimas, tačiau jis neturi tokio lankstumo kaip sąvokos „leistinas“ (angl. *admissible*), „įprastas“ (angl. *ordinary*) ar „protingas“ (angl. *reasonable*)[356].

Byloje *Kennedy* prieš Jungtinę Karalystę Europos Žmogaus Teisių Teismas laikėsi nuomonės, kad praktikoje sąvoka „griežtai būtina“ reiškia, jog ją taikant, teisės akte taip pat privalo būti numatytos ir tinkamos bei veiksmingos garantijos užkirsti kelią piktnaudžiavimui nustatomam teisės apribojimui (bylos atveju – slaptam piliečių sekimui), o šių garantijų pakankamumo vertinimas priklauso nuo įvairių aplinkybių, tokių, kaip galimų priemonių pobūdis, apimtis ir trukmė, pagrindai, reikalingi jas skirti, institucijos, kompetentingos jas sankcionuoti, vykdyti ir prižiūrėti, ir nacionalinės

---

[351] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *supra note,* 334: 49 p.

[352] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Nr. 9248/81 Leander prieš Švediją“, *supra note,* 358: 59 p.

[353] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *op. cit.,* 49 p.

[354] *Ibid*, 46, 49 p.

[355] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Nr. 9248/81 Leander prieš Švediją“, *op. cit.,* 59 p.

[356] „Europos Žmogaus Teisių Teismo 1976 m. gruodžio 7 d. sprendimas byloje Nr. 5493/72 Handyside prieš Jungtinę Karalystę“, 48 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-57499.

teisės aktuose numatytos teisių gynimo priemonės rūšis[357].

Taikomų stebėjimo priemonių teisėtumo peržiūra gali būti atliekama trimis etapais: pirmą kartą priimant sprendimą vykdyti stebėjimą, jam vykstant arba jį nutraukus[358]. Kalbant apie pirmuosius du etapus, pati slapto sekimo prigimtis ir logika reikalauja, kad ne tik pats sekimas, bet ir su juo susijusi peržiūra būtų atliekama asmeniui nežinant. Kadangi asmuo neišvengiamai negalės pasinaudoti veiksminga teisių gynimo priemone arba tiesiogiai dalyvauti bet kokioje peržiūros procedūroje, teismas byloje *Klass* ir kiti prieš Vokietiją nustatė, kad labai svarbu, jog vykdomosios valdžios institucijų kišimasis į asmens teises būtų veiksmingai kontroliuojamas, o tai paprastai turėtų užtikrinti teisminė valdžia, bent jau kraštutiniu atveju, nes teisminė kontrolė suteikia geriausias nepriklausomumo, nešališkumo ir tinkamos procedūros garantijas, o tai ypač svarbu srityje, kurioje piktnaudžiavimas potencialiai toks lengvas bei gali turėti tokių žalingų pasekmių visai demokratinei visuomenei[359].

Tačiau teisminės kontrolės nebuvimas nebūtinai reiškia Konvencijos 8 straipsnio pažeidimą, nes šį trūkumą galima ištaisyti priežiūros ir kitų teisės aktuose numatytų apsaugos priemonių pobūdį. *Klass* prieš Vokietiją byloje šias kitas priemones sudarė valdyba iš penkių parlamento narių (į kurios sudėtį proporcingai įėjo ir opozicijos atstovai) ir komisija, kurios abi buvo nepriklausomos nuo priežiūrą vykdančių institucijų ir kurioms buvo suteikta pakankamai įgaliojimų ir kompetencijos veiksmingai ir nuolatinei kontrolei vykdyti, todėl šios bylos atveju teismas padarė išvadą, kad abi priežiūros institucijos yra pakankamai nepriklausomos, kad galėtų priimti objektyvų sprendimą[360].

Byloje *Uzun* prieš Vokietiją, siekiant ištirti kaltinimus pasikėsinimu nužudyti politikus ir valstybės tarnautojus, už kuriuos atsakomybę prisiėmė teroristinis judėjimas, ir užkirsti kelią tolesniems sprogdinimams, GPS sistema pagalba buvo stebima transporto priemonė, todėl ši taikoma priemonė tarnavo nacionalinio saugumo ir visuomenės saugumo, nusikaltimų prevencijos tikslams[361]. Vertindamas priemonės

---

357 „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją“, *supra note,* 342: 78 p.; „Europos Žmogaus Teisių Teismo 2010 m. gegužės 18 d. nutarimas byloje Nr. 26839/05 Kennedy prieš Jungtinę Karalystę“, *supra note,* 343: 153 p.

358 „Europos Žmogaus Teisių Teismo 2010 m. gegužės 18 d. nutarimas byloje Nr. 26839/05 Kennedy prieš Jungtinę Karalystę“, *ibid*.

359 „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *supra note,* 334: 55 p.

360 *Ibid*, 21 p.

361 „Europos Žmogaus Teisių Teismo 2010 m. rugsėjo 2 d. sprendimas byloje Nr. 35623/05 Uzun prieš Vokietiją“, *supra note,* 349: 76 p.

proporcingumą, Europos Žmogaus Teisių Teismas išnagrinėjo numatytas garantijas (pavyzdžiui, tas, kurias visų pirma paminėjo *Kennedy* byloje – galimų priemonių pobūdį, apimtį ir trukmę) ir nustatė, kad GPS sekimas buvo vykdomas palyginti trumpą laiką (tris mėnesius); pareiškėją paveikė tik tada, kai jis važiavo savo bendrininko automobiliu, todėl jokiu būdu pareiškėjui nebuvo taikomas visiškas ir išsamus sekimas; jų skyrimo pagrindus – šiuo atveju tai buvo tyrimas dėl labai sunkių nusikaltimų[362]. Pažymėtina, kad šioje byloje teismas taip pat atsižvelgė į tai, kad GPS sekimas buvo įsakytas tik po to, kai kiti, mažiau intervenciniai metodai, pasirodė esą ne tokie sėkmingi[363].

Europos Žmogaus Teisių Teismo praktika dėl reikalavimo pranešti asmenims, kuriems buvo taikoma sekimo priemonė, autoriaus vertinimu, yra nevienareikšmė. Svarbu, kad suformuota bendra taisyklė, kad asmeniui turi būti pranešama apie jo atžvilgiu taikytas slapto sekimo priemones, tačiau tai gali būti atliekama ir vėliau, kad nesukelti pavojaus pagrindiniam tikslui, dėl kurio slapto sekimo priemonė apskritai ir buvo taikoma[364]. Tačiau vien tai, kad nustojus stebėti asmenį jam nepranešama, negali būti nesuderinama su Konvencijos 8 straipsniu, nes būtent slapta sekimo priemonė ir užtikrina „kišimosi" į jo privatumą veiksmingumą[365].

Kita vertus, esminis šiuo atveju yra teismo toleruojamas pranešimo apie taikytas slaptas priemones atidėjimo aspektas. Pagal teismo praktiką, pavojus, dėl kurio sekimas apskritai buvo taikytas, gali išlikti daugelį metų ar net dešimtmečius po konkrečios priemonės taikymo pabaigos, todėl net ir vėlesnis pranešimas subjektui gali kelti grėsmę ilgalaikiam tikslui, dėl kurio iš pradžių buvo pradėtas stebėjimas[366]. Taigi, teismas tikėtinai teisėtu pripažintų net kelių dešimtmečių ilgumo atidėjimo laikotarpį. Autoriaus vertinimu, tai yra kritiškai vertintina pozicija, kuri neužtikrina galimybės subjektams, kurių atžvilgiu buvo taikytos slaptos sekimo priemonės, efektyviai ir realiai apginti savo pažeidžiamas teises. Jokie ikiteisminiai tyrimai neturi būti vykdomi dešimtmečiais; o jei tokios praktikos ir egzistuoja, tai atsižvelgiant į Europos Žmogaus Teisių Teismo teisėjo Pettiti pritariančiąją nuomonę (angl. *concurring opinion*) *Kopp* prieš Šveicariją byloje, tokia priemonė gali būti laikoma ilgalaike informacijos „žvejoji-

---

362 *Ibid*, 80 p.

363 *Ibid.*

364 „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją", *supra note,* 342: 136 p.

365 „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją", *supra note*, 334: 58 p.

366 „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją", *op. cit.*, 136 p.

mo“ praktika, kuri prieštarauja žmogaus teisės į privatumą esmei[367].

Taip pat analizuojant pranešimo apie taikytas slaptas priemones atidėjimą, aktualu tai, kad „pavojaus“ teisėsaugos ar žvalgybos institucijų atliekamam tyrimui nustatymas yra subjektyvus sprendimas, tačiau nuo jo priklauso asmens, kurio atžvilgiu taikytos slaptos sekimo priemonės, galimybės apginti savo teises, jei jų pažeidimai buvo padaryti. T. y. nuo to subjekto, kuris priims sprendimą ar pavojus atliekamoms tyrimams ir su jais susijusioms veikloms išnyko, priklauso asmenų teisinės ir faktinės galimybės nustatyti ar jų teisė į privatumą buvo pažeista. Bylose *Klass* prieš Vokietiją ir *Weber ir Saravia* prieš Vokietiją Europos Žmogaus Teisių Teismas nustatė, kad šį sprendimą (informuoti asmenis apie jų atžvilgiu taikytas slaptas sekimo priemones, ar ne) priėmė nepriklausomas subjektas (G10 komisija)[368]. Būtent tokia Vokietijos teisinio reguliavimo nuostata (nepriklausomo subjekto įtraukimas į sprendimo dėl taikytų privatumą ribojančių priemonių pranešimo asmeniui priėmimą) užtikrino veiksmingą pranešimo mechanizmą, kuris suteikė galimybę kištis į privatų gyvenimą neviršijant to, kas būtina teisėtiems tikslams pasiekti, priešingai nei teismas sprendė byloje *Zakharov* prieš Rusiją dėl Rusijos teisinio reguliavimo analogišku klausimu[369].

Autoriaus vertinimu, tokia teisės aktų interpretacija sudaro galimybes valstybėms narėms piktnaudžiauti pranešimo asmenims apie jų atžvilgiu taikytas priemones atidėjimu. Pagal aukščiau analizuotą Europos Žmogaus Teisių Teismo praktiką, jei teisės aktai numato procedūrą dėl pranešimo asmeniui apie taikytas slaptas priemones atidėjimo pagrįstumo vertinimą ir nėra jokių įrodymų ar požymių, kad faktinė taikoma praktika skiriasi nuo teisės aktuose nustatytos praktikos, teismas preziumuoja, kad tokios taisyklės yra taikomos pagrįstai ir teisėtai[370]. Taigi, jei valstybės savo teisės aktuose nusimato tokią procedūrą ir sugeba jos priimamus sprendimus išlaikyti paslaptyje, nepriklausomai nuo jų kokybės ir pagrįstumo, pareiga pranešti apie taikytas apsaugos priemones nebus įgyvendinama. Tokiu būdu teisės į privatumą esmė bus pažeidžiama, o asmenys neturės jokios teisinės galimybės ją apginti.

Teismas taip pat nagrinėjo teisės į privatumą ribojimo proporcingumo kriteri-

[367] Teisėjo Pettiti pritariančioji nuomonė „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendime byloje Nr. 30194/09 Kopp prieš Šveicariją“*, supra note,* 363.

[368] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *supra note*, 334: 19 p.; „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją“, *supra note,* 342: 136 p.

[369] „Europos Žmogaus Teisių Teismo 2015 m. gruodžio 4 d. sprendimas byloje Nr. 47143/06 Zakharov prieš Rusiją“, 288 p.*,* Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-159324.

[370] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“, *op. cit.*, 59 p.

jus bylose, susijusiose su ilgalaikiu informacijos saugojimu saugumo bylose. Europos Žmogaus Teisių Teismas byloje *Rotaru* prieš Rumuniją padarė išvadą, kad informacijos apie pareiškėjo privatų gyvenimą (studijas, politinę veiklą ir jo teistumą, kai kuri informacija buvo senesnė nei 50 metų) saugojimas ir naudojimas pažeidė pareiškėjo teisę į privatų gyvenimą[371].

Panaši situacija buvo kilusi byloje *Segerstedt-Wiberg* ir kiti prieš Švediją, kurioje atsakovė Švedija, siekdama pateisinti bylų saugojimą Saugumo policijoje, visų pirma rėmėsi nacionalinio saugumo pagrindu[372]. Nagrinėdamas atliekamo teisės į privatumą ribojimo proporcingumo klausimą, teismas atsižvelgdamas į informacijos pobūdį ir saugojimo trukmę nustatė, kad informacijos apie keturių iš penkių pareiškėjų (pvz., vieno pareiškėjo dalyvavimas politiniame susirinkime Varšuvoje 1967 m.; kito pareiškėjo tariamas pasisakymas už smurtinį pasipriešinimą prieš policijos kontrolę 1969 m. demonstracijų metu) saugojimas nebuvo pagrįstas svarbiomis ir pakankamomis priežastimis, susijusiomis su nacionalinio saugumo apsauga, todėl tai buvo laikomas neproporcingu kišimusi į pareiškėjų privatų gyvenimą[373].

Sprendimas byloje *Dalea* prieš Prancūziją susijęs su pareiškėjo negalėjimu susipažinti su savo duomenimis, ilgą laiką įrašytais Šengeno informacinės sistemos bylose ir juos ištaisyti (po to, kai Prancūzijos saugumo žvalgybos agentūra duomenis apie asmenį įrašė į šią sistemą, jam buvo uždrausta patekti į visas Šengeno susitarimą taikančias šalis)[374]. Byloje Europos Žmogaus Teisių Teismas pabrėžė, kad kiekvienam asmeniui, kuriam taikoma nacionalinio saugumo pagrindais grindžiama teisių ribojimo priemonė, turi būti užtikrinta apsauga nuo savavališkumo: nors jis (teismas) negali užginčyti nacionalinių valdžios institucijų sprendimo, susijusio su nacionalinio saugumo sumetimais, kompetentinga nepriklausoma institucija turi peržiūrėti sprendimo motyvus ir atitinkamus įrodymus, taikydama tam tikrą rungimosi principą[375].

Atsižvelgdamas į šią praktiką, Europos Žmogaus Teisių Teismas atsižvelgė į kelias pareiškėjui prieinamas teisės gynimo priemones pagal Prancūzijos teisę: pareiškė-

---

371 „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 28341/95 Rotaru prieš Rumuniją“, *supra note*, 348: 62 p.

372 „Europos Žmogaus Teisių Teismo 2006 m. birželio 6 d. sprendimas byloje Nr. 62332/00 Segerstedt-Wiberg ir kiti prieš Švediją“, 49 p., Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-75591.

373 *Ibid*, 90 p.

374 „Europos Žmogaus Teisių Teismo 2010 m. vasario 2 d. sprendimas byloje Nr. 964/07 Dalea prieš Prancūziją*“, Hudoc*, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-97520.

375 „Europos Žmogaus Teisių Teismo 2013 m. spalio 21 d. sprendimas byloje Nr. 55508/07 ir 29520/09 Janowiec ir kiti prieš Rusiją“, *supra note,* 368: 213 p.

jas galėjo prašyti, kad ginčijamą priemonę peržiūrėtų – iš pradžių Prancūzijos nacionalinė duomenų apsaugos komisija, vėliau – *Conseil d'Etat* (institucija, kuri pataria vykdomajai valdžiai ir yra aukščiausiasis teismas administracinių ginčų srityje)[376]. Nors pareiškėjui niekada nebuvo suteikta galimybė ginčyti tikslių jo įtraukimo į Šengeno duomenų bazę motyvų, jam buvo suteikta galimybė susipažinti su visais kitais su juo susijusiais duomenimis ir jis buvo informuotas, kad Prancūzijos saugumo tarnybos iniciatyva ataskaita buvo parengta dėl valstybės saugumo, gynybos ir visuomenės saugumo sumetimų, todėl teismas padarė išvadą, kad tai, jog pareiškėjas negalėjo asmeniškai susipažinti su visa jo prašoma informacija, savaime neįrodo, kad kišimasis nebuvo pateisinamas nacionalinio saugumo interesais ar neproporcingas[377].

Kita vertus, priešingas sprendimas buvo priimtas byloje *Janowiec* ir kiti prieš Rusiją. Pareiškėjai šioje byloje buvo 1940 m. sovietų slaptosios policijos be teismo nužudytų lenkų karininkų ir pareigūnų giminaičiai, kurie siekė susipažinti su informacija apie 1990 m. pradėtą masinių žudynių tyrimą, kuris 2004 m. buvo nutrauktas. Sprendimo nutraukti tyrimą tekstas liko įslaptintas ir pareiškėjai neturėjo galimybės susipažinti nei su šiuo dokumentu, nei su kita su tyrimu susijusia informacija. Rusijos teismai sistemingai atmesdavo daugkartinius prašymus leisti susipažinti su sprendimu ir išslaptinti jo slaptumo žymą, o valdžios institucijos taip pat atsisakė pateikti sprendimo kopiją Europos Žmogaus Teisių Teismui, motyvuodamos tuo, kad šis dokumentas neturi esminės reikšmės pareiškėjų bylai ir kad vidaus teisė draudžia atskleisti įslaptintą informaciją[378].

Šioje byloje Europos Žmogaus Teisių Teismas negalėjo pritarti Rusijos paaiškinimams, kad reikalaujamų dokumentų pateikimas paveiktų Rusijos nacionalinį saugumą atsižvelgdamas į tai, kad nacionalinis teismas šių aplinkybių savarankiškai netyrė ir nevertino[379]; Rusija turėjo teisę pateikti bent jau dalinai išslaptintą dokumentą arba prašyti konfidencialių teismo posėdžių, tačiau tuo nepasinaudojo[380]. Atkreiptinas dėmesys, kad reikšmingiausia Europos Žmogaus Teisių Teismo praktika šiuo klausimu (valstybės atsisakymu pateikti prašomus dokumentus) suformuota bylose būtent prieš

---

376 „Europos Žmogaus Teisių Teismo 2010 m. vasario 2 d. sprendimas byloje Nr. 964/07 Dalea prieš Prancūziją", *supra note,* 396.

377 *Ibid.*

378 „Europos Žmogaus Teisių Teismo 2013 m. spalio 21 d. sprendimas byloje Nr. 55508/07 ir 29520/09 Janowiec ir kiti prieš Rusiją*, supra note,* 368: 207 p.

379 *Ibid*, 214 p.

380 *Ibid*, 215 p.

Rusiją[381].

Apibendrinant analizuoutą Europos Žmogaus Teisių Teismo praktiką, darytina išvada, kad valstybės, vertindamos grėsmes nacionaliniam saugumui ir spręsdamos, kaip su jomis kovoti, turi netgi didelę veiksmų laisvę. Vis dėlto, aktualioje praktikoje, teismas linkęs reikalauti, kad nacionalinės institucijos patikrintų, ar bet kokia grėsmė, siejama su nacionalinio saugumo pagrindo taikymu, yra pagrįsta. Dėl sąlygos, kad kišimasis turi būti atliekamas „pagal įstatymą", Europos Žmogaus Teisių Teismas laikosi nuomonės, kad įstatymas, tiek prieinamas, tiek ir numatomas, turi būti gana išsamus. Teismas ypatingą dėmesį skiria apsaugos priemonėms, kurios turi būti taikomos stebint ir saugant įrašus. Kalbant apie būtinumo demokratinėje visuomenėje sąlygą, teismas sprendimą priima atsižvelgdamas į Valstybės atsakovės interesą apsaugoti savo nacionalinį saugumą ir pareiškėjo teisės į privataus gyvenimo gerbimo pažeidimo rimtumą; griežtas būtinumas praktikoje apibrėžiamas kaip reikalaujantis tinkamų ir veiksmingų garantijų nuo piktnaudžiavimo ir teisminių institucijų ar bent jau nepriklausomų priežiūros institucijų vykdomos priežiūros.

## 4.2. Didžiausia sėkmingo asmens duomenų perdavimo tarp skirtingų teisinių sistemų problema pagal *Schrems II* bylą

JAV mokslininkai Europos Sąjungos Teisingumo Teismo išaiškinimus *Schrems II* byloje kritikuoja ir nurodo, kad teismo atliktas JAV teisės aktų proporcingumo vertinimas, buvo paviršutiniškas ir neaiškus, todėl nežinia, kokios konkrečiai teisės aktuose įtvirtintos teisės į privatumą ribojimo priemonės gali būti vertinamos perteklinėmis (ne „griežtai būtinos")[382]. Atitinkamai, neišsami teismo analizė pateikia mažai rekomendacijų reikalingiems ir ateityje neišvengiamai numatomiems priimti sprendimams dėl teisės į privatumo apsaugos tinkamumo JAV. Autoriaus vertinimu, pateikiamos už-

[381] Žr. pvz. „Europos Žmogaus Teisių Teismo 2010 m. rugsėjo 16 d. sprendimas byloje Nr. 75472/01 Tigran Ayrapetyan prieš Rusiją", Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-100377&filename=001-100377.pdf.; „Europos Žmogaus Teisių Teismo 2008 m. sausio 24 d. sprendimas byloje Nr. 839/02 Maslova ir Nalbandov prieš Rusiją", Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-2241782-2402590&filename=003-2241782-2402590.pdf.; „Europos Žmogaus Teisių Teismo 2005 m. liepos 5 d. sprendimas byloje Nr. 49790/99 Trubnikov prieš Rusiją", Hudoc, žiūrėta 2021 m. rugpjūčio 2 d., http://hudoc.echr.coe.int/eng?i=001-69616.

[382] „National Security Law - Surveillance - Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield – Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020)", *supra note,* 253: 1567.

sienio mokslininkų pozicijos ir kritika Europos Sąjungos Teisingumo Teismo sprendimui *Schrems II* byloje yra pagrįsta, tačiau ne šie teismo sprendimo trūkumai laikytini esminiais – keliančiais didžiausią grėsmę sėkmingo susitarimo tarp Europos Sąjungos ir JAV pasiekimui ir po *Schrems II* sprendimo.

Autoriaus vertinimu, reikšmingiausia Europos Sąjungos Teisingumo Teismo pozicija *Schrems II* byloje sėkmingo susitarimo dėl privatumo apsaugos tarp Europos Sąjungos ir JAV atžvilgiu yra susijusi su vienu pirmųjų ir (mažiausiai motyvuotu) teismo nagrinėtu klausimu – ar BDAR yra taikomas asmens duomenų perdavimui, atliktam valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, jei atliekant šį perdavimą ar po jo šios trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais.

Generalinis advokatas šioje byloje pateiktoje išvadoje nurodė, kad siekiant nustatyti, ar Europos Sąjungos teisė taikytina nagrinėjamam duomenų perdavimui, reikia atsižvelgti tik į veiklą, kurią vykdant perduodami šie duomenys ir nėra svarbu, kokiu tikslu vėliau trečiosios paskirties šalies viešosios valdžios institucijos galbūt tvarkys perduotus duomenis[383].

Autoriaus vertinimu, tokia prielaida nors ir yra suprantama iš asmens duomenų tvarkymo perspektyvos, tačiau yra itin reikšminga galimo susitarimo dėl asmens duomenų perdavimo su bet kuria trečiąja šalimi dėl duomenų perdavimo pasiekimo, nes tokiu būdu *de jure* į duomenų perdavimo į trečiąją šalį atitikties vertinimą BDAR atžvilgiu įtraukia ir trečiosios šalies nacionalinio saugumo sritį. Primintina, kad būtent žvalgybos institucijų prieiga prie į JAV perduodamų asmens duomenų ir buvo viena iš pagrindinių faktinių *Privacy Shield* susitarimo panaikinimo priežasčių[384].

Šiuo aspektu pabrėžtina, kad pagal Europos Sąjungos Sutarties 4 str. 2 d., kiekviena valstybė narė yra išimtinai atsakinga visų pirma už savo nacionalinį saugumą[385]. Atitinkamai, BDAR įtvirtinta, kad BDAR netaikomas pagrindinių teisių ir laisvių apsaugai, susijusiai su Europos Sąjungos teisės nereglamentuojama veikla, pa-

---

383 „Generalinio advokato Henrik Saugmandsgaard Øe išvada, pateikta 2019 m. gruodžio 19 d. byloje Nr. C-311/18 Schrems II“, 105 p., InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3638243.

384 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 165 p.

385 „Europos Sąjungos sutartis“, *supra note,* 78.

vyzdžiui, su nacionaliniu saugumu susijusia veikla[386].

Kita vertus, net atsižvelgdamas į Europos Sąjungos Sutarties 4 str. 2 d. nuostatas, Europos Sąjungos Teisingumo Teismas pabrėžė, kad ši Europos Sąjungos Sutarties garantija yra skirta išimtinai tik valstybių narių atžvilgiu, todėl nagrinėjant klausimą dėl duomenų perdavimo į trečiąsias šalis, klausimas dėl galimybės taikyti teisės į privatumą apribojimus, kildinamus iš Europos Sąjungos Sutarties ir susijusius su nacionaliniu saugumu, apskritai net neaktualus[387]. Tokiu būdu Europos Sąjungos Teisingumo Teismas užėmė poziciją, kad atvejais, kai asmens duomenys yra perduodami iš Europos Sąjungos į trečiąją šalį, vertinant trečiosios šalies taikomas duomenų apsaugos taisykles, privalo būti vertinamas šios trečiosios šalies nacionalinio taikomų saugumo užtikrinimo priemonių proporcingumas teisės į privatumą (kaip ji suprantama ir taikoma Europos Sąjungoje), atžvilgiu.

Kaip nurodyta aukščiau, tokia išvada padaryta nepaisant to, kad pačios Europos Sąjungos valstybės narės turi visišką laisvę užtikrinant savo nacionalinį saugumą ir jį užtikrinančių priemonių proporcingumas nėra tikrinamas atitikties BDAR atžvilgiu. Autoriaus vertinimu, tokia Europos Sąjungos Teisingumo Teismo pozicija sukuria pamatinį kliuvinį Europos Sąjungai siekiant ateityje sudaryti duomenų perdavimo susitarimą su bet kuria trečiąja šalimi, nes ši šalis privalės atsisakyti savo nacionalinio saugumo užtikrinimo priemonių, taikomų perduodamų asmens duomenų iš Europos Sąjungos atžvilgiu, arba suteikti galimybę Europos Sąjungos Teisingumo Teismui būti arbitru, ar konkrečios trečios šalies taikomos nacionalinio saugumo užtikrinimo priemonės yra proporcingos BDAR atžvilgiu, ar ne.

Toks Europos Sąjungos Teisingumo Teismo požiūris ir formuojama praktika nors ir yra vedina kilnių norų saugoti Europos Sąjungos piliečių teisę į privatumą, trečiosioms šalims *de facto* primeta net ne Europos Sąjungos taikomą (t. y. aukštą) teisės į privatumo apsaugą standartą, bet dar aukštesnį teisės į privatumą apsaugos standartą – nes šios šalys privalo ir savo nacionalinį saugumą užtikrinančias priemones (taikomas iš Europos Sąjungos gaunamai informacijai) suderinti su BDAR[388], ko neturi atlikti Europos Sąjungos valstybės narės. Tokia pozicija, autoriaus vertinimu, laikytina drąsia

---

386 „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)“, *supra note,* 60: 2 str. 2 d. d) p. ir preambulės 16 p.

387 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8*:* 81 p.

388 *Ibid*, 88 p.

ir ją galėtų primesti tik dominuojantis subjektas silpnesniajam kontrahentui, tačiau ar Europos Sąjungos vaidmuo yra toks svarbus, nėra vienareikšmiškai aišku. Doktrinoje pateikiamos nuomonės, kad ši Europos Sąjungos lyderystė įgyja pagreitį ir dėl savo didelės rinkos galios bei pasaulinės įtakos Europos Sąjunga šiuo metu ryškėja kaip *de facto* pasaulinė privatumo reguliavimo institucija, nes BDAR principais pagrįsti privatumo apsaugos režimai įtvirtinami Brazilijoje, Tailande, Indijoje ir kitose jurisdikcijose[389].

Transatlantiniai duomenų srautai tarp Europos Sąjungos ir JAV yra greičiausi ir didžiausi pasaulyje, bei sudaro daugiau nei pusę Europos duomenų srautų ir apie pusę JAV duomenų srautų; JAV ir Europos Sąjungos yra svarbiausios komercinės partnerės kalbant apie skaitmenines paslaugas[390]. Atsižvelgdami į Europos Sąjungos ir JAV tarpusavio ryšius bei ekonominę priklausomybę, kritiški JAV mokslininkai Europos Sąjungos Teisingumo Teismo poziciją laiko „dviveidiška teisminio imperializmo apraiška“[391]. Autoriaus vertinimu, tikėtinas Europos Sąjungos Teisingumo Teismo motyvas, nusprendžiant dėl Europos Sąjungos privatumo apsaugos taisyklių primetimo JAV, panaikinant *Safe Harbour* ir *Privacy Shield* susitarimus, buvo tas, kad ekonominė JAV įmonių svarba egzistuojant tarpvalstybiniams Europos Sąjungos ir JAV asmens duomenų srautams padės priversti JAV reformuoti jei savo asmens duomenų naudojimo taisykles, ar bent tai, kaip JAV nacionalinės saugumo agentūros renka ir naudoja asmens duomenis.

Iki Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje, toks lūkestis buvo pagrįstas ir, manytina, pildėsi, nes po *Safe Harbour* susitarimo panaikinimo, JAV parodė gerą valią – norą derėtis ir atlikti tam tikrą privatumo apsaugos JAV teisinėje sistemoje reformą bei sudarė daug kompromisų, atsižvelgiant į Europos Sąjungos teisės į privatumo reguliavimą bei Europos Sąjungos Teisingumo Teismo pozicijas *Schrems* byloje (pvz., *Privacy Shield* susitarime įsteigiant specialaus ombudsmeno poziciją etc.). Tačiau net ir čia JAV reformos, siekiant priimti gauti pozityvų sprendimą dėl siūlomos asmens duomenų apsaugos adekvatumo, buvo ribotos ir, kaip dabar žinome (dėl Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje pagrindu pa-

---

389 Paul M. Schwartz, „Global Data Privacy: The E.U. Way“, *New York University Law Review* 94, 4 (2019): 771; Mark Scott ir Lauren Cerulus, „Europe's New Data Protection Rules Export Privacy Standards Worldwide“, *Politico* (2018): 4.

390 Daniel S. Hamilton ir Joseph P. Quinlan, *The Transatlantic Economy 2020: Annual Survey Of Jobs, Trade And Investment Between The United States And Europe* (2020), 8.

391 Stewart Baker, „The Cyberlaw Podcast: Solipsistic Europocrisy Meets Judicial Imperialism“, *LAWFARE*, žiūrėta 2021 m. gegužės 10 d., https://www.lawfareblog.com/cyberlaw-podcast-solipsistic-europocrisy-meets-judicial-imperialism.

naikinto *Privacy Shield* susitarimo), Europos Sąjungos Teisingumo Teismo vertinimu, nepakankamos.

Apibendrinant nurodytus argumentus, autoriaus vertinimu, aktualiausia Europos Sąjungos Teisingumo Teismo sprendime byloje *Schrems II* suformuota problema, kelianti didžiausią iššūkį galimiems susitarimams dėl duomenų perdavimo tarp Europos Sąjungos ir JAV – trečiosios šalies taikomų nacionalinį saugumą užtikrinančių priemonių atitikties vertinimo BDAR atžvilgiu taikymas.

Atkreiptinas dėmesys, kad tarptautinėje teisėje pripažįstamas *estoppel* principas. Šis principas gina teisėtus vienos valstybės lūkesčius, siekiant susitarimo su kontrahentu ir pasitikint kitos valstybės (ar supranacionalinės organizacijos) gera valia bei sąžiningumu[392]. Europos Sąjungos Teisingumo Teismo sprendimas byloje *Schrems II* paneigia *estoppel* principą ir pasitikėjimą JAV gera valia, nes priešingai nei Europos Sąjungos valstybių narių atžvilgiu, JAV atžvilgiu Europos Sąjungos Teisingumo Teismas rodo nepasitikėjimą ir pripažįsta privalomą BDAR taikymą asmens duomenų tvarkymo atžvilgiu, net kai šių duomenų tvarkymas atliekamas JAV nacionalinio saugumo interesais, nors Europos Sąjungos valstybėms narėms šiuo atžvilgiu yra taikoma išimtis ir jos neturi nei atskleisti savo nacionalinio saugumo gynimo priemonių, nei jų riboti (ar pritaikyti) atsižvelgdamos į imperatyvų BDAR reguliavimą.

Ankstesnėse darbo dalyse pateikta nacionalinio saugumo sampratos analizė nurodo, kad nacionalinis saugumas negali būti apibrėžtas kaip teisinė kategorija ir apima įvairius šalių fizinio, ekonominio saugumo ir net svarbiomis laikomų vertybių apsaugos aspektus. Taigi, šiuo aspektu neaišku, ar Europos Sąjungos Teisingumo Teismo sprendimu *Schrems II* byloje sprendimu sukurta teisinė problema apskritai gali būti išspręsta.

## 4.3. Proporcingumo principo reikšmė privatumo apsaugai perduodant asmens duomenis tarp skirtingų teisinių sistemų

### 4.3.1. Proporcingumo principo samprata

Teisėsaugos ir saugumo institucijų sėkminga veikla remiasi masiniu duomenų rinkimu ir analize, o ypač – asmens duomenimis, kurie naudojami kaip pagrindinis

[392] R. Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press, 2007).

tyrimo įrankis[393]. Teisine prasme svarbu tai, kad duomenų rinkimas ir apdorojimas iš esmės nepriklauso nuo duomenų kilmės vietos ar teisinės jurisdikcijos. Ši besikeičianti praktika ir itin platus asmens duomenų naudojimas kelia teisines ir praktines problemas nustatant prioritetus konkuruojantiems tikslams, t. y. renkantis tarp nacionalinio saugumo užtikrinimo ir nusikalstamumo prevencijos bei pagrindinių teisių (ypač teisės į privatumą) apsaugos. Europos Sąjungos teisės kontekste, proporcingumo principas yra vienas reikšmingiausių teisinių konceptų, galinčių padėti nustatyti protingą pusiausvyrą tarp viešųjų interesų. Teisės doktrinoje galima rasti pritariančių pozicijų, kad raktas į teisingą sprendimą dėl žmogaus teisių apsaugos į dėl tinkamo asmens duomenų apdorojimo iš esmės slypi Europos Sąjungos Teisingumo Teismo praktikoje dėl proporcingumo principo taikymo[394].

Tačiau, autoriaus vertinimu, šiuo atveju proporcingumo principo taikymas nėra toks paprastas. Dėl sparčiai besikeičiančių ir tobulėjančių technologijų, kurios įgalina tiek asmenis bendrauti tarpusavyje, patogiai, greitai ir, dažniausiai, neatlygintinai, kaupti duomenis, tiek teisėsaugos ar saugumo institucijas prieiti prie jų, statiškų teisės aktų proporcingas taikymas tampa žymiai sudėtingesniu uždaviniu. Šis uždavinys tampa dar sunkiau įveikiamas, kai žvalgybos priemonės taikomos skirtingų valstybių teritorijose, kaip, pavyzdžiui, duomenų perdavimo tarp Europos Sąjungos ir JAV atveju.

*Schrems* bylos atveju, Europos Sąjungos Teisingumo Teismas konstatavo, kad *Safe Harbour* susitarimas (kuris suteikė duomenų perdavimui tarp Europos Sąjungos į JAV teisinį pagrindą), negalioja. Šis susitarimas buvo panaikintas Europos Sąjungos Teisingumo Teismui nustačius, kad jis neužtikrina adekvataus asmens duomenų apsaugos lygio JAV. Tačiau šios išvados pagrindinis motyvas yra paremtas proporcingumo principo taikymu, nes pagrindas šiai išvadai buvo neproporcingas masinis (t. y. neindividualizuotas) asmens duomenų rinkimas ir prieiga prie jų, kuri buvo suteikta JAV žvalgybos institucijoms (kaip atskleidė NSA pranešėjas Edvardas Snoudenas)[395]. Nors JAV institucijų taikoma praktika dėl asmens duomenų naudojimo ir atitiko *Safe Harbour* susitarimo reikalavimus, Europos Sąjungos Teisingumo Teismas nustatė, kad tokia plati, neapribota prieiga prie jų ir taikomos žvalgybos priemonės

---

393 David Lyon, „Surveillance after Snowden“, *European Journal of Communication* 31, 3 (2016): 366-67.

394 C.B. Tranberg, „Proportionality and Data Protection in the Case Law of the European Court of Justice“, *International Data Privacy Law* 1, 4 (2011): 239.

395 Christina Lam, „Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in *Schrems* v. Irish Data Protection Commissioner”, *Boston College International and Comparative Law Review* 40, 3 (2017): 1.

pažeidžia asmens teisę į privatumą, kurią suteikia Europos Sąjungos teisė[396] ir, kuri, pagal Europos Sąjungos Teisingumo Teismo praktiką, turi būti ginama neformaliai[397].

Analogiškai, *Schrems II* bylos atveju, Europos Sąjungos Teisingumo Teismas pripažino negaliojančiu *Privacy Shield* susitarimą negaliojančiu dėl JAV taikomų duomenų apsaugos apribojimų, kurie pažeidžia proporcingumo principą, nes JAV vykdomos asmens duomenų rinkimo ir analizės programos (pvz. PRISM, UPSTREAM) nenustato „minimalių apsaugos priemonių" ir nėra „apribotos tuo, kas griežtai būtina"[398].

Proporcingumo principo ištakos Europos teisėje siejamos su XVIII ir XIX amžiaus Prūsijos teise, kur ji atsirado kaip septinitas principas, ribojantis valstybės administracinius įgaliojimus[399]. Po Antrojo pasaulinio karo jis buvo pripažintas pagrindiniu Vokietijos teisės principu (vok. *Verhältnismassigkeit*), kuris taip pat atsispindi ir Vokietijos konstitucijoje (vok. *Grundgesetz*)[400]. Asmens teisių apsaugos ir jų apribojimų viešojo intereso tikslais tarpusavio priklausomybę atspindi būtent proporcingumo principas, kuris Europos Sąjungos teisėje ir Europos Sąjungos Teisingumo Teismo praktikoje buvo pripažintas vienu bendrųjų Europos Sąjungos teisės principų[401].

Proporcingumo principo reikšmė randant santykį tarp asmenims suteiktų teisių ir pagrįstų jų ribojimo pagrindų tiesiogiai atsispindi ir Europos Sąjungos Pagrindinių Teisių chartijoje, kurioje nustatyta, kad „Bet koks šios Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės. Remiantis proporcingumo principu, apribojimai galimi tik tuo atveju,

---

396 Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", *supra note,* 7: 107 p.

397 Žr. pvz., „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt." *", supra note,* 202, „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", *supra note,* 7, „Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas byloje Nr. C-203/15 ir C-698/15 Tele2 Sverige*",* InfoCuria, ***žiūrėta 2021 m. rugpjūčio 2 d.,*** https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3643172, t.t.

398 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II")", *supra note,* 8: 176 p.

399 Nicholas Emiliou, *The Principle of Proportionality in European Law: A Comparative Study* (London: Kluwer Law International, 1996).

400 Takis Tridimas, *The General Principles of EU Law, 2nd ed.*, (Oxford: Oxford University Press, 2006), 136.

401 Pvz., „Europos Sąjungos Teisingumo Teismo 1970 m. gruodžio 17 d. sprendimas byloje Nr. C-11-70 Internationale Handelsgesellschaft*"*, InfoCuria, žiūrėta 2021 m. rugpjūčio 11 d., https://curia.europa.eu/juris/showPdf.jsf?text=&docid=88063&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3644321, „Europos Sąjungos Teisingumo Teismo 1990 m. lapkričio 13 d. sprendimas byloje Nr. C-331/88 FEDESA*",* InfoCuria*,* žiūrėta 2021 m. rugpjūčio 11 d., https://curia.europa.eu/juris/showPdf.jsf?text=&docid=88063&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3644321.

kai jie būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti“[402].

Proporcingumo principo taikymo ypatybės pagrindinių žmogaus teisių ribojimų teisėtumo atžvilgiu geriausiai atsispindi Europos Sąjungos Teisingumo Teismo praktikoje, suformuotoje būtent teisės į privatumą atžvilgiu. Teisės į privatumą užtikrinimo vertinimui aktualios Direktyvos 95/46/EB ir BDAR preambulių 10 p. nuostatos, kurios nurodo, kad šiais teisės aktais buvo (Direktyvos 95/46/EB atveju) ir yra siekiama užtikrinti aukšto lygio fizinių asmenų duomenų apsaugą, kuri turėtų būti užtikrinama tvarkant asmens duomenis visose valstybėse narėse. Šis aukšto apsaugos lygio siekis netiesiogiai atsispindi ir Europos Sąjungos Pagrindinių Teisių chartijoje, kurios 8 str. įtvirtinama teisė į asmens duomenų apsaugą, kuri traktuojama kaip savarankiška teisė, lyginant su bendrąja teise į privatų ir šeimos gyvenimą[403].

Europos Sąjungos Teisingumo Teismas, vertindamas teisės į duomenų apsaugą ribojimų proporcingumą, eilėje savo sprendimų užėmė griežtą poziciją dėl būtinumo sąlygos taikymo egzistavimo. Vienas geriausių Europos Sąjungos Teisingumo Teismo proporcingumo principo taikymo asmens duomenų apsaugos atžvilgiu pavyzdžių yra sprendimas *Satamedia* byloje[404]. Šioje byloje kilo klausimas dėl Suomijos regioniniuose leidiniuose pateikiamų 1,2 milijonų fizinių asmenų, kurių pajamos yra didesnės nei nustatytas dydis, vardai bei pavardės, kapitalo pajamos, darbo pajamos ir informacija apie jų turto mokesčius 100 eurų tikslumu[405]. Pagrindinis Europos Sąjungos Teisingumo Teismo nagrinėtas klausimas buvo susijęs su tinkamos pusiausvyros nustatymu tarp, viena vertus, teisės į privatumą ir, kita vertus, teisės į saviraiškos laisvę. Šios bylos sprendimui aktualiame Direktyvos 95/46/EB 9 str. buvo nustatyta, kad asmenų teisės pagal šios direktyvos IV bei VI skyrius gali būti apribotos, kai „asmens duomenys tvarkomi tik žurnalistiniais sumetimais arba meninės ar literatūrinės raiškos tikslais, bet tiktai tuomet, jeigu šios išimtys reikalingos, norint privatumo teisę suderinti su laisve reikšti savo mintis ir įsitikinimus reglamentuojančiomis taisyklėmis“. Aiškindamas balansą tarp šių konkuruojančių teisių, Europos Sąjungos Teisingumo Teismas nurodė, kad „Siekiant atsižvelgti į saviraiškos laisvės svarbą visai demokratinei bendruomenei

---

402 „Europos Sąjungos pagrindinių teisių chartija“, *supra note*, 51: 52 str. 1 d.

403 „Europos Sąjungos pagrindinių teisių chartija“, *supra note*, 51: 8 str.

404 „Europos Sąjungos Teisingumo Teismo 2008 m. gruodžio 16 d. sprendimas byloje Nr. C-73/07 Satamedia“, InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=76075&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=1629974.

405 *Ibid*, 26 p.

reikia, pirma, su ja susijusias sąvokas, įskaitant žurnalistiką, aiškinti plačiai. Antra, siekiant subalansuotos šių dviejų pagrindinių teisių pusiausvyros, pagrindinės teisės į privatų gyvenimą apsauga reikalauja, kad nuo pirmiau nurodytų direktyvos skirsniuose numatytų duomenų apsaugos nukrypstančios nuostatos ir apribojimai griežtai atitiktų būtinumo sąlygą“[406].

Europos teisės mokslininkų vertinimu, tokiu būdu Europos Sąjungos Teisingumo Teismas būtent šioje byloje pirmąsyk kvalifikavo teisėtų išimčių iš teisės į asmens duomenų apsaugą privalomumo, taikydamas „griežto būtinumo“ (angl. *strict necessity*) sąlygą[407]. Tokia pozicija buvo detalizuota tolimesnėje Europos Sąjungos Teisingumo Teismo praktikoje. Pavyzdžiui, *Schecke ir Eifert* byloje taip pat buvo nagrinėjamas klausimas dėl duomenų paskelbimo teisėtumo. Federalinės žemės ūkio ir mitybos tarnybos interneto svetainėje (kurioje buvo galima paieška), remiantis imperatyviu Europos Sąjungos reglamento reguliavimu[408], buvo viešai skelbiami paramos gavėjų pagal konkrečias programas asmenvardžiai, gyvenamoji arba įsteigimo vieta su pašto kodu ir gautos metinės išmokos dydis[409]. Europos Sąjungos Teisingumo Teismas, visų pirma konstatavo, kad asmens duomenų paskelbimas interneto tinklalapyje laikytinas teisės į privatumą ir asmens duomenų apsaugą ribojimu, todėl toliau sprendė ar toks teisių ribojimas gali būti laikomas proporcingu. Taikydamas „griežto būtinumo“ testą, suformuotą jau minėtoje *Satamedia* byloje, Europos Sąjungos Teisingumo Teismas konstatavo, kad toks teisinis reguliavimas, kuriuo yra leidžiamas asmenų, gaunančių paramą, duomenų skelbimas interneto tinklalapyje, neproporcingai pažeidžia asmenų teises į privatumą ir duomenų apsaugą, nes „galima įsivaizduoti mažiau minėtą fizinių asmenų pagrindinę teisę apribojančias, tačiau leidžiančias veiksmingai pasiekti Sąjungos teisės aktų tikslus, priemones“[410]. Taigi, Europos Taryba ir Europos Komisija, priėmusios reglamentus,

406 *Ibid*, 56 p.

407 Tranberg, *supra note,* 416: 239, 245

408 „2005 m. birželio 21 d. Tarybos reglamentas (EB) Nr. 1290/2005 dėl bendrosios žemės ūkio politikos finansavimo su pakeitimais, padarytais 2007 m. lapkričio 26 d.Tarybos reglamentu (EB) Nr. 1437/2007, 42 straipsnio“ 8b p., 44a str., EUR-lex, žiūrėta 2021 m. rugpjūčio 11 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32007R1437; „2008 m. kovo 18 d. Komisijos reglamentas (EB) Nr. 259/2008, kuriuo nustatomos išsamios Reglamento Nr. 1290/2005 nuostatų dėl informacijos apie Europos žemės ūkio garantijų fondo ir Europos žemės ūkio fondo kaimo plėtrai paramos gavėjus skelbimo taikymo taisyklės“, EUR-lex, žiūrėta 2021 m. rugpjūčio 11 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32008R0259.

409 „Europos Sąjungos Teisingumo Teismo 2009 m. lapkričio 9 d. sprendimas sujungtose bylose Nr. C-92 ir C-93/09 Schecke ir Eifert*“*, 26 p., InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=125512.

410 *Ibid*, 86 p.

kuriuose buvo įtvirtintos pareigos skelbti paramą gavusių asmenų duomenis interneto tinklalapiuose, nenustatė tinkamos pusiausvyros tarp asmenų teisės į privatų gyvenimą bei duomenų apsaugą ir viešųjų finansų skaidrumo tikslų.

Europos Sąjungos Teisingumo Teismo praktikoje proporcingumo principas buvo taikomas ir vystomas toliau, sprendžiant ir kitus kylančius ginčus dėl teisės į privatumą ir asmens duomenų apsaugą ribojimų teisėtumo. Todėl toliau pateikiama trumpa Europos Sąjungos Teisingumo Teismo praktikos, kuri autoriaus vertinimu yra reikšmingiausia nustatant proporcingumo principo taikymo subtilybes, analizė.

### 4.3.2. Proporcingumo principo taikymas *Digital Rights Ireland* byloje

*Digital Rights Ireland* byloje Europos Sąjungos Teisingumo Teismas pripažino negaliojančia Direktyvą 2006/24, kuri nustatė pareigą telekomunikacinių paslaugų teikėjams vartotojų ryšių metaduomenis saugoti iki dvejų metų. Kaip ir *Schecke ir Eifert* byloje, pirmiausiai buvo analizuojamas klausimas, ar Direktyva 2006/24 ribojo asmenų teisę į privatumą ir asmens duomenų apsaugą. Teismas nusprendė, kad direktyvoje esantys saugojimo reikalavimai ir teisėsaugos institucijoms suteikiamos prieigos galimybės laikytinos Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių apribojimais, kurie yra plataus masto ir laikytini ypač dideliais bei visuomenės nariams galintys sudaryti įspūdį, kad jų privatus gyvenimas yra nuolat stebimas[411].

Europos Sąjungos Teisingumo Teismo vertinimu, duomenų saugojimo pareiga nepažeidė teisės į privatų gyvenimą esmės. Autoriaus vertinimu, tokia išvada galėjo būti daroma atsižvelgiant į tai, kad telekomunikacinių paslaugų teikėjai turėjo saugoti metaduomenis, bet ne patį susižinojimą (t. y. paslaugų vartotojų generuojamą turinį). Tačiau teismas tokią išvadą padarė nurodydamas, kad „Direktyvos 2006/24 7 straipsnyje numatyta su duomenų apsauga ir saugumu susijusi taisyklė, pagal kurią, nepažeidžiant nuostatų, priimtų taikant direktyvas 95/46 ir 2002/58, viešai prieinamų elektroninių ryšių paslaugų arba viešojo ryšių tinklo teikėjai turi laikytis tam tikrų duomenų apsaugos ir saugumo principų, kuriais valstybės narės užtikrina, kad būtų imtasi tinkamų techninių ir organizacinių priemonių, kad duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, atsitiktinio praradimo ar pakeitimo“[412]. Kokios tos

---

411 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 37 p.

412 *Ibid*, 40 p.

„tinkamos techninės ir organizacinės priemonės“, kurių turi būti imtasi ir kurios galėtų duomenis „apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, atsitiktinio praradimo ar pakeitimo“ ne tik nėra detalizuota, tačiau ir neaišku, kaip jų taikymas galėjo būti aktualus bylos nagrinėjimo atveju, nes teisėsaugos ir žvalgybos institucijos turėjo teisinį pagrindą prieigai prie telekomunikacinių paslaugų teikėjų saugomų metaduomenų bei neturėjo jokio intereso jų naikinti ar pakeisti, o greičiau – priešingai (užtikrinti jų integralumą ir patikimumą).

Taigi, nors Europos Sąjungos Teisingumo Teismo vertinimu, duomenų saugojimo pareiga ir nepažeidė teisės į privatų gyvenimą esmės, o terorizmo ir nusikalstamumo prevencija yra teisėti bendrojo gėrio tikslai, pagrindinis bylos klausimas tapo, ar šie neesminiai teisės į privatumą ir asmens duomenų apsaugą pažeidimai yra proporcingi. Teismas pažymėjo, kad jo vertintų Direktyvos 2006/24 nuostatų proporcingumas turi būti vertinamas atsižvelgiant į tai, jog ribojamos teisės yra pagrindinės asmens teisės, todėl Europos Sąjungos teisės aktų leidėjo vertinimo diskrecija Europos Sąjungos Teisingumo Teismo gali būti apribota pagal kelis kriterijus, įskaitant, be kita ko, atitinkamą sritį, Europos Sąjnugos Pagrindinių Teisių Chartija užtikrintos atitinkamos teisės pobūdį, apribojimo pobūdį, mastą ir tikslą[413]. Todėl šios bylos atveju, atsižvelgiant į asmens duomenų apsaugos svarbą pagrindinei teisei į privataus gyvenimo gerbimą ir į šios teisės apribojimo, kurį lemia Direktyva 2006/24, mastą, teismas sprendė, kad Europos Sąjungos teisės aktų leidėjo vertinimo diskrecija yra nedidelė, todėl būtina taikyti griežtą kontrolę.

Taikant šią griežtą Europos Sąjungos teisės aktų leidėjo vertinimo diskrecijos kontrolę, svarbu atsižvelgti į ankstesnę Europos Sąjungos Teisingumo Teismo praktiką, kad teisės į privatumą apsauga bet kuriuo atveju reikalauja, kad nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neviršytų to, kas yra griežtai būtina[414].

Šiuo atveju, kadangi Direktyvos 2006/24 3 str. įtvirtinta pareiga saugoti metaduomenis buvo taikoma itin plačiai (visoms bendravimo formoms, pvz. tiek judriojo ryšio, tiek interneto prieigos paslaugų atvejais) ir visų paslaugų naudotojų atžvilgiu, net ir nesant jokio (net ir netiesioginio) ryšio su nusikaltimais ar grėsme nacionaliniam saugumui, Direktyvos 2006/24 nuostatos ribojo teisę į privatumą ir

---

413 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 47 p.

414 „Europos Sąjungos Teisingumo Teismo 2013 m. lapkričio 7 d. sprendimas byloje Nr. C-473/12 IPI“, 39 p., InfoCuria, **žiūrėta 2021 m. rugpjūčio 2 d.,** https://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=1751136.

duomenų apsauga viršijant tai, kas yra griežtai būtina[415]. Taigi, atsižvelgdamas į Direktyvos 2006/24 nepagrįstai platų taikymą (pvz., taikymą asmenų, kurių padėtis nesudaro net netiesioginio pagrindo inicijuoti baudžiamąjį persekiojimą arba asmenų, kurių komunikacija pagal nacionalinę teisę pripažįstama profesine paslaptimi, atžvilgiu[416]), tinkamų saugiklių trūkumą (pvz., saugomi tik tie duomenys, kurie susiję su tam tikru laikotarpiu ir (arba) nustatyta geografine zona, ir (arba) tam tikrų asmenų, kurie, vienaip ar kitaip, galėtų būti siejami su vienu iš sunkių nusikaltimų, ratu arba asmenimis, kurių duomenų saugojimas galėtų būti naudingas sunkių pažeidimų prevencijai[417]), Europos Sąjungos Teisingumo Teismas konstatavo, kad ji sudaro plataus masto ir ypač didelį šių pagrindinių teisių apribojimą, kuris nėra tiksliai reglamentuotas nuostatomis, leidžiančiomis užtikrinti, kad jis iš tiesų neviršija to, kas yra griežtai būtina[418].

Kaip rodo paminėti Europos Sąjungos Teisingumo Teismo praktikos pavyzdžiai dėl asmens teisės į privatumą ir duomenų apsaugą ribojimų, teismas užima griežtą šių teisių gynimo poziciją, vertindamas jų ribojimo proporcingumą ir ypač daug dėmesio skiria ribojimų „griežtos būtinybės“ pagrindimui. Teisės mokslininkų vertinimu, tokia griežta Europos Sąjungos Teisingumo Teismo pozicija ir itin gili teisių apribojimų analizė savotiškai lemia mažesnę pagarbą Europos Sąjungos teisės aktų leidėjų iniciatyvoms bei priimtiems teisės aktams[419]. Autoriaus vertinimu, tokia išvada turi būti laikoma pagrįsta, nes beveik visa pastarojo dešimtmečio Europos Sąjungos Teisingumo Teismo praktika, vertinant teisės į privatumą ir asmens duomenų apsaugą ribojimų (ne)pagrįstumą, lėmė Europos Sąjungos teisės aktų panaikinimus – sprendimu *Digital Rights Ireland* byloje buvo panaikinta Direktyva 2006/24, sprendimu *Schrems* byloje – *Safe Harbour* susitarimas, byloje *Schrems II – Privacy Shield* susitarimas.

Papildant aukščiau nurodytą aplinkybę dėl ryžtingos Europos Sąjungos Teisingumo Teismo praktikos metamo šešėlio Europos Sąjungos teisės aktų leidėjų iniciatyvoms, teismo kuriamos proporcingumo principo taikymo subtilybės, autoriaus vertinimu, yra kvescionuotinos. Pavyzdžiui, nėra aišku ar toks aukštas teisių pažeidimo masto tyrimo lygis taikytinas visoms Europos Sąjungos pagrindinių teisių chartijos teisėms, ar tik teisei į privatumą. Kiti mokslininkai užima radikalesnę poziciją, nurodydami,

---

415 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 58 p.

416 *Ibid*, 59 p.

417 *Ibid.*

418 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“, *supra note,* 202: 65 p.

419 Granger ir Irion, *supra note,* 214: 835, 845

kad griežtas tikrinimo lygis apsiriboja teisėmis į nediskriminavimą, tinkamą procesą, nuosavybę, privatumą bei duomenų privatumą[420]. Nors Europos Sąjungos Teisingumo Teismas ir neišryškino jokios pagrindinių teisių hierarchijos, atsižvelgiant į minėtus sprendimus *Tele2 Sverige*, *Digital Rights Ireland*, *Schrems*, *Schrems II* bylose, akivaizdu, kad teisei į privatumą ir asmens duomenų apsauga taikoma ypatingai aukšta apsaugos kartelė.

Antra, įdomu kokia yra priklausomybė tarp pagrindinėms teisėms taikomų ribojimų ir Europos Sąjungos Teisingumo Teismo atliekamo jų proporcingumo vertinimo skrupulingumo. Nors iš Europos Sąjungos Teisingumo Teismo praktikos galima daryti išvadą, kad kuo pagrindinių teisių ribojimai yra reikšmingesni (paneigiantys konkrečių teisių esmę), tuo labiau tikėtina išvada, kad jie bus pripažįstami neteisėtais, tačiau paties teismo atliekamos analizės mastą ar jos detalumą nuspėti yra sunku. Pavyzdžiui, nors *Digital Rights Ireland* ir *Tele2 Sverige* bylose buvo nagrinėjami klausimai dėl elektroninių ryšių paslaugų vartotojų metaduomenų (o ne prieigos prie paties susižinojimo turinio) saugojimo teisėtumo, Europos Sąjungos Teisingumo Teismas vis tiek konstatavo esminį teisės į privatumą ir asmens duomenų apsaugą pažeidimą. Todėl nėra aišku, kokius pagrindinių teisių ribojimo atvejus Europos Sąjungos Teisingumo Teismas traktuotų ne tokiais „esminiais“ ar vertais mažiau „griežtos kontrolės“.

Trečia, *Digital Rights Ireland* byloje pateiktais motyvais Europos Sąjungos Teisingumo Teismas pademonstravo proporcingumo principo taikymo lankstumą, kuris pasireiškė galimybe atsižvelgti į aibę skirtingų aplinkybių, identifikuojančių teisės į privatumą ir asmens duomenų apsaugą, ribojimų teisėtumą. Spręsdamas pagrindinį klausimą šioje byloje, Europos Sąjungos Teisingumo Teismas ir taikė proporcingumo principą, kurio taikymo savotiškas „standartas“ yra suformuotas ilgametėje Europos Sąjungos Teisingumo Teismo praktikoje. Todėl manytina, kad šio principo taikymas nagrinėjamiems teisės klausimams turi būti tapęs metodišku ir nuspėjamu. Tačiau, deja, tokia išvada negali būti daroma, nes Europos Sąjungos Teisingumo Teismo išaiškinimai šioje byloje yra tokie kazuistiški (remiasi išimtinai šios bylos aplinkybėmis) ir mažai apibendrinti, kad net negali daroma vienareikšmiška išvada, ar masinis (neatrankinis) metaduomenų saugojimas apskritai gali būti proporcingas teisės į privatumą ir asmens duomenų apsaugą atžvilgiu.

Pabrėžtina, kad šią mintį patvirtina aplinkybė, kad praėjus porai metų po sprendimo *Digital Rights Ireland* byloje priėmimo, Europos Sąjungos Teisingumo Teismas

[420] *Ibid*, 835, 846

nagrinėjo *Tele2 Sverige* bylą, kurioje vėl buvo keliamas klausimas dėl nediferencijuoto elektroninių ryšių duomenų saugojimo proporcingumo[421]. Išanalizavus šias esmines proporcingumo principo taikymo *Digital Rights Ireland* byloje aplinkybes, reikia pereiti prie sudėtingesnio proporcingumo principo taikymo atvejo - Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje[422].

### 4.3.3. Proporcingumo principo taikymas *Schrems* byloje

Nors paviršutiniškai išanalizavus Europos Sąjungos Teisingumo Teismo sprendimą *Schrems* byloje, gali pasirodyti, kad jo esmę sudaro Direktyvos 95/46 26 str. 6 d. analizė ir *Safe Harbour* susitarimo teikiamo apsaugos lygio adekvatumo vertinimas, autoriaus vertinimu, šio sprendimo *ratio decidendi* išties apima trečios šalies taikomų sekimo priemonių proporcingumo nustatymą, kuriame teismas remiasi ankstesnių teismo sprendimų apie teisės į privatumą ir duomenų apsaugą ribojimų proporcingumą išaiškinimais bei analizuoja galimų teisių ribojimų teisėtumą atsižvelgdamas į jų „griežtą būtinumą".

Tokia išvada gali būti daroma remiantis Europos Sąjungos Teisingumo Teismo išaiškinimais, kad aukštas asmens teisės į privatumą apsaugos lygis reiškia, kad adekvati šios teisės apsauga trečiojoje šalyje turi būti suprantama kaip iš esmės tokia pati apsauga, kokia garantuojama Europos Sąjungoje[423]. Todėl proporcingumo principas reikalauja Europos Sąjungos teisinio reguliavimo standartus taikyti trečiajai šaliai iš esmės taip pat, kaip jie taikomi Europos Sąjungos valstybėse narėse.

Nors autoriaus vertinimu, Europos Sąjungos Teisingumo Teismo sprendimas *Schrems* byloje pagrįstas proporcingumo principo taikymu, pačiame sprendimo tekste tai tiesiogiai neatsispindi. Siekiant suprasti proporcingumo principo įtaką šios bylos sprendimui, reikalinga įsigilinti į generalinio advokato išvadą šioje byloje bei šiame dokumente apibūdintą platesnį kontekstą.

Pirma, generalinis advokatas, atsižvelgdamas Europos Sąjungos Teisingumo Teismo sprendimo *Digital Rights Ireland* byloje motyvus, nurodė, kad atsižvelgiant į didelį vartotojų skaičių ir perduodamų duomenų kiekį bei JAV institucijų turimą ne-

---

421 „Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas byloje Nr. C-203/15 ir C-698/15 Tele2 Sverige", *supra note,* 419.

422 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems*"*, *supra note,* 7.

423 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems*"*, *supra note,* 7: 74 p.

ribotą prieigą prie šių duomenų, toks teisės į privatumą ribojimas yra „plataus taikymo ir turi būti laikomas labai dideliu“[424]. Tuomet generalinis advokatas nustatė, kad kadangi JAV vykdoma PRISM programa suteikia prieigą prie vartotojų perduodamų duomenų turinio, toks teisės į privatumą ribojimas „pažeidžia pagrindinės teisės į asmens duomenų apsaugą esmę“[425]. Galiausiai, generalinis advokatas taikė „griežto būtinumo“ testo sąlygas, suformuotas *Digital Rights Ireland* byloje ir padarė išvadą, kad JAV institucijoms prieinamos masinio ir netikslinio sekimo priemonės yra iš esmės neproporcingos ir reiškia nepateisinamą teisių į privatumą ir asmens duomenų apsaugą ribojimą, atsižvelgdamas ne tik į turimą neribotą prieigą prie perduodamų duomenų, bet ir tai, kad teisė JAV institucijoms prieiti prie perduodamų duomenų yra suformuota bendrai ir neapribota tuo, kas griežtai būtina[426].

Be pristatyto teisės į privatumą ir asmens duomenų apsaugą pažeidimo neproporcingumo (dėl neribotos JAV institucijų prieigos prie perduodamų asmens duomenų), neigiamam Europos Sąjungos Teisingumo Teismo *Safe Harbour* susitarimo vertinimui ne mažesnę įtaką padarė ir administracinių ar teisminių teisių gynimo priemonių trūkumas Europos Sąjungos piliečių atžvilgiu. Europos Sąjungos Teisingumo Teismo praktikoje[427] ir doktrinoje[428] pripažįstama, kad teisės ribojimo proporcingumo vertinimas gali priklausyti nuo procedūrinių apsaugos priemonių egzistavimo, kurios juos (teisių ribojimus) gali pateisinti ir, kitu atveju, net itin reikšmingu kvalifikuojamą teisės ribojimą. Tačiau *Safe Harbour* susitarimo atveju, teismas pritarė generalinio advokato analizei, kad privataus arbitražo mechanizmai ir procedūros Federalinėje prekybos komisijoje (angl. *Federal Trade Commission*, FTC), apriboti komercinio pobūdžio ginčais, todėl kontrolė kaip JAV subjektai laikosi *Safe Harbour* susitarimo principų, negali būti įgyvendinama nagrinėjant ginčus dėl pagrindinių teisių apribojimų, kuriuos lemia valstybinio pobūdžio priemonės, teisėtumo[429]. Taigi, Europos Sąjungos Teisingumo Teismo vertinimu, Europos Sąjungos vartotojams nebuvo prieinamos jo-

[424] „Generalinio advokato Y. Bot išvada, pateikta 2015 m. rugsėjo 23 d. byloje Nr. C-362/14 Schrems“, *supra note,* 229: 171 p.

[425] *Ibid,* 177 p.

[426] „Generalinio advokato Y. Bot išvada, pateikta 2015 m. rugsėjo 23 d. byloje Nr. C-362/14 Schrems“, *supra note,* 229: 168, 200 p.

[427] „Europos Sąjungos Teisingumo Teismo 2005 m. liepos 12 d. sprendimas sujungtose bylose Nr. C-154/04 ir C-155/04 Nutri-Link “, InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=60405&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2089461.

[428] Sauter, *supra note,* 216: 14

[429] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note*, 7: 89 p.

kios jų teisių gynimo priemonės dėl jų pagrindinių teisių pažeidimų, kildinamų iš JAV subjektų veiksmų ar neveikimo.

Todėl, autoriaus vertinimu, daugeliu atžvilgiu, Europos Sąjungos Teisingumo Teismo sprendimas *Schrems* byloje pagrįstas proporcingumo principo taikymu asmens teisės į privatumą ir duomenų apsaugą ribojimų atžvilgiu, ypač tai, kaip jis buvo aiškintas *Digital Rights Ireland* byloje. Taikant šiuos išaiškinimus, *Safe Harbour* susitarime numatyti teisės į privatumą ir duomenų apsaugą ribojimai akivaizdžiai netenkino „griežto būtinumo" sąlygų, o šį vertinimą tik sustiprino ir efektyvių procedūrinių apsaugos priemonių gynimo nebuvimas, todėl *Safe Harbour* susitarimas pripažintas neproporcingai pažeidžiančiu pagrindines teises (į privatumą ir asmens duomenų apsaugą) ir negaliojančiu.

Skirtingai nuo *Digital Rights Ireland* bylos, *Schrems* bylos atveju teismas atkreipė dėmesį į tai, kad prie teisės į privatumą ir asmens duomenų apsaugą ribojimo neproporcingumo reikšmingai prisidėjo ta aplinkybė, kad JAV teisėsaugos ir žvalgybos institucijoms buvo suteikiama prieiga prie vartotojų duomenų turinio, o ne tik metaduomenų. Tačiau be šios aplinkybės, Europos Sąjungos Teisingumo Teismo sprendimas *Schrems* byloje nesuteikė reikšmingų atsakymų prognozuojant teisės į privatumą ir asmens duomenų apsaugą ribojimų ribas. Jau iš sprendimo *Digital Rights Ireland* byloje buvo aišku, kad net visuotinis ir neindividualizuotas metaduomenų kaupimas laikytinas neproporcingu teisės į privatumą ir asmens duomenų apsaugą pažeidimu, todėl sprendimas *Schrems* byloje neturėjo būti netikėtas. Tačiau Europos Sąjungos Teisingumo Teismo ir priėmus sprendimą *Schrems* byloje, liko neaišku, ar tokio pobūdžio (t. y. itin reikšmingi) teisės į privatumą ir asmens duomenų apsaugą ribojimai apskritai galėtų būti laikomi proporcingais, pavyzdžiui, jei duomenų subjektams būtų numatytos efektyvios procedūrinės teisių gynimo priemonės, ar kitais atvejais. Todėl, autoriaus vertinimu, Europos Sąjungos Teisingumo Teismo išaiškinimai šioje byloje taip pat laikytini kazuistiškais (remiasi išimtinai šios bylos aplinkybėmis) ir mažai apibendrintais, kad galėtų būti naudingi mėginant nustatyti jei ne praktines, tai bent teorines proporcingumo principo taikymo ribas asmens teisės į privatumą ir asmens duomenų apsaugą atžvilgiu.

### 4.3.4. Proporcingumo principo taikymas *Schrems II* byloje

Teisės mokslininkams ir praktikams, kurie analizavo Europos Sąjungos Teisingumo Teismo sprendimą *Schrems* byloje, teismo atliktas *Privacy Shield* susitarimo ver-

tinimas *Schrems II* byloje (kuria *Privacy Shield* susitarimas buvo panaikintas) neturėjo būti staigmena. Autoriaus vertinimu, *Privacy Shield* susitarimas buvo panaikintas dėl tų pačių priežasčių, kaip ir *Safe Harbour* susitarimas, panaikintas ankstesniu sprendimu *Schrems* byloje.

Europos Sąjungos Teisingumo Teismo sprendimą *Schrems II* byloje proporcingumo principo taikymas yra glaustas, tačiau, neabejotinai, išsamesnis nei anksčiau analizuotu *Schrems* bylos atveju. Nagrinėjamame sprendime *Schrems II* byloje, teismas nurodė, kad tam, kad būtų užtikrintas proporcingumo principas, pačiame teisiniame pagrinde, kuriuo leidžiami pagrindinių teisių suvaržymai, turi būti apibrėžta atitinkamos teisės įgyvendinimo ribojimo apimtis ir numatytos aiškios, tikslios taisyklės, kuriomis būtų reglamentuojama atitinkamos priemonės apimtis ir taikymas bei nustatomi minimalūs reikalavimai[430].

Autoriaus vertinimu, Europos Sąjungos Teisingumo Teismo motyvaciją dėl proporcingumo principo taikymo *Schrems II* byloje, galima skirstyti atsižvelgiant į anksčiau analizuotos pirmosios *Schrems* bylos atvejį. T. y. ir nagrinėjamoje byloje proporcingumo teismas principą taikė keliems savarankiškiems teisės į privatumą ir duomenų apsaugą ribojimo aspektams – pirma, duomenų subjektų teisių pažeidimo turinio atžvilgiu ir, antra, procedūrinių garantijų Europos Sąjungos duomenų subjektams atžvilgiu.

Pirmuoju aspektu, Europos Sąjungos Teisingumo Teismas pirmiausia konstatavo, kad JAV nacionalinis saugumas, viešasis interesas, o teisėsaugos interesai turi viršenybę ir gali riboti pagrindines Europos Sąjungos subjektų teises (t. y. jas pažeisti), tačiau JAV teisės aktai nėra pakankamai apibrėžti, kad Europos Sąjungos subjektų privatumo apsauga būtų iš esmės lygiavertė tai kuriuos užtikrinta Europos Sąjungos pagrindinių teisių chartija[431]. Todėl teismas padarė išvadą, kad JAV duomenų apsaugos apribojimai pažeidžia proporcingumo principą, nes JAV vykdomos asmens duomenų rinkimo ir analizės programos (pvz. PRISM, UPSTREAM) nenustato „minimalių apsaugos priemonių“ ir nėra „apribotos tuo, kas griežtai būtina“.

Antruoju aspektu svarbu priminti, kad pagal Europos Sąjungos Teisingumo Teismo praktiką[432] pripažįstama, kad teisės ribojimo proporcingumo vertinimas gali

---

430 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 180 p.

431 *Ibid,* 185 p.

432 „Europos Sąjungos Teisingumo Teismo 2005 m. liepos 12 d. sprendimas sujungtose bylose Nr. C-154/04 ir C-155/04 Nutri-Link“, *supra note,* 449.

priklausyti nuo procedūrinių apsaugos priemonių egzistavimo, kurios juos (teisių ribojimus) gali ir pateisinti. Todėl jei sudarant *Privacy Shield* susitarimą būtų išmoktos *Safe Harbour* susitarimo panaikinimo pamokos (iš Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje), vien tokia aplinkybė galėtų suteikti pagrįstą viltį *Privacy Shield* susitarimo išsaugojimui.

Tačiau nepaisant sprendimo ankstesnėje *Schrems* byloje motyvų, Europos Sąjungos Teisingumo Teismas ir šioje byloje (remdamasis JAV vyriausybės informacija) pripažino, kad duomenų subjektams nesuteikiamos įgyvendinamos teisės, kuriomis jie galėtų remtis teismuose JAV valdžios institucijų atžvilgiu[433]. Be to, *Privacy Shield* susitarime nurodytu ombudsmeno mechanizmu nesuteikiama teisių gynimo priemonė institucijoje, kurioje asmenims, kurių duomenys perduodami į JAV, būtų suteiktos garantijos, iš esmės lygiavertės toms, kurios reikalaujamos Europos Sąjungos Pagrindinių Teisių Chartijos 47 straipsnyje[434].

Pagal Europos Sąjungos Teisingumo Teismo suformuotą jurisprudenciją pats veiksmingos teisminės kontrolės, skirtos Europos Sąjungos teisės nuostatų laikymuisi užtikrinti, egzistavimas neatsiejamas nuo teisinės valstybės egzistavimo – taigi reglamentavimu, nenumatančiu asmeniui jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti, nepaisoma Europos Sąjungos pagrindinių teisių chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės[435]. Tokiu būdu, teismas padarė išvadą, kad *Privacy Shield* susitarimu taikomų teisės į privatumą ir duomenų apsaugą ribojimų neproporcingumas negali būti švelninamas net ir atsižvelgiant į veiksmingas teisių gynimo priemones, nes tokios Europos Sąjungos duomenų subjektams nėra suteikiamos JAV.

Europos Sąjungos Teisingumo Teismo užimta pozicija gali būti lengviau suprantama atsižvelgiant į Europos Sąjungos Teisingumo Teismo prezidento Koen Lenaerts straipsnį. Jame K. Lenaerts paaiškina, kad „pagarba“ pagrindinių teisių esmei yra viena iš šių teisių ribojimo teisėtumo sąlygų. Kai Europos Sąjungos teisės aktuose numatytos teisių ribojimai paneigia konkrečios pagrindinės teisės esmę, toks ribojimas

---

433 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *op. cit.,* 181, 182 p.

434 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 197 p.

435 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7: 95 p. ir nurodyta jurisprudencija.

turi būti laikomas neteisėtu ir atitinkamas teisės aktas – panaikinamas[436]. Atsižvelgdamas į Europos Sąjungos Teisingumo Teismo sprendimą *Schrems* byloje, K. Lenaerts nurodo, kad jo minimas pagrindinės teisės „esmės" konceptas reiškia, kad kiekviena pagrindinė teisė turi kietą branduolį (t. y. „esmę"), garantuojantį kiekvienam asmeniui laisvės sferą, kuri visada turi likti laisva ir, jo vertinimu, šis branduolys yra absoliutus, nes jam negali būti taikomi jokie apribojimai[437].

Atitinkamai, atsižvelgdamas į Europos Sąjungos Teisingumo Teismo sprendimus *Digital Rights Ireland*, *Tele2 Sverige*, *Schrems* bylose, K. Lenaerts nurodo, kad nustačius, kad pagrindinės teisės esmė buvo pažeista, konkreti pagrindinę teisę ribojanti priemonė yra nesuderinama su Europos Sąjungos Pagrindinių Teisių Chartija[438]. Jo vertinimu, tokios aplinkybės (pagrindinės teisės esmės pažeidimo) nustatymas eliminuoja būtinybę taikyti proporcingumo principą ir atlikti konkuruojančių interesų analizę ir teisingo jų balanso paiešką ir, remiantis *Schrems* sprendimu, priemonė, pažeidžianti pagrindinės teisės esmę, automatiškai yra neproporcinga[439].

### 4.3.5. Ar galima išspręsti asmens duomenų perdavimo tarp skirtingų teisinių sistemų problemą netaikant proporcingumo principo?

Aukščiau pateikta Europos Sąjungos Teisingumo Teismo praktikos analizė atskleidžia, kad pagrindinis teisėtumo testas vertinant teisės į privatumą ir asmens duomenų apsaugą ribojimų pagrįstumą yra proporcingumo principo taikymas.

Europos Sąjungos Teisingumo Teismas *Schrems II* byloje atliko *Privacy Shield* susitarimo bei JAV teisėsaugos bei žvalgybos institucijų taikomos asmens duomenų tvarkymo praktikos analizę ir taikė proporcingumo principo reikalavimus. Šios analizės rezultatas yra akivaizdi *Privacy Shield* susitarimo ir JAV taikomų asmens duomenų tvarkymo praktikų neatitiktis Europos Sąjungoje keliamiems itin aukštiems asmens duomenų apsaugos reikalavimams.

Tokia išvada nestebina, kadangi bylose *Digital Rights Ireland* ir *Tele2 Sverige* Europos Sąjungos Teisingumo Teismas jau sprendė, kad net metaduomenų kaupimas ir neribota prieiga prie jų, atliekamas nusikaltimų prevencijos tikslais, neproporcin-

436 Koen Lenaerts, „Limits on Limitations: The Essence of Fundamental Rights in the EU", *German Law Journal* 20, 6 (2019): 779–93, **žiūrėta 2021 m. rugpjūčio 2 d.,** https://www.cambridge.org/core/journals/german-law-journal/article/limits-on-limitations-the-essence-of-fundamental-rights-in-the-eu/3071D1A8FB881031F8E3F6D5799959BD.

437 *Ibid.*

438 „Europos Sąjungos pagrindinių teisių chartija", *supra note,* 51.

439 Lenaerts, *supra note,* 458.

gai pažeidžia teisės į privatumą ir asmens duomenų apsaugą. *Schrems II* bylos atveju, buvo tvarkomi ne metaduomenys, o patys turinio duomenys (t. y. komunikacija tarp elektroninių ryšių paslaugų naudotojų ir kt. jų asmens duomenys), todėl esant rimtesniam teisės į privatumą ir asmens duomenų apsaugą ribojimui nei *Digital Rights Ireland* ir *Tele2 Sverige* bylų atveju, priešingos išvados tikėtis nebuvo pagrįsta. Šiuo atveju asmens duomenų tvarkymas apėmė taip pat ir pačius jautriausius asmens duomenis (o ne, pavyzdžiui, metaduomenis), visi jie buvo prieinami JAV teisėsaugos ir žvalgybos institucijoms (neišskiriant duomenis tų asmenų, kurie gali turėti sąsajų su terorizmu, sunkiais nusikaltimais ar pan.), JAV teisėje nebuvo suteikta efektyvių priemonių apsiginti nuo galimo neteisėto asmens duomenų naudojimo etc.

Remiantis Europos Sąjungos Teisingumo Teismo prezidento K. Lenaerts pozicija, kad kiekviena pagrindinė teisė turi kietą branduolį (t. y. „esmę“), garantuojantį kiekvienam asmeniui laisvės sferą, kuri visada turi likti laisva ir šis branduolys yra absoliutus, nes jam negali būti taikomi jokie apribojimai[440], *Schrems II* bylos aplinkybės, neabejotinai, negalėjo atitikti griežtų proporcingumo principo reikalavimų.

Autoriaus vertinimu, aktualiausia Europos Sąjungos Teisingumo Teismo sprendime byloje *Schrems II* suformuota problema, kelianti didžiausią iššūkį galimiems susitarimams dėl duomenų perdavimo tarp Europos Sąjungos ir JAV – trečiosios šalies taikomų nacionalinį saugumą užtikrinančių priemonių atitikties vertinimo BDAR atžvilgiu taikymas. Dėl to labiausiai tikėtinas problemos dėl teisėto asmens duomenų perdavimo tarp Europos Sąjungos ir JAV, atsižvelgiant nacionalinio saugumo apsaugos poreikį, sprendimas yra susijęs su galimybe netaikyti imperatyvaus BDAR reguliavimo ir, kartu, proporcingumo principo reikalavimų dėl pagrindinių teisių ribojimų pagrįstumo.

Europos Sąjungos Teisingumo Teismo praktikos analizė patvirtina, kad teisinio pagrindo ir taikytinų taisyklių nustatymas duomenų perdavimui tarp Europos Sąjungos ir trečiųjų valstybių, atliekamam nacionalinio saugumo tikslais, nėra paprasta užduotis. Europos Sąjungos Teisingumo Teismas PNR (angl. *Passenger name records*) bylose proporcingumo principo taikymo galimybę sprendė kelissyk. PNR bylos yra susijusios su lėktuvų keleivių asmens duomenų perdavimo į trečiąsias šalis (visų pirma JAV, Kanadą) teisėtumo vertinimu.

Europos Sąjungos Teisingumo Teismas 2006 m. pirmąsyk nagrinėjo ginčą tarp Europos Parlamento ir Europos Sąjungos Tarybos bei Europos Bendrijų Komisijos dėl

[440] Lenaerts, *supra note,* 458.

PNR duomenų perdavimo. Dėl 2001 m. rugsėjo 11 d. įvykdytų teroristinių išpuolių JAV tų pačių metų lapkričio mėnesį priėmė teisės aktus, nustatančius, kad visi oro vežėjai, vykdantys skrydžius į JAV ir iš jų arba per jų teritoriją tranzitu, turi leisti JAV muitinių įstaigoms elektroniniu būdu susipažinti su kompiuterinėse užsakymų ir išvykimo kontrolės sistemose laikomais keleivių duomenimis (PNR duomenys)[441]. Nors Europos Komisija kreipėsi į JAV teigdama, kad PNR duomenų perdavimas prieštarauja Europos Sąjungos teisės aktams, JAV nuo 2003 m. ėmė taikyti sankcijas PNR duomenų neatskleidžiantiems oro vežėjams[442].

Ginčo sprendimo metu galiojo Direktyva 95/46, kurioje buvo įtvirtinta, kad ji netaikoma kai „[...] kai atliekamos tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu (taip pat ir valstybės ekonomine gerove, kai tvarkymo operacija susijusi su valstybės saugumo klausimais) ir su valstybės veiksmais baudžiamosios teisės srityje“[443].

Europos Sąjungos Teisingumo Teismas, atsižvelgdamas į tai, kad PNR duomenys bus naudojami tik užkertant kelią terorizmui ir susijusiems nusikaltimams, kitiems tarpvalstybinio pobūdžio sunkiems nusikaltimams, įskaitant organizuotą nusikalstamumą, slėpimuisi nuo arešto ar įkalinimo už minėtus nusikaltimus bei kovai su jais, nusprendė, kad privačių subjektų – oro vežėjų – vykdomas PNR duomenų perdavimas laikytinas tvarkymo operacija, susijusia su visuomenės saugumu ir su valstybės veiksmais baudžiamosios teisės srityje ir todėl patenka į Direktyvos 95/46 netaikymo išimtį[444].

Taigi, Europos Sąjungos Teisingumo Teismas padarė išvadą, kad PNR duomenų perdavimas iš privačių subjektų (oro linijų) JAV kompetentingoms institucijoms yra asmens duomenų tvarkymo operacija, kuriai Direktyvos 95/46 nuostatos netaikomos ir tokiu būdu *de jure* išvengė proporcingumo principo taikymo asmens duomenų tvarkymo operacijoms, kurios atliekamos trečiųjų šalių institucijų dėl trečiųjų šalių nacionalinio saugumo interesų.

Tokia Europos Sąjungos Teisingumo Teismas pozicija palengvintų galimo tei-

441 „Europos Sąjungos Teisingumo Teismo 2006 m. gegužės 30 d. sprendimas sujungtose bylose Nr. C-317/04 ir C-318/04 PNR byla“, 33 p., InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=145330.

442 *Ibid.*

443 „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“, *supra note,* 198: 3 str. 2 d.

444 Europos Sąjungos Teisingumo Teismo 2006 m. gegužės 30 d. sprendimas sujungtose bylose Nr. C-317/04 ir C-318/04 PNR byla“, supra note, 463: 68 p.

sėto asmens duomenų perdavimo tarp Europos Sąjungos ir JAV teisinio mechanizmo sukūrimą, tačiau svarbu atkreipti dėmesį, kad ji buvo pakeista.

Lietuvos doktrinoje randamos nuomonės, kad remiantis minėta Europos Sąjungos Teisingumo Teismo pozicija, suformuota PNR byloje, patenka į Direktyvos 95/46 netaikymo išimtį[445], tačiau svarbu pabrėžti, kad tokia išvada yra nebeaktuali.

Europos Sąjunga ir Kanada derėjosi dėl susitarimo dėl PNR duomenų perdavimo ir tvarkymo, kuris buvo pasirašytas 2014 metais. Europos Taryba paprašė Europos Parlamento patvirtinti susitarimą, o Europos Parlamentas nusprendė kreiptis į Europos Sąjungos Teisingumo Teismą su prašymu pateikti nuomonę, ar numatytas susitarimas atitinka Europos Sąjungos teisę ir, ypač, nuostatas, susijusias su pagarba asmeniniam gyvenimui ir asmens duomenų apsaugai[446].

Nagrinėdamas Europos Parlamento kreipimąsi, Europos Sąjungos Teisingumo Teismas analizavo Europos Sąjungos ir Kanados susitarimą dėl PNR duomenų perdavimo ir tvarkymo daugeliu aspektu, o ypač – dėl suderinamumo su teise į privatumą ir asmens duomenų apsauga. Europos Sąjungos Teisingumo Teismas išsamiai pasisakė dėl susitarimu atliekamų teisių į privatumą ir asmens duomenų apsaugą ribojimų pagrįstumo, *inter alia* remdamasis ir proporcingumo principu[447]. Europos Sąjungos Teisingumo Teismas pateikė nuomonę, kad teismui pateiktas vertinti susitarimas tarp Europos Sąjungos ir Kanados dėl PNR duomenų perdavimo, negali būti sudarytas, nes jis neužtikrina tinkamos teisės į privatumą ir asmens duomenų apsaugą įgyvendinimo. Šią poziciją teismas užėmė *inter alia* remdamasis ir Direktyvos 95/46 reguliavimu, todėl darytina išvada, kad pamatinė Europos Sąjungos Teisingumo Teismo pozicija dėl Direktyvos 95/46 (ir, atitinkamai, BDAR) pakito lyginant su Europos Sąjungos Teisingumo Teismo sprendimu PNR byloje 2006 metais, kuriuo buvo konstatuota, kad PNR duomenų perdavimas į trečiąją šalį (PNR bylos atveju – JAV) patenka į Direktyvos 95/46 netaikymo išimtį.

Tokią prielaidą patvirtina ir vėlesnis Europos Sąjungos Teisingumo Teismo sprendimas *Schrems II* byloje, kuriuo *Privacy Shield* susitarimas (kartu ir asmens duomenų perdavimo į JAV teisėtumas) buvo vertinamas atsižvelgiant į imperatyvų BDAR

---

445 Stankevičiūtė, *supra note*, 6: 134.

446 „Europos Sąjungos Teisingumo Teismo 2017 m. liepos 26 d. pranešimas spaudai Nr. 84/17“, Curia Europa, **žiūrėta 2021 m. rugpjūčio 2 d.,** https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf.

447 „Europos Sąjungos Teisingumo Teismo 2017 m. liepos 26 d. nuomonė Nr. 1/15“, 119 - 231 p., InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3653149.

reguliavimą bei taikant proporcingumo principą taip pat ir duomenų perdavimo iš Europos Sąjungos į JAV, siejamam su nacionaliniu saugumu, atžvilgiu.

Taigi, Europos Sąjungos Teisingumo Teismo sprendime *Schrems II* byloje bei nuomonėje dėl Europos Sąjungos ir Kanados dėl PNR duomenų perdavimo pateiktais motyvais yra paneigta galimybė netaikyti BDAR duomenų perdavimui tarp Europos Sąjungos ir JAV, kuris atliekamas nacionalinio saugumo tikslais. Tuo tarpu taikant BDAR reguliavimą ir proporcingumo principą (kaip teisinį testą, skirtą patikrinti, ar pagrindinių teisių ribojimai gali būti laikomi teisėtais), *Schrems II* byloje Europos Sąjungos Teisingumo Teismas nustatė, kad asmens duomenų perdavimas tarp Europos Sąjungos ir JAV, numatantis JAV teisėsaugos ir žvalgybos institucijų prieigą prie asmens duomenų, neproporcingai varžo teisę į privatumą ir asmens duomenų apsaugą. Todėl darytina išvada, kad naujas susitarimas dėl asmens duomenų perdavimo tarp Europos Sąjungos ir JAV gali būti pasiekiamas tik tuo atveju, jei Europos Sąjungos Teisingumo Teismas pakeis savo poziciją dėl trečiosios šalies nacionalinio saugumo intereso, kaip galimo BDAR taikymo išimties pagrindo, arba JAV atsisakys teisės įgyvendinti nacionalinio saugumo interesus iš Europos Sąjungos gaunamų duomenų atžvilgiu.

## 4.4. Galimo asmens duomenų perdavimo modelio tarp skirtingų teisinių sistemų kontūrai, atsižvelgiant į *Schrems II* bylos pamokas

Europos Sąjungos Teisingumo Teismui priėmus sprendimą *Schrems II* byloje, pirminė ir teisės doktrinoje labiausiai pastebima reakcija buvo kritinė. Kai kurie mokslininkai kaltino Europos Sąjungos Teisingumo Teismą veidmainiavimu, teigdami, kad JAV prieinamos žvalgybos priemonės ir metodai yra išviešinti labiausiai iš viso pasaulio šalių ir JAV taiko aukštesnės kokybės žvalgybos sankcionavimo modelį, nei kai kurios Europos Sąjungos valstybės narės[448]. Kiti abejojo teismo atlikto vertinimo pagrįstumu, nesutikdami su kai kuriomis padarytomis išvadomis, pavyzdžiui teigdami, kad teismas neatsižvelgė į tai, kad jei kuris nors pagal *Privacy Shield* susitarimą įsteigtam ombudsmenui pateiktas skundas patvirtina JAV įstatymų pažeidimą, neteisėtai surinkti duomenys pašalinami iš JAV vyriausybės duomenų bazių ir iš JAV žvalgybos institucijų ataskaitų[449].

[448] Stewart Baker, „How Can the US Respond to Schrems II?“, *LAWFARE*, **žiūrėta 2021 m. rugpjūčio 2 d.,** https://www.lawfareblog.com/how-can-us-respond-*Schrems*-ii.

[449] „National Security Law - Surveillance - Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield – Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020)“, *supra note,* 253.

Sprendimas *Schrems II* byloje panaikino *Privacy Shield* susitarimą ir įsigaliojo iškart[450]. *Privacy Shield* susitarimo panaikinimo reikšmė buvo didžiulė, nes šį susitarimą kaip asmens duomenų perdavimo teisinį pagrindą naudojo daugiau kaip 3500 verslo subjektų[451]. Todėl teisės doktrinoje iškart prasidėjo diskusijos apie tai, koks bus naujas duomenų perdavimo mechanizmas. Kai kurie mokslininkai siūlė tobulinti JAV žalos atlyginimo mechanizmus, kurie suteiktų asmenims realią teisę teikti skundus dėl jų atžvilgiu taikytų sekimo priemonių[452]. Verslo grupės siekė, kad JAV ir Europos Sąjungos atstovai nedelsiant pradėtų derybas dėl naujo universalaus duomenų perdavimo susitarimo pasiekimo[453]. Kita vertus, Europos vartotojų organizacija (BEUC) išreiškė itin kritišką nuomonę JAV teisinio reguliavimo atžvilgiu, reikalaudami reikšmingų permainų JAV teisinėje sistemoje: „jei JAV nepriims tvirtos ir išsamios duomenų apsaugos sistemos, įskaitant privatumo apsaugos įstatymą federaliniu lygmeniu, joks būsimas Europos Sąjungos ir JAV susitarimas dėl duomenų srautų teisme nebus laikomas pagrįstu“[454].

Taigi, doktrina ir abejose rinkose veikiantys ūkio subjektai nevienareikšmiškai reagavo į sprendimą *Schrems II* byloje. Tačiau nepaisant to, klausimai dėl asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinių pagrindų nustatymas išlieka aktualūs. Remiantis Europos Komisijos pranešimais spaudai, diskusijos dėl naujo susitarimo dėl duomenų perdavimo tarp Europos Sąjungos ir JAV yra pradėtos[455]. Atsižvelgiant į tai, kad Europos Sąjungos Teisingumo Teismui 2015 m. priėmus sprendimą *Schrems* byloje ir panaikinus *Safe Harbour* susitarimą, jį pakeitęs *Privacy Shield* susitarimas buvo priimtas jau 2016 m., galimas *Privacy Shield* pakeisiančio susitarimo projektas gali pasirodyti artimiausiu metu.

Kita vertus, kol naujas teisinis pagrindas universaliam asmens duomenų perda-

450 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note*, 8: 202 p.

451 Šio darbo rengimo metu, *Privacy Shield* kompanijų sąraše vis dar nurodyta 3794 įmonės. Prieiga internete: https://www.privacyshield.gov/list, žiūrėta 2021 m. rugpjūčio 2 d.

452 Kenneth Propp ir Peter Swire, „After Schrems II: A Proposal to Meet the Individual Redress Challenge“, *LAWFARE*, žiūrėta 2021 m. rugpjūčio 2 d., https://www.lawfareblog.com/after-*Schrems*-ii-proposal-meet-individual-redress-challenge.

453 „Bendras industrijos laiškas dėl *Schrems II* sprendimo“, žiūrėta 2021 m. rugpjūčio 2 d., https://www.itic.org/policy/JointIndustryLetter*Schrems*II-30July.pdf.

454 „EU Top Court Sides with Consumer Privacy in EU–US Data Shambles“, BEUC, žiūrėta 2021 m. rugpjūčio 2 d., https://www.beuc.eu/publications/eu-top-court-sides-consumer-privacy-eu-us-data-shambles/html.

455 „Europos teisingumo komisaro Didier Reynders ir JAV prekybos sekretoriaus Wilbur Ross pranešimas spaudai“, Europos Komisija, žiūrėta 2021 m. rugpjūčio 2 d., https://ec.europa.eu/newsroom/just/items/684836.

vimui tarp Europos Sąjungos ir JAV negalioja, o naujasis nėra sudarytas, toliau pateikiami pagrindiniai autoriaus vertinimai dėl aspektų, kuriais jis turėtų pasižymėti.

Prieš pradedant analizuoti galimus naujo universalaus asmens duomenų perdavimo tarp Europos Sąjungos ir JAV kontūrus, autorius siekia atkreipti dėmesį į abejotiną Europos Sąjungos Teisingumo Teismo poziciją dėl teisinio pagrindo, taikytino asmens duomenų perdavimui iš Europos Sąjungos į JAV, iškart po sprendimo *Schrems II* byloje priėmimo.

Europos Sąjungos Teisingumo Teismas paskutiniame bylos motyvaciniame paragrafe pateikė itin reikšmingą nuomonę dėl duomenų perdavimui į JAV taikytino teisinio režimo. Vertindamas, ar reikia atidėti šio sprendimo galiojimo padarinius siekiant išvengti teisės spragos atsiradimo, teismas pažymėjo kad bet kuriuo atveju, atsižvelgiant į BDAR 49 straipsnį, panaikinus *Privacy Shield* susitarimą, negali atsirasti tokia teisės spraga, nes šiame BDAR straipsnyje išsamiai nustatytos sąlygos, kuriomis asmens duomenys gali būti perduodami į trečiąsias šalis nepriėmus sprendimo dėl tinkamumo pagal BDAR 45 straipsnio 3 dalį arba tinkamų apsaugos priemonių pagal BDAR 46 straipsnį[456].

Taigi, iš esmės, Europos Sąjungos Teisingumo Teismas užėmė poziciją, kad panaikinus *Privacy Shield* susitarimą, asmens duomenų perdavimą iš Europos Sąjungos į JAV bus galima įteisinti kitais BDAR įtvirtintais duomenų eksporto į trečiąją šalį modeliais. Primintina, kad autorius šiame darbo 2 skyriuje jau atliko duomenų perdavimo tarp Europos Sąjungos ir JAV teisinių pagrindų, įtvirtintų BDAR, analizę ir padarė išvadą, kad Europos Sąjungos Teisingumo Teismui panaikinus *Privacy Shield* susitarimą dėl to, kad JAV neužtikrina tinkamo asmens duomenų apsaugos lygio, asmens duomenų perdavimas į JAV ir kitais pagrindais yra negalimas, nes bet kuriam asmens duomenų perdavimo į JAV teisiniam pagrindui (t. y. BDAR 45, 46 ar 49 str. įtvirtintiems mechanizmams) yra keliamas tas pats BDAR 44 str. įtvirtintas bendrinis tikslas – neturi būti pakenkta BDAR garantuojamam fizinių asmenų apsaugos lygiui. Taigi, Europos Sąjungos Teisingumo Teismui konstatavus, kad *Privacy Shield* panaikinamas dėl JAV teisinio reguliavimo teikiamo asmens teisės į privatumą ir asmens duomenų apsaugos trūkumų, jie negali būti ištaisyti bet kuriuo kitu BDAR 46 ar 49 str. įtvirtintu duomenų perdavimo mechanizmu, t. y. nepakeitus JAV teisinio reguliavimo.

Todėl, autoriaus vertinimu, analizuoti kitus galimus asmens duomenų perdavi-

[456] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 202 p.

mo tarp Europos Sąjungos ir JAV mechanizmus BDAR 46 ar 49 str. įtvirtintais pagrindais nėra prasminga, nes jie vis tiek negalės atitikti itin aukštos Europos Sąjungos Teisingumo Teismo *Digital Rights Ireland*, *Schrems*, *Schrems II* bylose suformuotos teisės į privatumą ir duomenų apsaugą apsaugos kartelės.

Kaip minėta šiame darbe, Europos Sąjungos Teisingumo Teismas proporcingumo teismas principą taikė keliems savarankiškiems teisės į privatumą ir duomenų apsaugą ribojimo aspektams – pirma, duomenų subjektų teisių pažeidimo turinio atžvilgiu ir, antra, procedūrinių garantijų Europos Sąjungos duomenų subjektams atžvilgiu.

Kalbant apie pirmąjį aspektą – dėl asmens teisės į privatumą ir duomenų apsaugą nepagrįsto ribojimo atsižvelgiant į perduodamą turinį – atkreiptinas dėmesys, kad Europos Sąjungos Teisingumo Teismas jam dėmesio ir reikšmingos teisinės analizės beveik neskyrė. Teismas tiesiog konstatavo, kad pagal JAV teisinį reguliavimą, teisėsaugos ir žvalgybos institucijoms suteikiama prieiga prie į JAV perduodamų duomenų, be aiškiai ir tiksliai nustatytos tokio masinio asmens duomenų rinkimo apimties ribos ir šiai prieigai netaikant jokios teismų kontrolės[457].

Autoriaus vertinimu, tokia motyvacija laikytina nepriimtinai skurdžia ir lemiančia nepakankamą teismo sprendimo aiškumą, nes iš pateiktų motyvų negalima padaryti aiškios išvados, kokios apimties prieigos prie perduodamų duomenų suteikimą Europos Sąjungos Teisingumo Teismas laikytų proporcingu. Ypač lyginant su Europos Sąjungos Teisingumo Teismo nuomone, pateikta dėl Europos Sąjungos ir Kanados susitarimo dėl PNR duomenų, kurioje teismas analizavo kiekvienos perduodamos asmens duomens kategorijos tikslingumą (pvz., ar galimas duomenų perdavimas, priklausančių kategorijoms „turima informacija apie dažnai lėktuvais keliaujančius keleivius ir nuolaidas (nemokamus bilietus, žemesnės klasės bilietų keitimą į aukštesnės klasės bilietus ir pan.)“, „“visa turima kontaktinė informacija (įskaitant rengėjo informaciją)“; „bendroms pastaboms, įskaitant kitą papildomą informaciją (OSI), specialiųjų tarnybų informaciją (SSI) ir specialiųjų tarnybų prašymų (SSR) informaciją“)[458].

Panašaus detalumo analizė, kurią Europos Sąjungos Teisingumo Teismas pateikė nuomonėje dėl PNR susitarimo, būtų ypač naudinga *Schrems II* bylos atveju, Europos Komisijai ir JAV valdžios institucijoms vedant derybas dėl galimo naujo ir tvaraus duomenų perdavimo tarp Europos Sąjungos ir JAV susitarimo (kuris, tikėtina, nebūtų

[457] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 183 p.

[458] „Europos Sąjungos Teisingumo Teismo 2017 m. liepos 26 d. nuomonė Nr. 1/15“, *supra note*, 469: 157, 158, 160 p.

panaikintas Europos Sąjungos Teisingumo Teismo po metų ar kelių nuo jo priėmimo, kaip *Safe Harbour* ar *Privacy Shield* susitarimai).

Kita vertus, jei Europos Sąjungos Teisingumo Teismas *Schrems II* byloje būtų aiškiai (ar imperatyviai) apribojęs duomenų kategorijas, prieiga prie kurių negalėtų būti pateisinama JAV žvalgybos institucijoms net siekiant apginti nacionalinio saugumo interesus, tai galėtų reikšmingai apsunkinti JAV nacionalinio saugumo įgyvendinimą. Atsižvelgiant į tai, kad nacionalinio saugumo samprata nėra apibrėžta nei Europos Sąjungos lygmeniu, nei JAV teisės aktuose ir yra laikoma labai plačia[459], prieigos prie konkrečių asmens duomenų kategorijų paneigimas galėtų užkardyti žvalgybos veiklas išskirtiniais atvejais ir užkirsti kelią apginti nacionalinį saugumą.

Kalbant apie antrąjį aspektą – procedūrinių garantijų Europos Sąjungos duomenų subjektams dėl galimų teisės į privatumą ir asmens duomenų apsaugą pažeidimų – teismo motyvacija buvo žymiai išsamesnė ir iš esmės apėmė visą sprendimo motyvacinę dalį.

Nors, kaip minėta, autoriaus vertinimu, Europos Sąjungos Teisingumo Teismo motyvų lakoniškumas dėl asmens teisės į privatumą ir duomenų apsaugą nepagrįsto ribojimo, atsižvelgiant į perduodamą turinį, yra nepateisinamas, teismo pateikiamų argumentų gausa apie galimas duomenų subjektų procedūrines garantijas ir teisių gynimo būdus yra suprantama atsižvelgiant į ankstesnę Europos Sąjungos Teisingumo Teismo praktiką.

Europos Sąjungos Teisingumo Teismo praktikoje[460] pripažįstama, kad teisės ribojimo proporcingumo vertinimas gali priklausyti nuo procedūrinių apsaugos priemonių egzistavimo, kurios juos (teisių ribojimus) gali ir pateisinti. Todėl, tikėtina, nagrinėjant *Schrems II* bylą, teismas įžvelgė reikšmingai didesnę galimybę, kad ateityje galimame sudaryti susitarime tarp Europos Sąjungos ir JAV bus numatytos efektyvios galimybės Europos Sąjungos duomenų subjektams apginti savo teises JAV teisinėje sistemoje, nei kad šis susitarimas nustatys proporcingus ribojimus dėl teisės į privatumą ir duomenų apsaugos esmės.

Europos Sąjungos Teisingumo Teismas nurodė, kad pats veiksmingos teisminės kontrolės, skirtos Europos Sąjungos teisės nuostatų laikymuisi užtikrinti, egzistavimas neatsiejamas nuo teisinės valstybės egzistavimo ir priminė ankstesnę savo praktiką, kad

---

459 Žr. šio darbo 4.1.2 skirsnį (Nacionalinio saugumo samprata JAV istorijoje ir teisiniame reguliavime).

460 „Europos Sąjungos Teisingumo Teismo 2005 m. liepos 12 d. sprendimas sujungtose bylose Nr. C-154/04 ir C-155/04 Nutri-Link*", supra note,* 449.

reglamentavimu, nenumatančiu asmeniui jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti, nepaisoma Europos Sąjungos pagrindinių teisių chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės[461].

Poziciją, kad JAV užtikrina apsaugos lygį, iš esmės lygiavertį tam, kuris garantuojamas Chartijos 47 straipsnyje, buvo mėginta įrodyti remiantis tuo, kad *Privacy Shield* susitarimo pagrindu įsteigus ombudsmeną buvo pašalintos spragos, kiek tai susiję su asmenų, kurių asmens duomenys perduodami į šią trečiąją šalį, teismine apsauga[462]. Tuo tarpu Europos Sąjungos Teisingumo Teismas ombudsmeno institutą kritikavo dviem aspektais – dėl nepakankamų nepriklausomumo garantijų ir abejonių dėl jo įgaliojimų ir galimų nurodymų privalomumo.

Konkrečiai, teismas nurodė, kad byloje nebuvo pateikta jokių duomenų apie tai, kad ombudsmeno atšaukimui iš pareigų ar jo paskyrimo panaikinimui būtų taikomos ypatingos garantijos ir dėl to gali kilti abejonių dėl ombudsmeno nepriklausomumo nuo vykdomosios valdžios[463]. Taip pat Europos Sąjungos Teisingumo Teismas pritarė generalinio advokato išvadoje nurodytai pozicijai, kad JAV vyriausybės įsipareigojimas, kad žvalgybos tarnybos turės ištaisyti kiekvieną *Privacy Shield* susitarimo ombudsmeno nustatytą taikytinų normų pažeidimą, neleidžia daryti išvados, kad šis ombudsmenas būtų įgaliotas priimti šioms tarnyboms privalomus sprendimus, taip pat nekalbama apie jokias teisines garantijas, kurios būtų siejamos su šiuo įsipareigojimu ir kuriomis galėtų remtis duomenų subjektai[464].

Galiausiai, šiuo aspektu pabrėžtina, kad bylos metu JAV užimta pozicija yra neaiški ir prieštaringa, nes viena vertus jie teigė, kad ombudsmeno nurodyti asmens duomenų apsaugos trūkumai privalės būti ištaisyti, bet tuo pačiu pripažino, kad pagal vieną JAV Prezidento nurodymą (angl. *Executive Order 12333*) nėra jokių teisių gynimo priemonių, todėl būtent su šiuo JAV Prezidento nurodymu susijusi teisminės apsaugos spraga kliudo konstatuoti JAV užtikrinamą apsaugos lygį, iš esmės lygiavertį tam, kuris garantuojamas Europos Sąjungoje[465].

---

461 „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, *supra note,* 7: 95 p.

462 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 190 p.

463 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 195 p.

464 *Ibid*., 196 p.

465 *Ibid,* 196 p., 191 p.

Taigi, atsižvelgiant į Europos Sąjungos Teisingumo Teismo pateiktą kritiką teisių gynimo priemonių nepakankamumui, darytina išvada, kad egzstuoja galimas teorinis modelis, kuris galėtų tenkinti aukštą Europos Sąjungos Teisingumo Teismo formuojamą standartą. Jis turi apimti platesnių įgaliojimų JAV ombudsmenui suteikimą, apimančių nepriklausomumo garantijas ir, ypač, teisę priimti privalomus sprendimus dėl asmens duomenų perdavimo iš Europos Sąjungos į JAV perdavimo pažeidimų, bei teisę duomenų subjektams kreiptis į jį dėl galimų jų teisių pažeidimų.

Nagrinėdamas *Schrems II* bylą, Europos Sąjungos Teisingumo Teismas tikrino ar JAV nacionaliniais teisės aktais arba tarptautiniais įsipareigojimus iš tikrųjų užtikrintų pagrindinių laisvių ir teisių apsaugos lygį, kuris būtų iš esmės lygiavertis tam, kuris garantuojamas Europos Sąjungoje, siejant jį Europos Sąjungos pagrindinių teisių chartija[466]. Turint omenyje, kad tiek remiantis Europos Sąjungos pagrindinių teisių chartija, tiek Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, teisė į privatumą yra saugoma bei nukrypimai nuo abejų teisės aktų yra galimi tik grindžiant proporcingumo principu, autoriaus vertinimu, remiantis analogija ir geręja praktika, suformuota Europos Žmogaus Teisių Teismo sprendimuose dėl pagrįstų teisės į privatumą ribojimų, yra pateisinama remtis ir nagrinėjant *Schrems II* bylos kazusą.

Šiuo aspektu kyla teorinis klausimas, ar šių dviejų teisių apsaugos sistemų (t. y. Europos Sąjungos Pagrindinių Teisių Chartijos bei Europos Žmogaus Teisių Konvencijos) gimininguma savaime reiškia ir jose įtvirtintų teisių suvokimo bei apsaugos ribų tapatumą. Tačiau jis jau yra atsakytas Lietuvos teisės mokslininkų, kurie teigia, kad Europos Sąjungos pagrindinių teisių chartijoje „nurodytų teisių, atitinkančių [Europos Žmogaus Teisių Konvencijos] garantuojamas teises, esmė ir taikymo sritis tokia pat kaip toje konvencijoje nustatyta“, nors tai ir nekliudo Europos Sąjungos teisėje numatyti didesnę apsaugą[467]. Atsižvelgiant į autorių pateikiamus vertinimus, kad „Teisingumo Teismui visada suvokiant, kad būtina visais atvejais įveikti EŽTT nustatytą „minimalaus aukščio apsaugos kartelę““[468], darytina išvada, kad Europos Žmogaus Teisių Teismo praktika bylose dėl teisės į privatumą apsaugos gali būti taikoma ir Europos Sąjungos Teisingumo Teismo praktikoje, nepaneigiant Europos Žmogaus Teisių Teismo suformuoto teisės apsaugos standarto, kaip minimalios apsaugos standarto.

Šiuo atveju tiksliausia analogija gali būti daroma pagal šiame darbe jau anali-

---

466 *Ibid*., 94 p.
467 Žalimienė, *supra note,* 79: 56.
468 *Ibid*, 64 psl.

zuotą Europos Žmogaus Teisių Teismo sprendimą *Dalea prieš Prancuziją* byloje, kurioje buvo nagrinėjamas klausimas dėl asmenims prieinamų teisių gynimo priemonių atvejais, kai teisę į privatumą ribojantys sprendimai yra susiję su nacionaliniu saugumu ir asmeniui konkretaus sprendimo motyvai nėra atskleidžiami. Teismas šioje byloje konstatavo, kad nors pareiškėjui niekada nebuvo suteikta galimybė susipažinti su tiksliais jo atžvilgiu priimto sprendimo motyvais ar juos ginčyti, jam buvo suteikta galimybė susipažinti su visais kitais su juo susijusiais duomenimis ir jis buvo informuotas, kad toks sprendimas priimtas dėl valstybės saugumo, gynybos ir visuomenės saugumo sumetimų[469]. Todėl Europos Žmogaus Teisių Teismas darė išvadą, kad vien ta aplinkybė, jog pareiškėjas negalėjo asmeniškai susipažinti su visa jo prašoma informacija, savaime nepagrindžia, kad kišimasis nebuvo pateisinamas nacionalinio saugumo interesais, nes kompetentinga ir nepriklausoma institucija gali peržiūrėti sprendimo motyvus ir atitinkamus įrodymus, taikydama tam tikrą rungimosi principą[470].

Taigi, taikant analogiją pagal Europos Žmogaus Teisių Teismo sprendimą byloje, kuris suformuotas tiek teisės į privatumą apsaugos kontekste, tiek sprendžiant dėl šios teisės ribojimų proporcingumo efektyvios teisės gynybos priemonių kontekste, darytina išvada, kad tikėtinai Europos Sąjungos Teisingumo Teismui priimtinas efektyvios asmenų teisių pažeidimų apsaugos modelis yra galimas (i) praplečiant nepriklausomo subjekto (pvz., ombudsmeno, kuris buvo numatytas pagal *Privacy Shield* susitarimą) galias ir įgaliojant priimti teisėsaugos ir žvalgybos tarnyboms privalomus sprendimus (įskaitant ir susijusius su JAV Prezidento nurodymu Nr. 12333), (ii) numatant aiškias šio nepriklausomo subjekto nepriklausomumo nuo vykdomosios valdžios garantijas, (iii) įtvirtinant asmenų skundų nagrinėjimo modelį, pasižymintį bent ribotu rungimosi principu, pavyzdžiui, asmeniui neatskleidžiant jo atžvilgiu surinktos informacijos turinio ir apimties, tačiau užtikrinant, kad kompetentingas ir nepriklausomas subjektas galės nešališkai ir pagrįstai išnagrinėti asmens skundą dėl teisėsaugos ar žvalgybos institucijų veiksmų pagrįstumo.

---

469 „Europos Žmogaus Teisių Teismo 2010 m. vasario 2 d. sprendimas byloje Nr. 964/07 Dalea prieš Prancūziją“, *supra note*, 396.

470 *Ibid*.

### 4.4.1. Galimo naujo asmens duomenų perdavimo tarp skirtingų teisinių sistemų kontūrai, atsižvelgiant į Europos Komisijos patvirtintas standartines duomenų apsaugos sąlygas

Kaip analizuota šio darbo 2 skyriuje, BDAR asmens duomenų perdavimui į trečiąsias valstybes arba tarptautinėms organizacijoms reglamentuoti yra skirtas V-asis BDAR skyrius. Šiame BDAR skyriuje yra įtvirtinti keli savarankiški asmens duomenų perdavimo įteisinimo būdai - duomenų perdavimas remiantis sprendimu dėl tinkamumo[471], duomenų perdavimas taikant tinkamas apsaugos priemones[472], kitos asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai sąlygos[473]. Šie asmens duomenų perdavimo pagrindai turi hierarchiją (aukščiausias – 45 str. įtvirtintas Europos Komisijos sprendimas dėl tinkamumo) ir paskesnis asmens duomenų perdavimo teisinis pagrindas gali būti taikomas tik tuomet, kai aukštesnis pagal hierarchiją teisinis pagrindas neegzistuoja.

*Privacy Shield* susitarimas buvo Europos Komisijos sprendimas dėl tinkamumo, t. y. asmens duomenų perdavimo į JAV teisinis pagrindas BDAR 45 str. prasme, kuris Europos Sąjungos Teisingumo Teismo buvo panaikintas sprendimu *Schrems II* byloje. Panaikinus šį teisinį asmens duomenų perdavimo į JAV pagrindą, iškart kilo poreikis naudotis kitais BDAR V skyriuje įtvirtintais duomenų perdavimo pagrindais.

Kaip minėta ankstesnėje darbo dalyje, Europos Sąjungos Teisingumo Teismas sprendime *Schrems II* byloje užėmė poziciją, kad panaikinus *Privacy Shield* susitarimą, asmens duomenų perdavimą iš Europos Sąjungos į JAV bus galima įteisinti kitais BDAR įtvirtintais duomenų eksporto į trečiąją šalį modeliais ir šiuo aspektu tiesiogiai paminėjo standartines duomenų apsaugos sąlygas pagal BDAR 46 str.[474]. Taigi, praėjus metams po sprendimo *Schrems II* byloje priėmimo (t. y. 2021 m. birželį), Europos Komisija pasinaudojo BDAR 46 str. 2 d. c) p. įtvirtinta galimybe ir patvirtino standartines duomenų apsaugos sąlygas.

Šiomis standartinėmis sutarčių sąlygomis užtikrinamos tinkamos tarptautinio duomenų perdavimo duomenų apsaugos priemonės, kurias duomenų eksportuotojas

---

471 „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)“, *supra note,* 60: 45 str.

472 *Ibid*, 46 str.

473 *Ibid*, 49 str.

474 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 202 p.

ir duomenų importuotojas gali nevaržomai įtraukti į platesnę sutartį bei taip pat yra skatinamas įtraukti kitas sąlygas arba papildomas apsaugos priemones, kurios tiesiogiai ar netiesiogiai neprieštarauja standartinėms sutarčių sąlygoms, nepažeidžia duomenų subjektų pagrindinių teisių ar laisvių ar nustato dar griežtesnes apsaugos priemones numatant sutartinius įsipareigojimus[475].

Taigi, Europos Komisijai patvirtinus standartines duomenų apsaugos sąlygas, kuriose yra atsižvelgiama į dalį Europos Sąjungos Teisingumo Teismo išaiškinimų *Schrems II* byloje, aktualu išanalizuoti, kokį galimą (kad ir tarpinį) sprendimą asmens duomenų perdavimui iš Europos Sąjungos į JAV mato Europos Komisija ir ar jis atlaikytų proporcingumo principo testą, Europos Sąjungos Teisingumo Teismo taikytus *Schrems* ir *Schrems II* bylose.

Pirma, dėl pagrindinių teisių ribojimo esmės, autoriaus vertinimu, aktualu remtis Europos Sąjungos Teisingumo Teismo prezidento K. Lenaerts doktrina, kad kiekviena pagrindinė teisė turi kietą branduolį (t. y. „esmę“), garantuojantį kiekvienam asmeniui laisvės sferą, kuri visada turi likti laisva ir šis branduolys yra absoliutus, nes jam negali būti taikomi jokie apribojimai[476]. Atsižvelgiant į šią poziciją, viena esminių problemų pagal *Schrems II* bylą buvo neribota JAV teisėsaugos ir žvalgybos institucijų prieiga prie duomenų[477]. Teisinis pagrindas tokioms JAV teisėsaugos ir žvalgybos institucijų veikloms yra JAV Prezidento nurodymas Nr. 12333 (angl. *Executive order 12333*), kuris vis dar galioja[478]. Taigi, pagrindo daryti išvadai, kad JAV taiko platesnės apimties apsaugą iš Europos Sąjungos gaunamiems asmens duomenims, nei buvo teikiama *Schrems II* bylos nagrinėjimo atveju, nėra.

Taip pat, autoriaus vertinimu neigiamai vertintina aplinkybė, kad Europos Komisijos standartinėse duomenų apsaugos sąlygose yra įtvirtinama deklaratyvi šalių garantija, kad jos „garantuoja, kad neturi pagrindo manyti, jog paskirties trečiosios valstybės įstatymai ir praktika, taikomi duomenų importuotojo atliekamam asmens duomenų tvarkymui, įskaitant bet kokius reikalavimus atskleisti asmens duomenis

---

475 „2021 m. birželio 4 d. Europos Komisijos įgyvendinimo sprendimas dėl standartinių sutarčių sąlygų, kuriomis asmens duomenys perduodami į trečiąsias valstybes pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679“, EUR-lex, žiūrėta 2021 m. rugpjūčio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32021D0914&from=EN.

476 Lenaerts, *supra note,* 458.

477 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *op.cit.,* 183 p.

478 „Nacionalinės žvalgybos direktoriaus biuro teisinių nuorodų knyga (angl. *Legal refference book*)“, **žiūrėta 2021 m. rugpjūčio 2 d.**, https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf.

arba priemones, kuriomis valdžios institucijoms suteikiama prieiga, trukdo duomenų importuotojui vykdyti jo prievoles pagal šias sąlygas. Tai grindžiama nuostata, kad teisės aktai ir praktika, kuriais paisoma pagrindinių teisių ir laisvių esmės ir kuriais neviršijama tai, kas būtina ir proporcinga demokratinėje visuomenėje siekiant apsaugoti vieną iš Reglamento (ES) 2016/679 23 straipsnio 1 dalyje išvardytų tikslų, neprieštarauja standartinėms sutarčių sąlygoms.“[479].

Šiuo atveju galima tik užduoti retorinį klausimą, kaip Europos Sąjungoje veikiantis duomenų eksportuotojas (perduodantis asmens duomenis JAV subjektui), galėtų pagrįsti tokio susitarimo su JAV subjektu teisėtumą šiuo aspektu, ypač atsižvelgiant į tai, kad Europos Sąjungos Teisingumo Teismo sprendime *Schrems II* byloje buvo konstatuota, kad JAV teisės aktai neproporcingai riboja duomenų subjektų teises į privatumą ir asmens duomenų apsaugą, o JAV teisinė bazė (ir žvalgybos bei teisėsaugos institucijų veiklos pagrindai) nepasikeitė.

Antra, analizuojant procedūrines garantijas Europos Sąjungos duomenų subjektams dėl galimų teisės į privatumą ir asmens duomenų apsaugą pažeidimų, primintina, kad Europos Sąjungos Teisingumo Teismo sprendimas *Schrems II* byloje suformavo pamatinę problemą, kad duomenų subjektams nesuteikiamos įgyvendinamos teisės, kuriomis jie galėtų remtis teismuose JAV valdžios institucijų atžvilgiu, t. y. šie asmenys neturi teisės į veiksmingą teisinę gynybą[480], o *Privacy Shield* susitarimo pagrindu sukurtas ombudsmeno institutas negali būti laikomas nepriklausomu ar turinčiu įgaliojimus priimti privalomus sprendimus[481].

Europos Komisija standartinėse duomenų apsaugos sąlygose šią problemą, tikėtina, mėginama spręsti keliais būdais. Susitarimo 15.1 sąlygoje yra įtvirtintas pranešimo apie valdžios institucijų prieigą prie turimų duomenų institutas. Jame yra įtvirtinta duomenų importuotojo (t. y. trečiosios šalies, pvz. JAV subjekto) pareiga informuoti duomenų eksportuotoją (Europos Sąjungos subjektą) ir, jei įmanoma, duomenų subjektą, tuo atveju jei (i) duomenų importuotojas gauna „teisiškai privalomą valdžios institucijos (įskaitant teismines institucijas) prašymą pagal paskirties valstybės teisės aktus atskleisti pagal šias sąlygas perduotus asmens duomenis“ bei (ii) „sužino apie bet

---

479 „2021 m. birželio 4 d. Europos Komisijos įgyvendinimo sprendimas dėl standartinių sutarčių sąlygų, kuriomis asmens duomenys perduodami į trečiąsias valstybes pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679“, *supra note,* 497: 14 sąlygos a) p.

480 „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *supra note,* 8: 192 p.

481 *Ibid*, 195, 196 p.

kokią tiesioginę valdžios institucijų prieigą prie asmens duomenų, perduotų pagal šias sąlygas, pagal paskirties valstybės teisės aktus“[482].

Autoriaus vertinimu, tokios garantijos duomenų subjektų atžvilgiu gali būti laikomos formaliomis, atsižvelgiant į kelias aplinkybes. JAV teisinėje sistemoje, bent daliai taikomų žvalgybos priemonių (pvz., JAV Prezidento nurodymo 12333 pagrindu), nėra taikoma išankstinė teisminė kontrolė[483], todėl, neabejotina, apie tai nėra pranešama nei duomenų importuotojams. Tokiu būdu, duomenų importuotojai neturės net teorinės galimybės įgyvendinti standartinėse duomenų apsaugos sąlygose numatytos pareigos[484] informuoti duomenų eksportuotojus ir subjektus apie valdžios institucijų prieigą prie jų tvarkomų duomenų. Be to, net pagal Europos Žmogaus Teisių Teismo praktiką pripažįstama, kad pavojus, dėl kurio sekimas apskritai buvo taikytas, gali išlikti daugelį metų ar net dešimtmečius po konkrečios priemonės taikymo pabaigos, todėl net ir vėlesnis pranešimas subjektui gali kelti grėsmę ilgalaikiam tikslui, dėl kurio iš pradžių buvo pradėtas stebėjimas[485]. Tokiu būdu, darytina išvada, kad standartinėse duomenų apsaugos sąlygų susitarimo 15.1 sąlygos a) p. numatytos pareiga pranešti duomenų subjektams apie valdžios institucijų prieigą prie jų asmens duomenų *de facto* nebus įgyvendinama.

Taip pat standartinėse duomenų apsaugos sąlygose (be bendros pareigos bendradarbiauti ir dėti visas pastangas, kad kilęs ginčas būtų taikiai išspręstas laiku[486]), yra įtvirtinta duomenų subjekto teisė pateikti skundą savo nuolatinės gyvenamosios vietos, darbo vietos valstybės narės priežiūros institucijai (arba kitai kompetentingai priežiūros institucijai) arba perduoti ginčą nagrinėti kompetentingiems teismams[487].

Taigi, autoriaus vertinimu, Europos Komisijos parengtose standartinėse duomenų apsaugos sąlygose nėra jokių Europos Sąjungos Teisingumo Teismo sprendimo

---

[482] „2021 m. birželio 4 d. Europos Komisijos įgyvendinimo sprendimas dėl standartinių sutarčių sąlygų, kuriomis asmens duomenys perduodami į trečiąsias valstybes pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679“, *supra note,* 497: 15.1 sąlygos a) p. i) ir ii) pp.

[483] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, *op. cit.,* 183 p.

[484] „2021 m. birželio 4 d. Europos Komisijos įgyvendinimo sprendimas dėl standartinių sutarčių sąlygų, kuriomis asmens duomenys perduodami į trečiąsias valstybes pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679“, *op. cit*., 15.1 sąlygos a) p. ii) pp.

[485] „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją“*, supra note,* 342: 136 p.

[486] „2021 m. birželio 4 d. Europos Komisijos įgyvendinimo sprendimas dėl standartinių sutarčių sąlygų, kuriomis asmens duomenys perduodami į trečiąsias valstybes pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679“, *supra note,* 497: 11 sąlygos b) p.

[487] *Ibid*, 11 sąlygos c) p.

*Schrems II* byloje suformuotų problemų dėl veiksmingos duomenų subjektų teisių apsaugos sprendimo būdų. Pabrėžtina, kad teisė kreiptis į kompetentingas institucijas Europos Sąjungoje egzistavo ir anksčiau bei galimybę pasinaudoti tokiomis teisių gynimo priemonėmis įrodo sprendimas *Schrems II* byloje – pats Austrijos pilietis M. Schrems sėkmingai kreipėsi į kompetentingą Airijos duomenų priežiūros instituciją bei inicijavo ginčą Europos Sąjungos teismuose. Tačiau tokio ginčo sprendimo galimas rezultatas yra tik paties duomenų perdavimo teisinio pagrindo (šiuo atveju – standartinių duomenų apsaugos sąlygų) panaikinimas. Be to, nepaisant tokių teisių gynimo priemonių prieinamumo ir netgi naudojimosi jomis, Europos Sąjungos Teisingumo Teismo sprendimas *Schrems II* byloje vis tiek konstatavo, kad būtent teisių gynimo priemonių JAV teisės sistemoje trūkumas yra ta aplinkybė, kuri lemia duomenų subjektų teisės į privatumą ir asmens duomenų apsaugą neproporcingą ribojimą.

Apibendrinant nurodytas aplinkybes, darytina išvada, kad pagrindinės Europos Sąjungos Teisingumo Teismo sprendime *Schrems II* byloje identifikuotos problemos yra susijusios su JAV teisės sistemoje (i) numatyta neribota teisėsaugos ir žvalgybos institucijų prieiga prie iš Europos Sąjungos gaunamų asmens duomenų bei (ii) egzistuojančiu teisių gynimo priemonių trūkumu. Europos Komisijos parengtos standartinės duomenų apsaugos sąlygos nesprendžia ir net negali išspręsti nė vienos iš šių problemų, nes JAV teisinis reguliavimas nepasikeitė. Be to, pačios standartinėse duomenų apsaugos sąlygos yra taikomos santykiams tarp privačių subjektų (duomenų subjekto, duomenų eksportuotojo ir importuotojo), o pagal *Schrems II* bylos aplinkybes, šių subjektų veiksmų teisėtumas ir nebuvo kvestionuojamas – pamatinė problema visuomet buvo JAV teisinės sistemos suteikiamos plačios galios teisėsaugos ir žvalgybos institucijoms bei iš esmės neribota prieiga prie Europos Sąjungos vartotojų asmens duomenų. Todėl, autoriaus vertinimu, Europos Komisijos parengtos standartinės duomenų apsaugos sąlygos turi būti vertinamos kaip kartojimas tos pačios klaidos, kaip ir *Privacy Shield* susitarimo sudarymas 2016 m. po Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje 2015 m. priėmimo.

## 5. Privatumo apsaugos elektroninėje erdvėje problemos Lietuvoje dėl skirtingų teisinių sistemų sąveikos

Lietuvos Respublika yra Europos Sąjungos narė, todėl joje yra tiesiogiai taikomas BDAR reguliavimas. Kaip analizuota ankstesnėse šio tyrimo dalyse, sąveikaujant Europos Sąjungos ir kitai teisinei sistemai, asmens duomenys gali būti perduodami tik pagal tam tikras taisykles, įtvirtintas BDAR.

BDAR asmens duomenų perdavimui į trečiąsias valstybes arba tarptautinėms organizacijoms reglamentuoti yra skirtas atskiras skyrius – V-asis BDAR skyrius. Šiame BDAR skyriuje yra įtvirtinti keli savarankiški asmens duomenų perdavimo įteisinimo būdai - duomenų perdavimas remiantis sprendimu dėl tinkamumo[488], duomenų perdavimas taikant tinkamas apsaugos priemones[489], kitos asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai sąlygos[490].

Todėl privatumo apsaugai elektroninėje erdvėje Lietuvoje dėl skirtingų teisinių sistemų sąveikos yra aktualios tos pačios teisinės problemos, kurios yra analizuotos ankstesniuose šio darbo skirsniuose.

Tačiau kaip ir kiekvienoje šalyje ir teisinėje sistemoje, taikant konkrečias taisykles, Lietuvoje taip pat kyla problemų ir teisinių ginčų, kurie, nors ir varijuoja savo svarba ir reikšmingumu, gali būti laikomi unikaliais.

Atsižvelgiant į šio tyrimo temą, autorius šiame darbo skyriuje siekia nustatyti ir atskleisti, ar Lietuvoje buvo kilusios problemos dėl privatumo apsaugos skirtingų teisinių sistemų sąveikoje.

Prieš įsigaliojant BDAR, Europos Sąjungoje ir Lietuvoje asmens duomenų perdavimą į trečiąsias šalis ir organizacijas reguliavo Direktyva 95/46. Lietuvoje ji buvo įgyvendinta Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymu. Asmens duomenų teikimas duomenų gavėjams, esantiems užsienio valstybėse, buvo reguliuojamas šio įstatymo 35 str. Šio straipsnio 5 dalyje buvo įtvirtintas sąrašas atvejų, kuomet buvo leidžiama asmens duomenis perduoti gavėjui į užsienio valstybę, 2 dalyje – numatyta pareiga gauti leidimą iš Valstybinės duomenų apsaugos inspekcijos asmens duomenų perdavimui kitais atvejais.

---

488 „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)“, *supra note*, 60: 45 str.

489 *Ibid*, 46 str.

490 *Ibid*, 49 str.

Dėl tokio asmens duomenų perdavimo į trečiąsias šalis teisinio mechanizmo, tyrimo atlikimo metu autoriui nepavyko rasti jokios Lietuvos teismų praktikos, kuri galėtų žymėti praktikoje kylančias privatumo apsaugos skirtingų sistemų sąveikoje problemas.

Nuo 2018 m. gegužės mėn. Direktyvos 95/46 reguliavimą pakeitė BDAR. Atsižvelgiant į tai, kad tai yra visoje Europos Sąjungoje tiesiogiai taikomas teisės aktas, jis taip pat įsigaliojo ir Lietuvoje. Atitinkamai, Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas buvo patikslintas, jį suderinant su BDAR reguliavimu.

Nuo BDAR įsigaliojimo, Lietuvoje jau yra kilę nemažai teisinių ginčų dėl BDAR reguliavimo taikymo, tačiau šio tyrimo temos atskleidimui aktualiu gali būti vertinamas tik vienas probleminis atvejis, susijęs su asmens duomenų perdavimu tarp skirtingų teisinių sistemų.

Lietuvos Vyriausiasis Administracinis Teismas 2020 m. gegužę nagrinėjo ginčą pagal fizinio asmens skundą dėl netinkamo jo asmens duomenų tvarkymo[491]. Pareiškėjas teigė, kad jo asmens duomenis (informaciją apie jo šeimai skirtas motinystės ir tėvystės pašalpas) Vilniaus miesto savivaldybės administracija ir Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos (SODRA) nepagrįstai perdavė Baltarusijos Respublikos viešosioms įstaigoms. Taigi, Lietuvos teismų praktikoje buvo kilęs ginčas dėl privatumo apsaugos Lietuvos ir Baltarusijos teisinių sistemų sąveikoje.

Atkreiptinas dėmesys, kad asmens duomenų perdavimo veiksmai šioje byloje buvo atlikti 2017 m. vasario mėn., todėl byloje buvo analizuotas tam laikotarpiui aktualus teisinis reglamentavimas – Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas ir Direktyva 95/46, kurią minėtas įstatymas įgyvendino.

Atsakovai šioje byloje užėmė poziciją, kad asmens duomenys galėjo būti perduodami vadovaujantis dvišaliais Lietuvos ir Baltarusijos Respublikų susitarimais: (i) Lietuvos Respublikos ir Baltarusijos Respublikos sutarties dėl socialinės apsaugos pagrindu bei (ii) Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos ir Baltarusijos Respublikos socialinės apsaugos ministerijos susitarimo dėl pensijų ir pašalpų skyrimo ir pašalpų skyrimo, pervedimo ir mokėjimo tvarkos, sudarytos taip pat pagal 1999 m. vasario 4 d. Lietuvos Respublikos ir Baltarusijos Respublikos sutartį dėl soci-

---

[491] „Lietuvos vyriausiojo administracinio teismo 2020 m. gegužės 14 d. nutartis administracinėje byloje Nr. eA-531-822/2020“, Liteko, žiūrėta 2021 m. rugpjūčio 21 d., http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9562e239-012c-49d8-9adc-91dfa77ebd46.

alinės apsaugos.

Lietuvos Vyriausiasis Administracinis Teismas šioje byloje laikė, kad asmens duomenų perdavimo į Baltarusijos Respubliką veiksmas laikytinas asmens duomenų tvarkymu, kaip jis suprantamas pagal Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymą. Tuomet teismas klausimą dėl asmens duomenų perdavimo teisėtumo mėgino išspręsti taikydamas Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 6 str., kuriame nurodyta, kad „Asmens duomenys šio įstatymo nustatytais atvejais teikiami pagal duomenų valdytojo ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį (daugkartinio teikimo atveju) arba duomenų gavėjo prašymą (vienkartinio teikimo atveju). Sutartyje turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis. Prašyme turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo bei gavimo teisinis pagrindas ir prašomų pateikti asmens duomenų apimtis.“[492].

Atsižvelgdamas į šį teisinį reguliavimą, autoriaus vertinimu, Lietuvos Vyriausiasis Administracinis Teismas laikė, kad asmens duomenų teikimas pagal šiuos prašymus laikytinas vienkartiniais teikimo atvejais pagal duomenų gavėjo prašymus Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 6 str. prasme[493]. Tuomet teismas pritarė pirmosios instancijos teismo vertinimui, kad duomenų gavėjo prašyme pateikti asmens duomenis, turi būti nurodomi išsamūs duomenys, kam bus naudojami gaunami asmens duomenys, bei pateiktas teisėtas pagrindas asmens duomenims gauti ir tvarkyti, tačiau gauti Baltarusijos Respublikos institucijų prašymai tokiais duomenimis nepasižymėjo[494].

Taigi, atsižvelgdamas į tai, kad (i) Lietuvos ir Baltarusijos Respublikų sudarytose sutartyse nėra detaliai reglamentuotos asmens duomenų perdavimo sąlygos ir procedūros, tokie susitarimai negali būti laikomi ilgalaikėmis asmens duomenų tiekimo sutartimis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 6 str. prasme ir (ii) iš Baltarusijos institucijų gautuose prašymuose nėra pateiktas pagrindas asmens duomenims gauti ir tvarkyti, teismas darė išvadą, kad toks pareiškėjo asmens duomenų tvarkymas (t. y. perdavimas Baltarusijos Respublikos institucijoms) negali

---

492 Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, redakcija galiojusi nuo 2017-01-01, LRS, žiūrėta 2021 m. rugpjūčio 2 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/niDiSWRPgI.

493 „Lietuvos vyriausiojo administracinio teismo 2020 m. gegužės 14 d. nutartis administracinėje byloje Nr. eA-531-822/2020“, *supra note*, 513: 39 p.

494 *Ibid*, 41 p.

būti laikomas teisėtu.

Autoriaus vertinimu, šios vienintelės Lietuvos teismuose analizuotos privatumo apsaugos problemos skirtingų teisinių sistemų sąveikoje sprendimo teisinis kelias yra, mažų mažiausiai, kvescionuotinas.

Pirmiausiai, klausimas kyla dėl Lietuvos Vyriausiojo Administracinio Teismo parinkto asmens duomenų perdavimo teisinio pagrindo kvalifikavimo. Kaip nurodyta aukščiau, asmens duomenų perdavimą į užsienio valstybes ginčo veiksmų atlikimo metu reguliavo Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 35 str. nuostatos.

Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 6 str. nustatytos bendrosios taisyklės dėl asmens duomenų teikimo teisinių pagrindų, tuo tarpu 35 str. įtvirtintos specialios taisyklės, kurios taikytinos asmens duomenų perdavimui, kai jų gavėjas yra būtent užsienio valstybėje. Taigi, Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 35 str. nuostatos turi būti laikomos *lex specialis* 6 str. numatytų bendrųjų taisyklių dėl asmens duomenų teikimo jų prašantiems gavėjams, atžvilgiu. Kaip minėta aukščiau, pagal Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 35 str. reguliavimą, asmenys duomenys į trečiąją šalį gali būti perduodami (i) gavus Valstybinės duomenų inspekcijos leidimą (35 str. 2 d.), arba (ii) esant vienai iš minėto įstatymo 35 str. 5 d. sąlygų.

Tarp Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 35 str. 5 d. galimų asmens duomenų perdavimo į trečiąją šalį teisinių pagrindų įtvirtinti tokie, kurie yra aktualūs ir spręsto ginčo atveju, pavyzdžiui „asmens duomenis teikti būtina (arba įstatymų nustatyta) dėl svarbių visuomenės interesų“[495], arba „būtina užkirsti kelią nusikalstamoms veikoms arba būtina jas tirti“[496].

Bylos nagrinėjimo atveju, atsakovai, gavę Baltarusijos institucijų paklausimą, sužinojo, jog pareiškėjas nesąžiningai (nuslėpdamas informaciją apie gaunamas išmokas Lietuvoje) siekė gauti išmokas, susijusias su vaiko gimimu, taip pat ir Baltarusijoje[497]. Todėl atsakovai savo sprendimą suteikti informaciją apie pareiškėją Baltarusijos institucijoms laikė teisėtų, viešąjį interesą atitinkančiu veiksmu.

Autoriaus vertinimu, Lietuvos ir Baltarusijos institucijos, administruodamos socialines išmokas ir siekdamos jas išmokėti laikantis teisės aktų reikalavimų, veikia

---

[495] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, *supra note*, 514: 35 str. 5 d. 4 p.

[496] *Ibid,* 35 str. 5 d. 6 p.

[497] „Lietuvos vyriausiojo administracinio teismo 2020 m. gegužės 14 d. nutartis administracinėje byloje Nr. eA-531-822/2020“, *supra note*, 513: 6 p.

tenkindamos svarbius visuomenės interesus. Tam, kad šias funkcijas galėtų įvykdyti laikantis teisės aktų reikalavimų (*inter alia* neišmokant valstybių skiriamų pašalpų teisės jas gauti neturintiems asmenims), tam tikrais atvejais joms objektyviai gali būti būtina keistis asmens duomenimis. Be to, tokie pareiškėjų veiksmai, kuriais yra siekiama gauti tuo pačiu pagrindu valstybių mokamas išmokas net gali būti laikomas nusikaltimu ar baudžiamuoju nusižengimu (pavyzdžiui, sukčiavimu) skirtingose teisinėse sistemose. Todėl atsižvelgiant į bylos nagrinėjimo metu nustatytas aplinkybes, pareiškėjo asmens duomenų perdavimas turėjo būti laikomas teisėtu vadovaujantis Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 35 str. 5 d. 4 p. ir/ar 6 p. (tuo atveju, jei pareiškėjo siekis gauti išmokas iš dviejų valstybių būtų įrodytas) nustatytais teisiniais pagrindais.

Apibendrinant pateiktus argumentus, gali būti daroma išvada, kad Lietuvos teisinei sistemai yra aktualios tos pačios privatumo apsaugos problemos, sąveikaujant su kita teisine sistema, kaip ir analizuotos kituose šio tyrimo skyriuose. Taip yra dėl to, kad teisė į privatumą Lietuvos teisinėje sistemoje *inter alia* saugoma ir BDAR, kuris yra taikytinas visoje Europos Sąjungoje. Tačiau Lietuvoje buvo kilęs vienas ginčas dėl privatumo apsaugos, sąveikaujant Lietuvos bei kitos šalies teisinei sistemai, kuris Lietuvos teismų buvo išspręstas, autoriaus vertinimu, net netaikant asmens duomenų perdavimo į trečiąją šalį teisinių pagrindų ir netinkamai kvalifikuojant asmens duomenų perdavimo veiksmus.

# IŠVADOS

1. Vadovaujantis atlikta analize, darytina išvada, kad nacionalinio saugumo sąvoka Lietuvos, Europos Sąjungos ar JAV teisės sistemose nėra apibrėžta. Visų šių teisės sistemų reguliavimo analizė atskleidžia, kad jos stokoja aiškios indikacijos apie galimas nacionalinio saugumo sampratos ribas. Ypač riba tarp žvalgybos veiklos (kuria saugomas nacionalinis saugumas) ir kriminalinės žvalgybos (kurios pagrindu kovojama su nusikalstamumu) yra neaiški, nes visuotinai sutariama, kad, pavyzdžiui, kova su terorizmu yra vedina valstybių tiek nacionalinio saugumo apsaugos, tiek nusikaltimų prevencijos tikslais. Todėl valstybės, siekdamos riboti asmenų teisę į privatumą ir pateisinti prieigą prie asmens duomenų gali tai daryti skirtingais teisiniais pagrindais ir pagal skirtingas taisykles – arba pagal nacionalinio saugumo apsaugos teisinį mechanizmą, arba nusikaltimų prevencijos tikslais. Nesant koncepcinių nacionalinio saugumo sampratos ribų, teisėsaugos ir žvalgybos institucijos gali piktnaudžiauti joms prieinamais teisės į privatumą ribojimo pagrindais. Siekiant minimizuoti šią riziką, siūlytina Lietuvos teisiniame reguliavime įtvirtinti konkrečius kriterijus, kurie leistų identifikuoti visuomeninio reiškinio priskyrimą nacionalinio saugumo apsaugos sričiai ir įgalintų brėžti ribas tarp žvalgybos ir kriminalinės žvalgybos veiklų.

2. Dėl teisės į privatumą apsaugos skirtingų sistemų sąveikoje, atsižvelgiant į asmens duomenų perdavimo teisinius pagrindus pagal BDAR, jų tarpusavio santykį bei priklausomybę:

2.1. duomenų valdytojai ar tvarkytojai, pageidaujantys perduoti duomenis į JAV (trečiąją šalį), kai Europos Sąjungos Teisingumo Teismas panaikino *Privacy Shield* susitarimą, patys negali duomenų subjektams užtikrinti „iš esmės lygiaverčio apsaugos lygio, koks garantuojamas Europos Sąjungoje“, nes jie negali suteikti jokių teisių ar garantijų duomenų subjektams, kurios galėtų „pagerinti“ duomenų subjektų padėtį ryšium su JAV valdžios institucijų neribota prieiga prie jų asmens duomenų ir masinio asmens duomenų rinkimo.

2.2. nepaisant prieštaringo BDAR preambulės 107 p. ir 44 str. reguliavimo, asmens duomenų perdavimas iš Europos Sąjungos į trečią šalį, teritoriją ar tarptautinę organizaciją negali būti laikomas teisėtu, jei ankstesnis asmens duomenų perdavimo teisinis pagrindas vienu iš V skyriuje įtvirtintų pagrindų (pvz., *Privacy Shield* susitarimas, sudarytas BDAR 45 str. 3 d. pagrindu) buvo panaikintas dėl priežasčių, kurių ištaisymas nepriklauso nuo trečiojoje šalyje veikiančio duomenų valdytojo ar tvarkytojo

ir jų galimų taikyti pavyzdinių tinkamų apsaugos priemonių BDAR V skyriaus prasme.

3. Dėl Europos Sąjungos Teisingumo Teismo praktikos, susijusios su asmens teisės į privatumą ir asmens duomenų apsauga ir reikšmingų JAV teisinio reguliavimo kliūčių, užkertančių kelią sėkmingam asmens duomenų perdavimui iš Europos Sąjungos į JAV:

3.1. Europos Sąjungos Teisingumo Teismo sprendimo *Digital Rights Ireland* byloje analizė leidžia daryti išvadą, kad elektroninių ryšių subjektų pareiga numatytą laikotarpį (*Digital Rights Ireland* bylos atveju – 6 – 24 mėn.) saugoti turimus srauto ir vietos nustatymo duomenis nusikaltimų prevencijos, atskleidimo, tyrimo arba patraukimo už juos atsakomybėn, taip pat valstybės saugumo užtikrinimo tikslais, yra neproporcinga ir neteisėta. Tačiau šis teismo sprendimas neleidžia daryti aiškios išvados, ar tokie veiksmai apskritai gali būti teisėti, esant kitokiam teisiniam reguliavimui ir galiojant papildomoms teisės į privatumą ir asmens duomenų apsaugą užtikrinimo priemonėms, kuriomis duomenų subjektai galėtų pasinaudoti.

3.2. Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje analizė leidžia daryti išvadą, kad susitarimas tarp Europos Sąjungos ir JAV (*Schrems* bylos atveju – *Safe Harbour* susitarimas) negali būti laikomas užtikrinančiu adekvačią asmenų teisės į privatumą ir asmens duomenų apsaugą JAV teisinėje sistemoje, kai susitarime įtvirtinti teisės į privatumą apsaugos principai apskritai netaikomi JAV valdžios įstaigoms arba kai JAV teisėsaugos ir žvalgybos institucijoms suteikiama prieiga prie JAV subjektams perduodamų Europos Sąjungos vartotojų asmens duomenų, o jie neturi procedūrinių garantijų apginti savo galimai pažeidžiamas teises JAV teritorijoje.

3.3. Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje analizė leidžia daryti išvadą, kad BDAR yra taikomas asmens duomenų perdavimui, atliktam valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, jei atliekant šį perdavimą ar po jo šios trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais. Todėl didžiausią iššūkį galimiems susitarimams dėl duomenų perdavimo tarp Europos Sąjungos ir JAV kelia būtent JAV taikomų nacionalinį saugumą užtikrinančių priemonių (pvz. vykdomo masinio sekimo) atitikties vertinimas BDAR atžvilgiu.

4. Dėl proporcingumo principo, kaip pagrindinės teisės ribojimo teisėtumo įvertinimo kriterijaus taikymo sprendžiant teisės į privatumą apsaugos skirtingų teisinių sistemų sąveikoje problemą:

4.1. Europos Sąjungos teisės kontekste, proporcingumo principas yra vienas

reikšmingiausių teisinių konceptų, galinčių padėti nustatyti protingą pusiausvyrą tarp viešųjų interesų konkurencijos (pvz. teisės į privatumą ir nacionalinio saugumo apsaugos). Todėl jis gali būti laikomas raktu į teisingą sprendimą dėl asmens teisės į privatumą apsaugos ribojimų teisėtumo nustatymo, tame tarpe ir pateisinant teisės į privatumą ir asmens duomenų apsaugą ribojimą, taikomą trečios šalies nacionalinio saugumo užtikrinimo tikslais.

4.2. Pagal Europos Sąjungos Teisingumo Teismo sprendimą byloje *Schrems II*, kad pats *Privacy Shield* susitarimas pažeidžia pagrindinės teisės į privatumą esmę. Tokio (t. y. teisės į privatumą esmės) pažeidimo nustatymas eliminuoja būtinybę taikyti proporcingumo principą ir atlikti konkuruojančių interesų analizę ir teisingo jų balanso paiešką. Konstatavus teisės į privatumą ir duomenų apsaugą esmės pažeidimą, JAV teisės sistemoje galiojančių teisės į privatumą ribojimų neproporcingumas negali būti švelninamas net ir atsižvelgiant į veiksmingas teisių gynimo priemones, jei tokios Europos Sąjungos duomenų subjektams ir būtų suteiktos JAV *Privacy Shield* susitarimo pagrindu.

4.3. Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje dėl Privacy Shield susitarimo panaikinimo netiesiogiai verčia JAV ar kitą trečiąją šalį, kuri pageidauja būti pripažinta užtikrinančia adekvatų teisės į privatumą ir asmens duomenų apsaugą lygį BDAR V skyriaus prasme, atsisakyti savo nacionalinio saugumo interesų įgyvendinimo iš Europos Sąjungos gaunamų duomenų atžvilgiu. Todėl Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje užkirto kelią susitarimo dėl asmens duomenų perdavimo tarp Europos Sąjungos ir kitos teisinės sistemos (tame tarpe ir JAV) sudarymui, trečiai šaliai neatsisakant savo nacionalinio saugumo intereso įgyvendinimo iš Europos Sąjungos gaunamų duomenų atžvilgiu.

5. Dėl būtinų privatumo apsaugos pokyčių JAV teisės sistemoje, siekiant teisėto asmens duomenų perdavimo iš Europos Sąjungos į JAV:

5.1. Atsižvelgiant į tai, kad JAV institucijoms suteikiant neribotą prieigą prie iš Europos Sąjungos subjektų gaunamų duomenų, yra pažeidžiama teisės į privatumą ir asmens duomenų apsaugą esmė, siekiant ilgalaikį sudaryti susitarimą dėl asmens duomenų perdavimo tarp Europos Sąjungos ir JAV, JAV teisinėje sistemoje turėtų būti apribota teisėsaugos ir žvalgybos institucijų prieiga prie skirtingų kategorijų duomenų, pavyzdžiui, suteikiant prieigą tik prie asmenų, siejamų su sunkiais nusikaltimais ar keliančių tiesioginį ir pagrįstą pavojų nacionalinio saugumo užtikrinimui, duomenų.

5.2. Atsižvelgiant į tai, kad teisės į privatumą ribojimo proporcingumas gali pri-

klausyti nuo duomenų subjektams prieinamų procedūrinių apsaugos priemonių egzistavimo, priimtinas efektyvios asmenų teisių pažeidimų apsaugos modelis yra galimas JAV teisinėje sistemoje įgyvendinant šiuos pagrindinius pakeitimus: (i) praplečiant nepriklausomo subjekto (pvz., ombudsmeno, kuris buvo numatytas pagal *Privacy Shield* susitarimą) galias ir įgaliojant priimti teisėsaugos ir žvalgybos tarnyboms privalomus sprendimus (įskaitant ir susijusius su JAV Prezidento nurodymu Nr. 12333), (ii) numatant nepriklausomo subjekto aiškias nepriklausomumo nuo vykdomosios valdžios garantijas, (iii) įtvirtinant asmenų skundų nagrinėjimo modelį, pasižymintį bent ribotu rungimosi principu, pavyzdžiui, asmeniui neatskleidžiant jo atžvilgiu surinktos informacijos turinio ir apimties, tačiau užtikrinant, kad kompetentingas ir nepriklausomas subjektas galėtų nešališkai ir pagrįstai išnagrinėti asmens skundą dėl teisėsaugos ar žvalgybos institucijų veiksmų pagrįstumo.

# PASIŪLYMAI

1. Pasiūlymai BDAR 45 str. teisinio reguliavimo tobulinimui:

*45 straipsnis*

**Duomenų perdavimas remiantis sprendimu dėl tinkamumo**

1. Perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai galima, jeigu Komisija nusprendė, kad atitinkama trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Tokiam duomenų perdavimui specialaus leidimo nereikia.

2. Vertindama apsaugos lygio tinkamumą, Komisija visų pirma atsižvelgia į šiuos aspektus:

| | |
|---|---|
| a) | teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, atitinkamus bendruosius ir atskiriems sektoriams skirtus teisės aktus, įskaitant susijusius su visuomenės saugumu, gynyba, nacionaliniu saugumu, baudžiamąja teise ir valdžios institucijų prieiga prie asmens duomenų, taip pat tokių teisės aktų įgyvendinimą, duomenų apsaugos taisykles, profesines taisykles ir saugumo priemones, įskaitant taisykles dėl tolesnio asmens duomenų perdavimo į kitą trečiąją valstybę ar kitai tarptautinei organizacijai, kurių laikomasi toje valstybėje arba kurių laikosi ta tarptautinė organizacija, teismų praktikos precedentus, taip pat veiksmingas ir vykdytinas duomenų subjektų teises ir veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones; |
| b) | tai, ar yra ir ar veiksmingai veikia viena ar kelios nepriklausomos priežiūros institucijos trečiojoje šalyje arba kurioms yra pavaldi tarptautinė organizacija ir kurių atsakomybė yra užtikrinti, kad būtų laikomasi duomenų apsaugos taisyklių ir jos būtų vykdomos, įskaitant tinkamus vykdymo įgaliojimus padėti duomenų subjektams naudotis savo teisėmis ir patarti, kaip tai daryti, ir bendradarbiauti su valstybių narių priežiūros institucijomis *ir valdžios institucijomis bei teikti jiems privalomus nurodymus dėl duomenų apsaugos taisyklių įgyvendinimo*; ir |

| | |
|---|---|
| c) | atitinkamos trečiosios valstybės arba tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus ar kitus įsipareigojimus, atsirandančius dėl teisiškai privalomų konvencijų ar priemonių, taip pat dėl jų dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma kiek tai susiję su asmens duomenų apsauga.; |
| | *d) aplinkybių, nulėmusių ankstesnių Komisijos sprendimų dėl tinkamumo panaikinimą arba dalinį pakeitimą šio straipsnio 5 dalies pagrindu, pasikeitimą trečiojoje valstybėje arba tarptautinėje organizacije ir padėties ištaisymą.* |

3. Komisija, įvertinusi apsaugos lygio tinkamumą, gali nuspręsti, priimdama įgyvendinimo aktą, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamo lygio apsaugą, kaip apibrėžta šio straipsnio 2 dalyje. *Įgyvendinimo akte Komisija privalo motyvuoti trečiosios valstybės arba tarptautinės organizacijos asmens duomenų tvarkymo teisinio reguliavimo (ar taikytinų taisyklių) atitiktį kiekvieno iš šio straipsnio 2 dalyje nurodytu apsaugos lygio tinkamumo aspektų atžvilgiu.* Įgyvendinimo akte numatomas periodinės peržiūros, atliekamos bent kas ketverius metus, kuria atsižvelgiama į visus atitinkamus pokyčius trečiojoje valstybėje ar tarptautinėje organizacijoje, mechanizmas. Įgyvendinimo akte nustatoma jo teritorinė ir sektorinė taikymo sritis ir, kai taikoma, nurodoma šio straipsnio 2 dalies b punkte nurodyta priežiūros institucija ar institucijos. Įgyvendinimo aktas priimamas laikantis 93 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

4. Komisija nuolat stebi pokyčius trečiosiose valstybėse ir tarptautinėse organizacijose, kurie galėtų daryti poveikį pagal šio straipsnio 3 dalį priimtų sprendimų ir pagal Direktyvos 95/46/EB 25 straipsnio 6 dalį priimtų sprendimų veikimui.

5. Komisija nusprendžia, kad trečioji valstybė, teritorija arba nurodytas vienas ar keli sektoriai trečiojoje valstybėje, arba tarptautinė organizacija nebeužtikrina tinkamo lygio apsaugos, kaip apibrėžta šio straipsnio 2 dalyje, jei tai paaiškėja iš turimos informacijos, visų pirma atlikus šio straipsnio 3 dalyje nurodytą peržiūrą, reikiamu mastu įgyvendinimo aktais panaikina arba iš dalies pakeičia šio straipsnio 3 dalyje nurodytą sprendimą, arba sustabdo jo galiojimą nustatydama, kad tai netaikoma atgaline data. *Komisijos įgyvendinimo akte, kuriuo yra panaikinamas ar iš dalies pakeičiamas šio straipsnio 3 dalyje nurodytas sprendimas, arba sustabdomas jo galiojimas, turi būti nurodoma, ar asmens duomenų perdavimas į trečiąją valstybę, teritoriją arba nurodytą*

*vieną ar kelis sektorius trečiojoje valstybėje, arba tarptautinę organizaciją yra galimas kitais šiame Reglamento skyriuje nurodytais teisiniais pagrindais.* Tie įgyvendinimo aktai priimami laikantis 93 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6. Komisija pradeda konsultacijas su trečiąja valstybe arba tarptautine organizacija, siekdama, kad padėtis, dėl kurios buvo priimtas sprendimas pagal 5 dalį, būtų ištaisyta.

7. Sprendimas pagal šio straipsnio 5 dalį nedaro poveikio asmens duomenų perdavimui į atitinkamą trečiąją valstybę, teritoriją arba nurodytą sektorių toje trečiojoje valstybėje, arba atitinkamai tarptautinei organizacijai pagal 46–49 straipsnius *tik tuo atveju, jei padėtis, dėl kurių sprendimas pagal šio straipsnio 5 dalį yra priimamas, gali būti ištaisoma priimant sprendimus pagal šio reglamento 46–49 straipsnius ir jais nėra pakenkiama šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui, kaip nurodyta šio reglamento 44 straipsnyje*.

8. Komisija *Europos Sąjungos oficialiajame leidinyje* ir savo interneto svetainėje paskelbia trečiųjų valstybių, teritorijų ir nurodyto vieno ar kelių sektorių trečiojoje valstybėje, taip pat tarptautinių organizacijų, kurios, kaip ji nusprendė, užtikrina tinkamą apsaugos lygį arba jo nebeužtikrina, sąrašą.

9. Sprendimai, kuriuos Komisija priėmė remdamasi Direktyvos 95/46/EB 25 straipsnio 6 dalimi, lieka galioti tol, kol Komisijos sprendimu, priimtu pagal šio straipsnio 3 ar 5 dalį, jie bus iš dalies pakeisti, pakeisti naujais sprendimais arba panaikinti.

2. Pasiūlymai BDAR 46 str. 1 d. teisinio reguliavimo tobulinimui:

*46 straipsnis*

**Duomenų perdavimas taikant tinkamas apsaugos priemones**

1. Jeigu nėra priimtas sprendimas pagal 45 straipsnio 3 dalį, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai tik tuo atveju, jeigu duomenų valdytojas arba duomenų tvarkytojas yra nustatęs tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis *ir nėra tenkinamos 45 straipsnio 7 dalyje įtvirtinto draudimo taikymo sąlygos*.

Pasiūlymai BDAR 49 str. 1 d. teisinio reguliavimo tobulinimui:

*49 straipsnis*

**Nukrypti leidžiančios nuostatos konkrečiais atvejais**

1. Jeigu nepriimtas sprendimas dėl tinkamumo pagal 45 straipsnio 3 dalį arba nenustatytos tinkamos apsaugos priemonės pagal 46 straipsnį, įskaitant įmonei privalomas taisykles, asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai arba tokių perdavimų seka ~~atliekami~~ *gali būti atliekamas* tik *tuomet, kai nėra tenkinamos 45 straipsnio 7 dalyje įtvirtinto draudimo taikymo sąlygos ir* su viena iš šių sąlygų:

| | |
|---|---|
| a) | duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu po to, kai buvo informuotas apie galimus tokių perdavimų pavojus duomenų subjektui dėl to, kad nepriimtas sprendimas dėl tinkamumo ir nenustatytos tinkamos apsaugos priemonės; |
| b) | duomenų perdavimas yra būtinas duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti arba ikisutartinėms priemonėms, kurių imtasi duomenų subjekto prašymu, įgyvendinti; |
| c) | duomenų perdavimas yra būtinas, kad būtų sudaryta arba įvykdyta duomenų subjekto interesais sudaroma duomenų valdytojo ir kito fizinio ar juridinio asmens sutartis; |
| d) | duomenų perdavimas yra būtinas dėl svarbių viešojo intereso priežasčių; |
| e) | duomenų perdavimas yra būtinas siekiant pareikšti, vykdyti ar ginti teisinius reikalavimus; |
| f) | duomenų perdavimas yra būtinas, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kitų asmenų interesai, jeigu duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo; |
| g) | duomenys perduodami iš registro, pagal Sąjungos arba valstybės narės teisę skirto teikti informaciją visuomenei, su kuria gali susipažinti plačioji visuomenė arba bet kuris asmuo, galintis įrodyti teisėtą interesą, tačiau tik tiek, kiek konkrečiu atveju laikomasi pagal Sąjungos arba valstybės narės teisę nustatytų susipažinimo su tokiame registre esančia informacija sąlygų. |

Kai perdavimas negali būti grindžiamas 45 arba 46 straipsnio nuostata, įskaitant nuostatas dėl įmonei privalomų taisyklių, ir netaikoma jokia pirmoje pastraipoje nurodyta konkrečioje situacijoje nukrypti leidžianti nuostata, perdavimas nėra kartojamas, yra

susijęs tik su ribotu duomenų subjektų skaičiumi, yra būtinas įtikinamų duomenų valdytojo ginamų teisėtų interesų, kai nėra už juos viršesnių duomenų subjekto interesų ar teisių ir laisvių, tikslais, jeigu duomenų valdytojas yra įvertinęs visas su duomenų perdavimu susijusias aplinkybes ir, remdamasis tuo vertinimu, yra nustatęs tinkamas su asmens duomenų apsauga susijusias apsaugos priemones. Duomenų valdytojas praneša priežiūros institucijai apie duomenų perdavimą. Be 13 ir 14 straipsniuose nurodytos informacijos, duomenų valdytojas praneša duomenų subjektui apie duomenų perdavimą ir apie įtikinamus ginamus teisėtus interesus.

# LITERATŪROS SĄRAŠAS

**Teisės aktai**

**Europos Tarybos ir kiti tarptautiniai teisės aktai**


1. „1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.
2. „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“. EUR-lex. Žiūrėta 2021 m. liepos 22 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.
3. „2000 m. liepos 26 d. Europos Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „Safe Harbor“ susitarimo privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų “Dažnai užduodamų klausimų”. Žiūrėta 2021 m. kovo 16 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32000D0520.
4. „2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų“. LRS. Žiūrėta 2021 m. rugpjūčio 6 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195.
5. „2005 m. birželio 21 d. Tarybos reglamentas (EB) Nr. 1290/2005 dėl bendrosios žemės ūkio politikos finansavimo su pakeitimais, padarytais 2007 m. lapkričio 26 d.Tarybos reglamentu (EB) Nr. 1437/2007, 42 straipsnio“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 11 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32007R1437.
6. „2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB“. EUR-lex. Žiūrėta 2021 m. liepos 30 d. https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:32006L0024.
7. „2008 m. kovo 18 d. Komisijos reglamentas (EB) Nr. 259/2008, kuriuo nustatomos išsamios Reglamento Nr. 1290/2005 nuostatų dėl informacijos apie Europos žemės ūkio garantijų fondo ir Europos žemės ūkio fondo kaimo plėtrai paramos gavėjus skelbimo taikymo taisyklės“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 11 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32008R0259.

8. „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“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016L0680.
9. „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)“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679.
10. „2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimas (ES) 2016/2297 kuriuo iš dalies keičiami sprendimai 2001/497/EB ir 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosioms šalims ir tokiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas“. EUR-lex. Žiūrėta 2021 birželio 20 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016D2297.
11. „2016 m. liepos 12 d. Europos Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl Europos Sąjungos ir JAV „Privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB“. EUR-lex. Žiūrėta 2021 m. liepos 20 d. https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX%3A32016D1250.
12. „2016 m. liepos 6 d.  Europos Parlamento ir Tarybos Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016L1148.
13. „2021 m. birželio 4 d. Europos Komisijos įgyvendinimo sprendimas dėl standartinių sutarčių sąlygų, kuriomis asmens duomenys perduodami į trečiąsias valstybes pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32021D0914&from=EN.
14. „Convention on Cybercrime“. Council of Europe. Žiūrėta 2021 m. rugpjūčio 6 d. https://rm.coe.int/1680081561.

15. „Europos Komisijos 2000 m. liepos 26 d. sprendimas dėl Šveicarijoje teikiamos pakankamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2000/518/EB“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32000D0518.
16. „Europos Komisijos 2001 m. gruodžio 20 d. sprendimas dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2002/2/EB”. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d.https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32002D0002.
17. „Europos Komisijos 2003 m. birželio 30 d. sprendimas dėl adekvačios asmens duomenų apsaugos Argentinoje, remiantis Europos Parlamento ir Tarybos direktyva 95/46/EB Nr. 2003/490/EB“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32003D0490&from=-BG.
18. „Europos Komisijos 2010 m. spalio 19 d. sprendimas dėl tinkamos asmens duomenų apsaugos Andoroje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2010/625/ES”. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32010D0625&from=EN.
19. „Europos Komisijos 2011 m. sausio 31 d. sprendimas dėl Izraelio Valstybės užtikrinamos tinkamos asmens duomenų apsaugos automatizuoto asmens duomenų tvarkymo srityje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB Nr. 2011/61/ES“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32011D0061&from=PL.
20. „Europos Komisijos 2019 m. sausio 23 d. sprendimas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Japonijoje pagal Asmeninės informacijos apsaugos įstatymą Nr. (EU)2019/419“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019D0419&from=EN.
21. „Europos Parlamento ir Tarybos 2018 m. gruodžio 11 d. direktyva (ES) 2018/1972 kuria nustatomas Europos elektroninių ryšių kodeksas“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=-CELEX:32018L1972&from=LT.
22. „Europos Parlamento ir Tarybos Direktyva 2002/58/EB 2002 m. liepos 12 d. dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriu-

je (Direktyva dėl privatumo ir elektroninių ryšių), L 201, 31/07/2002“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:02002L0058-20091219&from=EN.

23. „Europos Sąjungos ir Jungtinių Amerikos Valstijų 2010 m. liepos 27 d. susitarimas dėl finansinių mokėjimų pranešimų duomenų tvarkymo ir perdavimo iš Europos Sąjungos į Jungtines Valstijas terorizmo finansavimo sekimo programos tikslais“. EUR-lex. Žiūrėta rugpjūčio 7 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32010D0412.
24. „Europos Sąjungos pagrindinių teisių chartija“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 11 d.https://eur-lex.europa.eu/legal content/LT/TXT/PDF/?uri=-CELEX:12016P/TXT&from=EN.
25. „Europos Sąjungos pagrindinių teisių chartija“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 11 d. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=-CELEX:12016P/TXT&from=EN.
26. „Europos Sąjungos sutartis“. EUR-Lex. Žiūrėta 2021 m. rugpjūčio 2 d. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:LT:PDF.
27. „Europos žmogaus teisių komisijos 1993 m. balandžio 2 d. sprendimas dėl David Esbester v. Jungtinė Karalystė skundo priimtinumo“. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-1537&filename=001-1537.pdf&TID=ihgdqbxnfi.
28. „Sutartis dėl Europos Sąjungos veikimo“. Eur-Lex. Žiūrėta 2021 m. rugpjūčio 11 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12012E/TXT&from=LT.

**Lietuvos Respublikos įstatymai ir poįstatyminiai teisės aktai**

29. „Dėl Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komiteto atlikto parlamentinio tyrimo dėl asmenų, verslo subjektų ir kitų interesų grupių galimo neteisėto poveikio valstybės institucijoms priimant sprendimus ir galimos neteisėtos įtakos politiniams procesams išvados“. LRS. Žiūrėta 2021 m. balandžio 20 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3c03fbf26b0611e8b7d2b2d-2ca774092.
30. „Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/

f26839f08f5011e48028e9b85331c55d/asr.
31. „Lietuvos Respublikos elektroninių ryšių įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/asr.
32. „Lietuvos Respublikos kibernetinio saugumo įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e-495dc9901227533ee/asr.
33. „Lietuvos Respublikos Konstitucija“. LRS. Žiūrėta 2021 m. rugpjūčio 4 d. https://www.lrs.lt/home/Konstitucija/Konstitucija.htm.
34. „Lietuvos Respublikos kriminalinės žvalgybos įstatymas“. LRS. Žiūrėta rugpjūčio 3 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.434526/asr.
35. „Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 5 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498/asr.
36. „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.
37. „Lietuvos Respublikos saugios laivybos įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.107736/asr.
38. „Lietuvos Respublikos teismų įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 6 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.5825/asr.
39. „Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas“. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/asr.
40. „Lietuvos Respublikos žvalgybos įstatymas“. LRS. Žiūrėta rugpjūčio 3 d. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167549.
41. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“. Redakcija galiojusi nuo 2017-01-01. LRS. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/niDiSWRPgI.

**Jungtinių Amerikos Valstijų teisės aktai**

42. „1947 m. Nacionalinio saugumo įstatymas“. U.S. Government. Žiūrėta 2021 m. liepos 5 d. https://www.govinfo.gov/content/pkg/COMPS-1493/pdf/COMPS-1493.pdf.

43. „2004 m. Žvalgybos reformos ir terorizmo prevencijos įstatymas“. U.S. Government Printing Office. Žiūrėta 2021 m. liepos 2d. https://www.govinfo.gov/content/pkg/PLAW-108publ458/html/PLAW-108publ458.htm.
44. „2015 USA Freedom Act“. U.S. Congress. Žiūrėta 2021 m. kovo 16 d. https://www.congress.gov/bill/114th-368 congress/house-bill/2048/text.

**Vengrijos teisės aktai**

45. „Vengrijos saugumo tarnybų įstatymas“. Žiūrėta 2021 m. liepos 10 d. https://www.legislationline.org/download/id/4443/file/Act_National_Security_Service_1995_en.pdf.

**Vokietijos Federacinės Respublikos teisės aktai**

46. „Vokietijos Federacinės Respublikos Pagrindinis Įstatymas“. Žiūrėta 2021 m. rugpjūčio 4 d. http://www.gesetze-im-internet.de/gg/index.html.

**Rekomendacinio pobūdžio dokumentai**

47. „29 straipsnio darbo grupės 2016 m. balandžio 13 d. nuomonė Nr. 01/2016 dėl EU – JAV privatumo skydo projekto“. European Commission. Žiūrėta 2021 m. liepos 20 d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.
48. „Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU–US Data Flows, COM(2013) 846 fin“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 3 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0846.
49. „Communication from the Commission to the European Parliament and the Council on the Functioning of the *Safe Harbour* from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 fin“. EUR-lex. Žiūrėta 2021 m. rugpjūčio 3 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:-52013DC0847.
50. „Europos duomenų apsaugos priežiūros pareigūno 2016 m. gegužės 30 d. nuomonė Nr. 4/2016 dėl EU – JAV privatumo skydo projekto“. European Data Protection Supervisor. Žiūrėta 2021 m. liepos 20 d. https://edps.europa.eu/sites/default/files/publication/16-05-30_privacy_shield_en.pdf .

51. „Europos Komisijos personalo 2010 m. spalio 4 d. darbinis dokumentas „Komisijos sprendimo 520/2000/EB įgyvendinimas dėl tinkamos asmens duomenų apsaugos, kurią teikia „Safe Harbor“ susitarimo privatumo principai ir su jais susiję JAV komercijos departamento dažnai užduodami klausimai“. European Commission. Žiūrėta 2021 m. kovo 16 d., https://ec.europa.eu/transparency/documents-register/detail?ref=SEC(2004)1323&lang=en.
52. „Europos Sąjungos ir JAV „Privatumo skydo“ gairės“. European Commission. Žiūrėta 2021 m. kovo 16 d. http://ec.europa.eu/newsroom/document.cfm?doc_id=47770.
53. „Generalinio advokato nacionalinių FTB operacijų gairės“. Jungtinių Amerikos Valstijų Teisingumo departamentas. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.justice.gov/archive/opa/docs/guidelines.pdf.
54. „Nacionalinės žvalgybos direktoriaus biuro teisinių nuorodų knyga (angl. *Legal refference book*)“. **Žiūrėta 2021 m. rugpjūčio 2 d.** https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf.
55. „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2013 m. spalio 2 d. darbinis dokumentas Nr. 02/2013 nustatantis gaires gaunant sutikimą dėl slapukų (angl. *cookies*) naudojimo“. European Commission. Žiūrėta 2021 m. rugpjūčio 2 d. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
56. „Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės 2014 m. gruodžio 5 d. darbinis dokumentas Nr. WP228 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais“. European Commission. Žiūrėta balandžio 20 d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.
57. „Proposal for an ePrivacy Regulation“. European Commission, Žiūrėta 2021 m. rugpjūčio 11 d. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.
58. 29 straipsnio darbo grupės 1999 m. sausio 26 d. nuomonė Nr. 5092/98/EN/final“. European Commission. Žiūrėta 2021 m. kovo 16 d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf.

**Teismų praktika**

**Europos žmogaus teisių teismo praktika**


59. „Europos Žmogaus Teisių Teismo 1976 m. gruodžio 7 d. sprendimas byloje Nr. 5493/72 Handyside prieš Jungtinę Karalystę“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-57499.
60. „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Nr. 5029/71 Klass ir kiti prieš Vokietiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-57510.
61. „Europos Žmogaus Teisių Teismo 1983 m. kovo 25 d. sprendimas byloje Nr. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 Silver ir kt. prieš Jungtinę Karalystę“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf.
62. „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Nr. 8691/79 Malone prieš Jungtinę Karalystę“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf.
63. „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Nr. 9248/81 Leander prieš Švediją“. Bailii. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.bailii.org/eu/cases/ECHR/1987/4.html.
64. „Europos Žmogaus Teisių Teismo 1990 m. balandžio 24 d. sprendimas byloje Nr. 11801/85 Kruslin prieš Prancūziją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf.
65. „Europos Žmogaus Teisių Teismo 1992 m. gruodžio 16 d. sprendimas byloje Nr. 13710/88 Niemietz prieš Vokietiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-57887.
66. „Europos Žmogaus Teisių Teismo 1998 m. birželio 9 d. sprendimas byloje Nr. 10/1997/794/995-996 McGinley ir Egan prieš Jungtinę Karalystę“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-58175.
67. „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendimas byloje Nr. 30194/09 Kopp prieš Šveicariją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-58144.

68. „Europos Žmogaus Teisių Teismo 1998 m. liepos 30 d.sprendimas byloje Nr. 58/1997/842/1048 Valenzuela Contreras prieš Ispaniją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-58208&filename=001-58208.pdf.
69. „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 28341/95 Rotaru prieš Rumuniją“. Bailii. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.bailii.org/eu/cases/ECHR/2000/192.html.
70. „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Nr. 27798/95 Amman prieš Šveicariją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-58497.
71. „Europos Žmogaus Teisių Teismo 2005 m. liepos 5 d. sprendimas byloje Nr. 49790/99 Trubnikov prieš Rusiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-69616.
72. „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Nr. 54934/00 Weber ir Saravia prieš Vokietiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/fre?i=001-76586.
73. „Europos Žmogaus Teisių Teismo 2006 m. birželio 6 d. sprendimas byloje Nr. 62332/00 Segerstedt-Wiberg ir kiti prieš Švediją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-75591.
74. „Europos Žmogaus Teisių Teismo 2007 m. birželio 28 d. sprendimas byloje Nr. 62540/00 Ekimdzhiev prieš Bulgariją“. Bailii. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.bailii.org/eu/cases/ECHR/2007/533.html.
75. „Europos Žmogaus Teisių Teismo 2008 m. liepos 1 d. sprendimas byloje Nr. 58243/00 Liberty ir kiti prieš Jungtinę Karalystę“. Bailii. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.bailii.org/eu/cases/ECHR/2008/568.html.
76. „Europos Žmogaus Teisių Teismo 2008 m. sausio 24 d. sprendimas byloje Nr. 839/02 Maslova ir Nalbandov prieš Rusiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-2241782-2402590&filename=003-2241782-2402590.pdf.
77. „Europos Žmogaus Teisių Teismo 2009 m. vasario 10 d. sprendimas byloje Nr. 25198/02 Iordachi ir kiti prieš Moldovą“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/fre?i=002-1661.
78. „Europos Žmogaus Teisių Teismo 2010 m. gegužės 18 d. nutarimas byloje Nr. 26839/05 Kennedy prieš Jungtinę Karalystę“. Hudoc. Žiūrėta 2021 m. rugpjūčio

2 d. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf.

79. „Europos Žmogaus Teisių Teismo 2010 m. rugsėjo 16 d. sprendimas byloje Nr. 75472/01 Tigran Ayrapetyan prieš Rusiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-100377&filename=001-100377.pdf.
80. „Europos Žmogaus Teisių Teismo 2010 m. rugsėjo 2 d. sprendimas byloje Nr. 35623/05 Uzun prieš Vokietiją“. Bailii. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.bailii.org/eu/cases/ECHR/2010/2263.html.
81. „Europos Žmogaus Teisių Teismo 2010 m. vasario 2 d. sprendimas byloje Nr. 964/07 Dalea prieš Prancūziją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-97520.
82. „Europos Žmogaus Teisių Teismo 2011 m. birželio 21 d. sprendimas byloje Nr. 30194/09 Shimovolos prieš Rusiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.refworld.org/cases,ECHR,4e26e4d32.html.
83. „Europos Žmogaus Teisių Teismo 2013 m. spalio 21 d. sprendimas byloje Nr. 55508/07 ir 29520/09 Janowiec ir kiti prieš Rusiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-127684&filename=001-127684.pdf.
84. „Europos Žmogaus Teisių Teismo 2015 m. gruodžio 4 d. sprendimas byloje Nr. 47143/06 Zakharov prieš Rusiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-159324.
85. „Europos Žmogaus Teisių Teismo 2017 m. birželio 27 d. sprendimas byloje Nr. 931/13 Satakunnan Markkinapörssi Oy ir Satamedia Oy prieš Suomiją“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-175121.
86. „Europos Žmogaus Teisių Teismo 2018 m. rugsėjo 25 d. sprendimas byloje Nr. 76639/11 Denisov prieš Ukrainą“. Hudoc. Žiūrėta 2021 m. rugpjūčio 2 d. http://hudoc.echr.coe.int/eng?i=001-186216.

**Europos Sąjungos teisingumo teismo praktika**

87. „Europos Sąjungos Teisingumo Teismo 1963 m. kovo 27 d. sprendimas sujungtose bylose Nr. 28 iki 30-62 Da Costa en Schaake NV ir kt. prieš Administratie der Belastingen”. InfoCuria. Žiūrėta 2021 m. liepos 30 d. https://curia.europa.eu/

juris/showPdf.jsf?text=&docid=87133&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3549379.

88. „Europos Sąjungos Teisingumo Teismo 1970 m. gruodžio 17 d. sprendimas byloje Nr. C-11-70 Internationale Handelsgesellschaft“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 11 d. https://curia.europa.eu/juris/showPdf.jsf?text=&docid=88063&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3644321.
89. „Europos Sąjungos Teisingumo Teismo 1990 m. lapkričio 13 d. sprendimas byloje Nr. C-331/88 FEDESA“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 11 d. https://curia.europa.eu/juris/showPdf.jsf?text=&docid=88063&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3644321.
90. „Europos Sąjungos Teisingumo Teismo 1997 m. liepos 17 d. sprendimas sujungtose bylose Nr. C-248/95 ir C-249/95 SAM Schiffahrt ir Stapf prieš Bundesrepublik Deutschland“. InfoCuria. Žiūrėta 2021 m. liepos 30 d. https://curia.europa.eu/juris/showPdf.jsf?text=&docid=43712&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3553114.
91. „Europos Sąjungos Teisingumo Teismo 2001 m. liepos 12 d. sprendimas byloje Nr. C-189/01 Jippes ir kt.“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=46530&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3389081.
92. „Europos Sąjungos Teisingumo Teismo 2005 m. liepos 12 d. sprendimas sujungtose bylose C154/04 ir C155/04 Alliance for Natural Health ir kt.“. InfoCuria. Žiūrėta 2021 m. liepos 5 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=60405&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3555378.
93. „Europos Sąjungos Teisingumo Teismo 2005 m. liepos 12 d. sprendimas sujungtose bylose Nr. C-154/04 ir C-155/04 Nutri-Link“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=60405&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2089461.
94. „Europos Sąjungos Teisingumo Teismo 2006 m. gegužės 30 d. sprendimas sujungtose bylose Nr. C-317/04 ir C-318/04 PNR byla“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=145330.

95. „Europos Sąjungos Teisingumo Teismo 2008 m. gruodžio 16 d. sprendimas byloje Nr. C-73/07 Satamedia“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=76075&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=1629974.
96. „Europos Sąjungos Teisingumo Teismo 2008 m. sausio 29 d. sprendimas byloje Nr. C-275/06 Promusicae“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 5 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=1623552.
97. „Europos Sąjungos Teisingumo Teismo 2008 m. rugsėjo 3 d. sprendimas byloje Nr. C-402/05 P ir C-415/05 P Kadi ir Al Barakaat International Foundation prieš Tarybą ir Komisiją“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 3 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=67611&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3395010.
98. „Europos Sąjungos Teisingumo Teismo 2009 m. lapkričio 9 d. sprendimas sujungtose bylose Nr. C-92 ir C-93/09 Schecke ir Eifert“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=125512.
99. „Europos Sąjungos Teisingumo Teismo 2009 m. spalio 1 d. sprendimas byloje Nr. C-247/08 Gaz de France – Berliner Investissement“. InfoCuria. Žiūrėta 2021 m. liepos 30 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=78359&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3552751.
100. „Europos Sąjungos Teisingumo Teismo 2010 m. birželio 22 d. sprendimas sujungtose byloje Nr. C-188/10 ir C-189/10 Melki ir Abdeli“. InfoCuria. Žiūrėta 2021 m. liepos 10 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=80748&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3551700.
101. „Europos Sąjungos Teisingumo Teismo 2013 m. lapkričio 7 d. sprendimas byloje Nr. C-473/12 IPI“. InfoCuria. **Žiūrėta 2021 m. rugpjūčio 2 d.** https://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=1751136.
102. „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland ir Seitlinger ir kt.“. InfoCuria.

*Žiūrėta 2021 m. liepos 30 d.* https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3541738.

103. „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“. InfoCuria. **Žiūrėta 2021 m. rugpjūčio 2 d.** https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3390590.
104. „Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas byloje Nr. C-203/15 ir C-698/15 Tele2 Sverige“. InfoCuria. ***Žiūrėta 2021 m. rugpjūčio 2 d.*** https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3643172.
105. „Europos Sąjungos Teisingumo Teismo 2017 m. liepos 26 d. nuomonė Nr. 1/15“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3653149.
106. „Europos Sąjungos Teisingumo Teismo 2017 m. liepos 26 d. pranešimas spaudai Nr. 84/17“. Curia Europa. **Žiūrėta 2021 m. rugpjūčio 2 d.** https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf.
107. „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf;jsessionid=8508220193825AFC3D98FABEA15645EC?text=&docid=228677&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3350436.
108. „Generalinio advokato Henrik Saugmandsgaard Øe išvada, pateikta 2019 m. gruodžio 19 d. byloje Nr. C-311/18 Schrems II“. InfoCuria. Žiūrėta 2021 m. rugpjūčio 2 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3638243.
109. „Generalinio advokato Yves Bot išvada, pateikta 2015 m. rugsėjo 23 d. byloje Nr. C-362/14 Schrems“. InfoCuria. Žiūrėta 2021 m. liepos 30 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3553683.
110. Europos Sąjungos Teisingumo Teismo 2013 m. liepos 18 d. sprendimas sujung-

tose bylose Nr. C-584/10 P, C-593/10 P ir C-595/10 P Komisija ir kt. prieš Kadi“. InfoCuria. Žiūrėta 2021 m. liepos 10 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3551313.

**Lietuvos Respublikos teismų praktika**

111. „Lietuvos Aukščiausiojo teismo 2020 m. balandžio 16 d. nutartis civilinėje byloje Nr. e3K-3-99-969/2020“. Liteko. Žiūrėta 2021 m. rugpjūčio 6 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=0ad0c05c-5e8e-41bc-8d36-27f135921d6f.
112. „Lietuvos Aukščiausiojo teismo 2020 m. balandžio 9 d. nutartis civilinėje byloje Nr. e3K-7-115-469/2020“. Liteko. Žiūrėta 2021 m. rugpjūčio 6 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=1911e8ff-60cd-4979-ac3f-b3e-ac4b116d6.
113. „Lietuvos Aukščiausiojo teismo 2020 m. birželio 25 d. nutartis civilinėje byloje Nr. 3K-3-203-403/2020“. Liteko. Žiūrėta 2021 m. rugpjūčio 6 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=12db1f84-3ba6-4be1-bb81-9f14c4ba8ff2.
114. „Lietuvos Aukščiausiojo teismo 2020 m. gruodžio 3 d. nutartis civilinėje byloje Nr. e3K-3-323-469/2020“. Liteko. Žiūrėta 2021 m. rugpjūčio 6 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=e3dd0049-d3e8-4137-9575-90bdca-c38f5d.
115. „Lietuvos Aukščiausiojo teismo 2020 m. vasario 12 d. nutartis civilinėje byloje Nr. 3K-3-21-916/2020“. Liteko. Žiūrėta 2021 m. rugpjūčio 6 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=2dd8a7a8-01e4-43ea-8f84-3356155d5b27.
116. „Lietuvos Aukščiausiojo teismo 2021 m. liepos 5 d. nutartis civilinėje byloje Nr. e3K-3-251-916/2021“. Liteko. Žiūrėta 2021 m. rugpjūčio 6 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=21221907-ed71-44f0-ba19-8ba-7172d5ab5.
117. „Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas „Dėl kriminalinės žvalgybos informacijos panaudojimo tiriant korupcinio pobūdžio tarnybinius nusižengimus““. LRKT. Žiūrėta 2021 m. balandžio 20 d. https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta1927/content.

118. „Lietuvos Respublikos Konstitucinio Teismo 2020 m. birželio 12 d. nutarimas „Dėl Seimo laikinajai tyrimo komisijai pavedamo tyrimo ribų““. LRKT. Žiūrėta 2021 m. balandžio 20 d. https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta2161/content.
119. „Lietuvos Respublikos Konstitucinio Teismo 2021 m. kovo 4 d. nutarimas "Dėl baudžiamojo persekiojimo kaip pagrindo pripažinti asmenį neatitinkančiu nacionalinio saugumo interesų"". LRKT. Žiūrėta 2021 m. balandžio 20 d. https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta2379/content.
120. „Lietuvos vyriausiojo administracinio teismo 2018 m. rugsėjo 18 d. nutartis administracinėje byloje Nr. eAS-624-756/2018" . Liteko. Žiūrėta 2021 m. balandžio 21 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=79b87395-dc5e-4e3a-92a0-ef57a79a69ac.
121. „Lietuvos vyriausiojo administracinio teismo 2018 m. rugsėjo 6 d. sprendimas administracinėje byloje Nr. eA-5177-602/2018". Liteko. Žiūrėta 2021 m. balandžio 21 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=92a0f05a-59d5-4b72-b58e-0226bf4f6de8.
122. „Lietuvos vyriausiojo administracinio teismo 2019 m. gruodžio 30 d.nutartis administracinėje byloje Nr. eAS-738-575/2019". Liteko. Žiūrėta 2021 m. balandžio 21 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=fcfce450-5b83-4043-8fbd-5e0373281d69.
123. „Lietuvos vyriausiojo administracinio teismo 2020 m. gegužės 14 d. nutartis administracinėje byloje Nr. eA-531-822/2020". Liteko. Žiūrėta 2021 m. rugpjūčio 21 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9562e239-012c-49d8-9adc-91dfa77ebd46.
124. „Lietuvos vyriausiojo administracinio teismo 2021 m. balandžio 7 d.nutartis administracinėje byloje Nr. A-749-556/2021". Liteko. Žiūrėta 2021 m. balandžio 21 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=5783f33b-8ab1-4b87-9933-1c63b756cf5f.
125. „Vilniaus apygardos teismo Civilinių bylų skyriaus 2020 m. vasario 11 d. nutartis civilinėje byloje Nr. 2A-95-340/2020". Liteko. Žiūrėta 2021 m. balandžio 21 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=d7c034af-a5a6-4723-bc63-3943e611f86e.
126. „Vilniaus apygardos teismo Civilinių bylų skyriaus 2021 m. sausio 19 d. nutartis civilinėje byloje Nr. e2A-165-567/2021". Liteko. Žiūrėta 2021 m. balan-

džio 22 d. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=c-1f3413a-53ad-4655-8852-c90faa5941e6.

**Jungtinių Amerikos Valstijų teismų praktika**

127. „Boyd v. United States“. US Supreme Court Justia. Žiūrėta 2021 m. rugpjūčio 6 d. https://supreme.justia.com/cases/federal/us/116/616/.
128. „Clapper v. Amnesty International“, CaseText, žiūrėta 2021 m. rugpjūčio 5 d., https://casetext.com/case/clapper-v-amnesty-intl-usa-7.
129. „Katz v. United States (1967)“. FindLaw. Žiūrėta 2021 m. liepos 4 d. https://case-law.findlaw.com/us-supreme-court/389/347.html.
130. Airijos Respublikos teismų praktika
131. „Airijos Aukščiausiojo Teismo 2014 m. birželio 18 d. sprendimas byloje Nr. IEHC 310“. Bailii. Žiūrėta 2021 m. liepos 30 d. https://www.bailii.org/ie/cases/IEHC/2014/H310.html.

**Specialioji literatūra**

132. „Arms Control“ 13, 3 (1992): 463-544.
133. „Intelligence Activities and the Rights of Americans“. *Final Report of the U.S. Select Commity to Study Governmental Operations with Respect to Intelligence Activities* S. Rep. 94 – 755, bk. II. Washington: U.S. Government printing Office, 1976.
134. „National Security Law - Surveillance - Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield – Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.,* ECLI:EU:C:2020:559 (July 16, 2020)“. *Harvard Law Review* 134, 4 (2021): 1571. Žiūrėta 2021 m. rugpjūčio 2 d. https://harvardlawreview.org/2021/02/data-protection-commissioner-v-facebook-ireland-ltd/.
135. „Road Map for National Security: Imperative for Change“. *The Phase III Report of the U.S. Commission on National Security/21st Century*. Washington: GPO, 2001.
136. „Supplementary Detailed Staff Reports on Intilligence Activities and the Rights of Americans“. *Final Report of the U.S. Select Commity to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee")* Rep. 94 – 755, bk. III. Washington: U.S. Government printing Office, 1976.
137. Adams, Brittany. „Striking A Balance: Privacy And National Security In Section 702 U.S. Person Queries“. *Washington Law Review* 94, 1 (2019): 401-451.

138. Allison, Graham, ir Gregory F. Treverton. *Rethinking America's Security: Beyond Cold War to New World Order.* New York, 1992.
139. Arenas, Marcelo, Pablo Barceló, Leonid Libkin ir Filip Murlak. *Foundations of Data Exchange*. Cambridge: Cambridge University Press, 2014.
140. Asinari, Pelez, María Verónica Pérez, ir Yves Poullet. „Privacy, Personal Data Protection and the *Safe Harbour* Decision". *The Future of Transatlantic Economic Relations: Continuity Amid Discord* 101 (2005).
141. Atkinson, L. Rush. „The Fourth Amendment's National Security Exception: Its History and Limits". *Vanderbilt Law Review* 66, 5 (2013): 1344-1358.
142. Ažubalytė, Rima. „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema". *Jurisprudencija* 26, 2 (2019): 260–291. doi:10.13165/JUR-19-26-2-02.
143. Baublys, Linas. *Teisės Teorijos įvadas: Vadovėlis. 2-asis Patais. Ir Papild. Leid. ed.* (Vilnius: Mes, 2012).
144. Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon ir R. B. J. Walker. „After Snowden: Rethinking the Impact of Surveillance". *International Political Sociology* 8, 2 (2014): 121-144.
145. Beinoravičius, Darijus, ir Milda Vainiutė. „Kodifikavimo reikšmė, metodai ir tendencijos". *Jurispridencija* 92, 2 (2007): 13-17.
146. Belevičius, Linas. „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas", *Jurisprudencija : mokslo darbai* 29 (2002): 72–85.
147. Bygrave, Lee A. „The Place of Privacy in Data Protection Law". *University of New South Wales Law Journal* 24, 1 (2001): 277-283.
148. Birkinshaw, Patrick. *Freedom of Information: The Law, the Practice, and the Ideal. Fourth ed.* Cambridge University Press, 2010.
149. Booth, Ken. „Security and Emancipation". *Review of International Studies* 17, 4 (1991): 313-26.
150. Brown, Lester R. „Redefining National Security". *Worldwatch Paper* 14 (1977).
151. Carr, James, ir Patricia Bellia. *The Law of Electronic Surveillance*, 2017-2 Ed., 1 dalis. Clark Boardman Callaghan, 2017.
152. Carter, Ashton B. „The Architecture of Government in the Face of Terrorism", *International Security* 26, 3 (2001/2002): 5-23.
153. Charns, Alexander. „Cloak and Gavel: FBI Wiretaps, Bugs, Informers, and the Supreme Court" 23 (1992).

154. Christou, George. „The Collective Securitisation of Cyberspace in the European Union“. *West European Politics* 42, 2 (2019): 278-301.
155. Civilka, Mindaugas, ir Lina Šlapimaitė. „Asmens duomenų samprata elektroninėje erdvėje“. *Teisė* 96 (2015): 126-148.
156. Clinton, William. *A National Security Strategy for a New Century*. 1999.
157. De Busser, Els. „EU Data Protection in Transatlantic Cooperation in Criminal Matters Will the EU Be Serving Its Citizens an American Meal?”. *Utrecht Law Review* 6, 1 (2010): 86-100.
158. Dešriūtė, Justina. „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“. *Teisės problemos* 1, 91 (2016): 25-51.
159. Dinh, Viet D., ir Wendy J. Keefer. „FISA and the Patriot Act: A Look Back and a Look Forward Note“. *Annual Review of Criminal Procedure* 35 (2006): iii–xxxiv.
160. Emiliou, Nicholas. *The Principle of Proportionality in European Law: A Comparative Study.* London: Kluwer Law International, 1996.
161. Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Springer, 2013.
162. Glendon, Mary Ann, Michael W. Gordon, ir Christopher Osakwe. *Vakarų Teisės Tradicijos*. Vilnius: Pradai, 1993.
163. Goda, Gintaras. „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys“. *Teisė* (2000): 17-27.
164. Goda, Gintaras. *Vertybiniai prioritetai baudžiamajame procese: monografija*. Vilnius: Registrų centras, 2014.
165. Gray, David C., ir Stephen E. Henderson. *The Cambridge Handbook of Surveillance Law*. Cambridge University Press, 2017.
166. Granger, Marrie-Pierre, ir Kristina Irion. „The Court of Justice and the Data Retention Directive in *Digital Rights Ireland*: telling off the EU legislator and teaching a lesson in privacy and data protection“. *European Law Review* 39, 6 (2014): 835-850.
167. Gutauskas, Aurelijus. „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas“. *Teisė* 113 (2019): 8–26. doi:10.15388/Teise.2019.113.1.
168. Halbert, Debora, ir Stefan Larsson. „By Policy or Design? Privacy in the US in a

Post-Snowden World“. *Journal of Law, Technology and Public Policy* 1, 2 (2015): 1-17.

169. Hamilton, Daniel S., ir Joseph P. Quinlan. *The Transatlantic Economy 2020: Annual Survey Of Jobs, Trade And Investment Between The United States And Europe*. 2020.
170. Heisbourg, Francois. „American Hegemony? Perceptions of the U.S.Abroad“. *Survival* 41, 4 (1999-2000): 5-19.
171. Helmholz, R. H. „Continental Law and Common Law: Historical Strangers or Companions?”. *Duke Law Journal* 1990, 6 (1990): 1207-1228.
172. Hillebrand, Claudia. „Counter-Terrorism Networks in the European Union: Maintaining Democratic Legitimacy After 9/11“. *Terrorism and Political Violence* 26, 4 (2014): 727-28.
173. James Carr ir Patricia Bellia, The Law of Electronic Surveillance, 2017-2 Ed., 1 dalis, (Clark Boardman Callaghan, 2017).
174. Johnson, Chalmer A. *Blowback: The Costs and Consequences of American Empire*. New York: Metropolitan, 2000.
175. Kiškis, Mindaugas, Rimantas Petrauskas, Irmantas Rotomskis, ir Darius Štitilis. *Teisės informatika ir informatikos teisė: vadovėlis*. Vilnius: Mykolo Romerio universitetas, 2006.
176. Kiškis, Mindaugas. „Intelektinės Nuosavybės Elektroninėje Erdvėje Ypatumai Ir Teisinis Reglamentavimas“, *Teisė* 71. Vilnius: Vilniaus Universiteto Leidykla, 2009.
177. Kokott, Juliane, ir Christoph Sobotta. „The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR“. *International Data Privacy Law* 3, 4 (2013).
178. Lam, Christina. „Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner“. *Boston College International and Comparative Law Review* 40, 3 (2017): 1-13.
179. Lenaerts, Koen. „Limits on Limitations: The Essence of Fundamental Rights in the EU”. *German Law Journal* 20, 6 (2019): 779–93. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.cambridge.org/core/journals/german-law-journal/article/limits-on-limitations-the-essence-of-fundamental-rights-in-the-eu/3071D1A8FB881031F8E3F6D5799959BD.
180. Lyon, David. „Surveillance after Snowden“. *European Journal of Communication* 31, 3 (2016): 366-67.

181. Lyon, David. „Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique“. *Big Data & Society* 1, 2 (2014): 205395171454186.
182. M.Walt, Stephen. „Beyond bin Laden: Reshaping U.S. Foreign Policy“. *International Security* 26, 3 (Winter 2001/2002): 56-78.
183. Machovenko, Jevgenij. *Teisės Istorija: Vadovėlis*. Vilnius: Registrų Centras, 2013.
184. Macnish, Kevin. „Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World“. *Journal of Applied Philosophy* 35, 2 (2016): 417-32.
185. Matthews, Jessica Tuchman. „Redefining Security“. *Foreign Affairs* 68, 2 (1989): 162-77.
186. McLeod, Douglas M, ir Dhavan V Shah. „News Frames and National Security“. *Communication, Society and Politics*. Cambridge University Press, 2014.
187. Miller, Russell A. *Privacy and Power*. Cambridge: Cambridge University Press, 2017.
188. Misiūnaitė-Kamarauskienė, Dalia. „Europos Sąjungos Teisingumo Teismo praktikos aktualijos pagrindinių teisių į privatų ir šeimos gyvenimą bei asmens duomenų apsaugą srityje”. *Jurisprudencija* 21, 4 (2014): 1233-1245.
189. Murphy, Maria Helen. „The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe?“. *Information & Communications Technology Law* 23, 3 (2014): 192-219.
190. Nacionalinė saugumo komisija. *Transforming Defense: National Security in the 21st Century*. 1997.
191. Ni Loideain, Nora. „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era“. *Media and Communication (Lisboa)* 3, 2 (2015): 53-62.
192. Ntouvas, Ioannis. „Exporting Personal Data to EU-based International Organizations under the GDPR” *International Data Privacy Law* 9, 4 (2019).
193. O'Reilly, Kenneth. „A New Deal for the FBI: The Roosevelt Administration, Crime Control, and National Security“. *The Journal of American History* 69, 3 (1982): 639-658.
194. Ott, Nikolas, ir Hugo Zylberberg. „A European Perspective on the Protection of Personal Data in Cyberspace: Explaining How the European Union Is Redefining Ownership and Policies of Personal Data beyond National Borders“. *Kennedy School Review* 16 (2016): 69-75.
195. Pakutinskas, Paulius. „Elektroninių Komunikacijų Teisinio Reguliavimo Modeliai“. Daktaro disertacija, Mykolo Romerio Universitetas, 2009. Prieiga per ELABa

– Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.
196. Parsons, Sarah. „Sources and Methods for Cryptologic History: NSA.gov - a Tour through Its History and Resources“. *Cryptologia* 44, 4 (2020): 371-382.
197. Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage* 35 (2002).
198. Peterson, John, ir Hugh Ward. „Coalitional Instability and the New Multidimensional Politics of Security: A Rational Choice Argument for US-EU Cooperation“. *European Journal of International Relations* 1 (1995): 131-56.
199. Petraitytė, Ilona. „Asmens Duomenų Apsauga Ir Teisė į Privatų Gyvenimą“. *Teisė* 80 (2011): 163-74.
200. Petraitytė, Ilona. „Asmens Duomenų Teisinės Apsaugos Principai“. Daktaro disertacija, Vilniaus Universitetas, 2013. Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.
201. Petrauskaitė, Audronė, ir Laurynas Šaltenis. „Žvalgybos Veiklos Ir Etikos Sąveika Nacionalinio Saugumo Kontekste: Teorinė Problemos Apžvalga“. *Lietuvos Metinė Strateginė Apžvalga* 16, 2017-2018 (2018): 393-414.
202. Posen, Barry R. „The Struggle Against Terrorism: Grand Strategy, Strategy, and Tactics“. *International Security* 26, 3 (Winter 2001/2002): 39-55.
203. Posen, Barry R., ir Andrew L. Ross. „Competing Visions for U.S. Grand Strategy“. *International Security* 21, 3 (1996/97): 5-53.
204. Possler, Daniel, Sophie Bruns, ir Julia Niemann-Lenz. „Data Is the New Oil--But How Do We Drill It? Pathways to Access and Acquire Large Data Sets in Communication Science.“. *International Journal of Communication*, 2019. Žiūrėta 2021 m. kovo 16 d. https://ijoc.org/index.php/ijoc/article/download/10737/2763.
205. Pranevičienė, Birutė. „Limiting of the Right to Privacy in the Context of Protection of National Security“. *Jurisprudencija* 18, 4 (2011): 1609-1622.
206. Preibusch, Sören. „Privacy Behaviors after Snowden“. *Communications of the ACM* 58, 5 (2015): 48-55.
207. Price, Michael W. „Rethinking Privacy: Fourth Amendment"Papers"and the Third Party Doctrine“. *J. Nat ' l Security L. & Pol ' Y* 8, 2 (2016): 247-300.
208. Pujol, Jordi. „Is This the End of Privacy? Snowden and the Power of Conscience“. *Church, Communication and Culture* 5, 1 (2020): 140-44.
209. Ratai, Balazs. „Understanding Lessig: Implications for European Union Cyberspace Policy“. *International Review of Law, Computers & Technology* 19, 3 (2005).

210. Raz, Joseph. *The Concept of a Legal System: An Introduction to the Theory of Legal System. 2nd ed.* Oxford: Clarendon Press, 2003.
211. Rice, Condolezza. „Promoting the National Interest". *Foreign Affairs* 79, 1 (2002): 45-62.
212. Roberts, Andrew. „Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications". *Modern Law Review* 78, 3 (2015): 535-48.
213. Rodman, Peter W. „The World's Resentment: Anti-Americanism as a Global Phenomenon". *National Interest* 60 (2000): 33-41.
214. Romm, Joseph J. *Defining National Security*. New York: Council on Foreign Relations, 1993.
215. Rotenberg, Marc. „*Schrems II*, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection". *European Law Journal : Review of European Law in Context* 26, 1-2 (2020): 141-152;
216. Rudgers, David. „The Church Committee on Intelligence Activities Investigation, 1975 – 76". Iš *Congress Investigates: A Critical and Documentary History*, Roger A. Burns, David L. Hostetter, Raymond W. Smock. New York: Facts on File, 2011.
217. Sarat, Austin. *A World without Privacy*. New York: Cambridge University Press, 2014.
218. Sauter, Wolf. „Proportionality in EU Law: A Balancing Act?". *TILEC Discussion Paper No. 2013-003*. 2013.
219. Schwartz, Bernard. *The Bill of Rights: A Documentary History* 1 (1971).
220. Schwartz, Paul M. „Global Data Privacy: The E.U. Way". *New York University Law Review* 94, 4 (2019): 771-818.
221. Schwartze, Jurgem. *European administrative law: Revised First Edition* London: Sweet&Maxwell, 2006.
222. Scott, Mark, ir Lauren Cerulus. „Europe's New Data Protection Rules Export Privacy Standards Worldwide". *Politico*. 2018.
223. Seiple, Chris. „Homeland Security Concepts and Strategy". *Orbis* 46, 2 (2002): 264-65.
224. Setty, Sudha N. National Security Secrecy: Comparative Effects on Democracy and the Rule of Law. *Cambridge University Press*, 2017.
225. Shaw, Martin. „There Is No Such Thing as Society: Beyond Individualism and Statism in International Security Studies". *Review of International Studies* 19, 2

(1993): 159-75.
226. Solove, Daniel J. *Understanding Privacy.* Harvard University Press, 2009.
227. Stankevičiūtė, Sigutė. „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas". Daktaro disertacija, Mykolo Romerio Universitetas, 2020. Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.
228. Stern, Simon, "The Third-Party Doctrine and the Third Person" *New Criminal Law Review* 16, 3 (2013).
229. Sury, Ursula. „Die Auswirkungen Des EuGH-Urteils C-311/18 "*Schrems*-II" Auf Den Datenaustausch Mit Den USA". *Informatik-Spektrum* 43, 5 (2020): 354-355.
230. Svantesson, Dan Jerker B., ir Dariusz Kloza. *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*. Intersentia, 2017.
231. *Štitilis, Darius, Inga Dauparaitė, Paulius Pakutinskas, ir Marius Laurinaitis.* „Asmens Identifikavimo Fizinėje Ir Elektroninėje Erdvėje Teisinio Reguliavimo Prielaidos". *Jurisprudencija* 18, 2 (2011): 703-24.
232. Štitilis, Darius, ir Marius Laurinaitis. „IP telefonija - iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui". *Socialinių mokslų studijos* 1 (2009): 205–221.
233. *Štitilis, Darius, ir Marius Laurinaitis. „Tapatybės Vagystė Elektroninėje Erdvėje». Informacijos Mokslai* 50 (2009).
234. Tarasevičius, Petras. „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos". *Teisė* (2017): 84–99. doi:10.15388/Teise.2017.105.11114.
235. Tetley, William. „Mixed Jurisdictions: Common Law v. Civil Law (Codified and Uncodified)". *Louisiana Law Review* 60, 3 (2000): 678-738.
236. The United States Commission on National Security/21st Century. „New World Coming: American Security in the 21st Century". *The Phase 1 Report on the Emerging Global Security Environment for the First Quarter of the 21st Century*. 1999.
237. The United States Commission on National Security/21st Century. „Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom". The Phase *II Report on a U.S. National Security Strategy for the 21st Century*. 2000.
238. Tickner, J. Ann, „Re-visioning Security". Iš, *International Relations Theory Today*, Ken Booth ir Steve Smith. Oxford, 1995.
239. Tracol, Xavier. „*Schrems II*": The Return of the Privacy Shield". *The Computer Law and Security Report 39 (2020): The Computer Law and Security Report* 39 (2020)

105484.
240. Tranberg, C.B. „Proportionality and Data Protection in the Case Law of the European Court of Justice“. *International Data Privacy Law* 1, 4 (2011): 239-48.
241. Tridimas, Takis. *The General Principles of EU Law, 2nd ed.* Oxford: Oxford University Press, 2006.
242. Tromblay, Darren E. „The U.S. Domestic Intelligence Enterprise: History, Development, and Operations“ 15 (2015).
243. Ullman, Richard H. „Redefining Security“. *International Security* 81, 1 (1983): 129-53.
244. Unger, David C. „The Emergency State: America's Pursuit of Absolute Security at All Costs“ 41 (2013).
245. Vėlyvis, Stasys, ir Marius Jonaitis. „XII lentelių įstatymai:Bendrųjų šiuolaikinės teisės principų pradmenys“. *Jurisprudencija* 101, 11 (2007): 33-41.
246. Waranch, Rubin S. „*Digital Rights Ireland* Deja Vu? Why The Bulk Acquisition Warrant Provisions Of The Investigatory Powers Act 2016 Are Incompatible With The Charter Of Fundamental Rights Of European Union”. *The George Washington International Law Review* 50, 1 (2017): 209.
247. Warren, Samuel D., ir Louis D. Brandeis. „The Right to Privacy“. *Harvard Law Review* 4, 5 (1890): 193– 220. doi:10.2307/1321160.
248. Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.
249. Whitman, James Q. „The Two Western Cultures of Privacy: Dignity versus Liberty”. *The Yale Law Journal* 113, 6 (2004): 1151-1222.
250. Wolfrum, R. Rüdiger (ed.). *Max Planck Encyclopedia of Public International Law.* Oxford: Oxford University Press, 2007.
251. Zaleskis, Julius. *Europos Sąjungos Bendrasis Duomenų Apsaugos Reglamentas Ir Asmens Duomenų Apsaugos Teisė: Monografija*. Vilnius: Registrų Centras, 2019.
252. Zekos, Georgios I. „Cyberspace and IPRs Stimulus on Foreign Direct Investment in the European Union“. *Journal of Internet Law* 20, 6 (2016).
253. Zygmunt Bauman et al., 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8(2) *International Political Sociology* 122.
254. Zweigert, Konrad, ir Hein Kötz. *Lyginamosios Teisės įvadas.* Vilnius: Eugrimas, 2001.
255. Žalimienė, Skirgailė. *Europos Sąjungos Pagrindinių Teisių Chartijos, Kaip Individualių Teisių Gynybos Standarto, Taikymas Supra- Ir Nacionaliniu Lygmenimis:*

*Kolektyvinė Monografija*. Vilnius: Vilniaus Universiteto Leidykla, 2019.

**Kiti šaltiniai**

256. „Bendras industrijos laiškas dėl *Schrems II* sprendimo“. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.itic.org/policy/JointIndustryLetter*Schrems*II-30July.pdf.
257. „EU Top Court Sides with Consumer Privacy in EU–US Data Shambles“. BEUC. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.beuc.eu/publications/eu-top-court-sides-consumer-privacy-eu-us-data-shambles/html.
258. „EU Top Court Sides with Consumer Privacy in EU–US Data Shambles“. BEUC. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.beuc.eu/publications/eu-top-court-sides-consumer-privacy-eu-us-data-shambles/html.
259. „EU Top Court Sides with Consumer Privacy in EU–US Data Shambles“. BEUC. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.beuc.eu/publications/eu-top-court-sides-consumer-privacy-eu-us-data-shambles/html.
260. „Europos Komisijos ataskaita dėl viešos konsultacijos apie e-privatumo direktyvos įvertinimą ir peržiūrą“. European Commission. Žiūrėta 2021 m. rugpjūčio 11 d. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40777.
261. „Europos teisingumo komisaro Didier Reynders ir JAV prekybos sekretoriaus Wilbur Ross pranešimas spaudai“. Europos Komisija. Žiūrėta 2021 m. rugpjūčio 2 d. https://ec.europa.eu/newsroom/just/items/684836.
262. „JAV Cornell universiteto mokomoji medžiaga“. Žiūrėta 2021 m. rugpjūčio 4 d. https://www.law.cornell.edu/wex/legal_systems.
263. „Palmer Raids“. FBI. Žiūrėta 2021 m. liepos 4 d. https://www.fbi.gov/history/famous-cases/palmer-raids.
264. „Pasaulio turtingiausių asmenų sąrašas“. Žiūrėta 2021 m. kovo 16 d. https://www.forbes.com/real-time-billionaires/#1dcf6c0b3d78.
265. „Schrems II: Initial Reactions – Solove, Antonipillai, Zanfir-Fortuna, Sauer, Litt“. Žiūrėta 2021 m. kovo 16 d. https://www.youtube.com/watch?v=irZHx7CI5K0.
266. „The Bill of Rights“ A Transcription“. National Archives. Žiūrėta 2021 m. liepos 4 d. https://www.archives.gov/founding-docs/bill-of-rights-transcript.
267. Baker, Stewart. „How Can the US Respond to Schrems II?“. *LAWFARE*. Ži**ūrėta 2021 m. rugpjūčio 2 d.** https://www.lawfareblog.com/how-can-us-respond-*Schrems*-ii.
268. Baker, Stewart. „The Cyberlaw Podcast: Solipsistic Europocrisy Meets Judicial

Imperialism“. *LAWFARE*. Žiūrėta 2021 m. gegužės 10 d. https://www.lawfareblog.com/cyberlaw-podcast-solipsistic-europocrisy-meets-judicial-imperialism.
269. Bernstein, Carl, ir Woodward, Bob. „FBI Finds Nixon Aides Sabotaged Democrats“. *Washington Post*. 1972 m. spalio 10 d., A01. Žiūrėta 2021 m. liepos 5 d. https://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/101072-1.htm.
270. Bignami, Francesca. „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens“. European Parliament. Žiūrėta 2020 m. rugsėjo 10 d. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.
271. Connolly, Chris. „The US Safe Harbor – Fact or Fiction?“. *Galexia*. 2008. Žiūrėta 2021 m. rugpjūčio 3 d. https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.
272. Hersh, Seymour M. „Huge C.I.A. Operation Reported in U.S. against Antiwar Forces, Other Dissidents in Nixon Years“. *The New York Times*. 1974 m. gruodžio 22 d. Žiūrėta 2021 m. liepos 5 d. https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html.
273. Kerry, Cameron F. „One year after Schrems II, the world is still waiting for U.S. privacy legislation“. Žiūrėta 2021 m. rugpjūčio 30 d. https://www.brookings.edu/blog/techtank/2021/08/16/one-year-after-schrems-ii-the-world-is-still-waiting-for-u-s-privacy-legislation/.
274. Lomas, Natasha. „Max Schrems on the EU court ruling that could cut Facebook in two“. Techcrunch. Žiūrėta 2021 m. kovo 16 d. https://techcrunch.com/2020/08/25/max-*Schrems*-on-the-eu-court-ruling-that-could-cut-facebook-in-two/.
275. Propp, Kenneth, ir Peter Swire. „After Schrems II: A Proposal to Meet the Individual Redress Challenge“. *LAWFARE*. Žiūrėta 2021 m. rugpjūčio 2 d. https://www.lawfareblog.com/after-*Schrems*-ii-proposal-meet-individual-redress-challenge.
276. Teisinis tinklaraštis *TeachPrivacy.* Žiūrėta 2021 m. rugpjūčio 2 d. (https://www.youtube.com/channel/UCqODltywqZCuxprcz72kc-Q)
277. Turner, Serrin, ir Stephen J. Schulhofer. *The Secrecy Problem in Terrorism Trials. Brennan Center for Justice*. 2005. Žiūrėta 2021 m. kovo 30 d. https://www.brennancenter.org/sites/default/files/legacy/publications/20050000.TheSecrecyProbleminTerrorismTrials.pdf.
278. Weiler, Joseph. „Vedamasis straipsnis“. *EJIL Talk* 19, 5 (2009). Žiūrėta 2021 m. kovo 16 d. https://www.ejiltalk.org/letters-to-the-editor-respond-to-ejil-editorials-vol-195/.

MYKOLO ROMERIO UNIVERSITETAS

**Edgaras Markevičius**

# ASMENS DUOMENŲ PERDAVIMO ELEKTRONINĖJE ERDVĖJE TARP EUROPOS SĄJUNGOS IR JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINĖS PROBLEMOS

Daktaro disertacijos santrauka
Socialiniai mokslai, teisė (S 001)

Vilnius, 2022

Daktaro disertacija rengta 2015–2021 metais Mykolo Romerio universitete, ginama Mykolo Romerio universitete pagal Mykolo Romerio universitetui ir Vytauto Didžiojo universitetui Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

*Mokslinis vadovas:*
prof. dr. Darijus Beinoravičius (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Mokslo daktaro disertacija ginama Mykolo Romerio universiteto ir Vytauto Didžiojo universiteto teisės mokslo krypties taryboje:

*Pirmininkė:*
prof. dr. Toma Birmontienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

*Nariai:*
prof. dr. Vida Davidavičienė (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Aurelijus Gutauskas (Vilniaus universitetas, socialiniai mokslai, teisė, S 001);
habil. dr. Dorota Lis-Staranowicz (Varmijos Mozūrų universitetas Olštyne, Lenkijos Respublika, socialiniai mokslai, teisė, S 001);
doc. dr. Juozas Valčiukas (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Daktaro disertacija bus ginama viešame Teisės mokslo krypties tarybos posėdyje 2022 m. rugsėjo 5 d. 14 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, 08303 Vilnius.

Daktaro disertacijos santrauka išsiųsta 2022 m. rugpjūčio 5 d.

Daktaro disertaciją galima peržiūrėti Lietuvos nacionalinėje Martyno Mažvydo bibliotekoje (Gedimino pr. 51, Vilnius), Mykolo Romerio universiteto bibliotekoje (Ateities g. 20, Vilnius) ir Vytauto Didžiojo universiteto bibliotekoje (K. Donelaičio g. 52, Kaunas).

**Edgaras Markevičius**

# ASMENS DUOMENŲ PERDAVIMO ELEKTRONINĖJE ERDVĖJE TARP EUROPOS SĄJUNGOS IR JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINĖS PROBLEMOS

## SANTRAUKA

**Temos aktualumas**. Pastarieji dešimtmečiai pasižymėjo itin sparčia technologijų pažanga, kuri pakeitė daugybę kasdienio gyvenimo sričių. Viena iš labiausiai paveiktų sričių apima asmenų socialinį gyvenimą – bendro darbo, tarpusavio bendravimo priemones ir įpročius. Šiuo metu tapo įprasta rengti ne *gyvus* sutikimus, o telekonferencijas; skambinti nebe GSM ryšiu, o susisiekti videoryšiu (pvz., programėlių *Viber, Messenger, FaceTime* pagalba) ir pan.

Ši technologijų pažanga lemia vis didėjantį asmenų, įmonių ir organizacijų elektroninių ryšių tinklų ir debesų technologijų naudojimą paslaugoms teikti, įrašams kaupti ir tvarkyti būtent elektroninėje erdvėje. Vis platesnis šių ryšių naudojimas suteikia beprecedentę galimybę sistemingai rinkti ir naudoti įvairius duomenis (tame tarpe ir asmens duomenis) skirtingiems tikslams. Technologijų pagalba kaupiama bei apdorojama informacija ir duomenys naudojami ne tik fizinių ir juridinių asmenų poreikių patenkinimo tikslais, tačiau ir įvairiais kitais tikslais.

Itin plačiai paplitusio asmens duomenų kaupimo ir naudojimo kontekste teisine prasme probleminis tampa asmens teisės į privatų gyvenimą užtikrinimas. Nors asmenims ir yra laiduojama teisė į privatumą, tačiau negalima ignoruoti kitų interesų, kurių patenkinimui šie duomenys gali būti naudojami. Šie interesai apima tiek privačius, tiek visuomeninius prioritetus – sunkių nusikaltimų (pavyzdžiui, terorizmo, narkotikų gamybos ir gabenimo, prekybos žmonėmis etc.) prevenciją ir ikiteisminio tyrimo vykdymą, valstybių nacionalinio saugumo užtikrinimą, viešojo administravimo paslaugų teikimą elektroninėmis priemonėmis etc.

Teisinės analizės prasme sudėtingas klausimas visuomet yra susijęs su dviejų interesų – asmens teisės į privatumą bei visuomenės kolektyvinio saugumo intereso

– konkurencija bei proporcingo šių interesų balanso nustatymu. Šis klausimas tampa dar sudėtingesniu, kai privatumo apsaugą reikia derinti ne tik konkuruojančių interesų atžvilgiu, tačiau ir tarp skirtingų teisinių sistemų, kuriose tiek privatumo, tiek visuomenės kolektyvinis saugumo interesai yra suprantami ir aiškinami skirtingai.

Europos Sąjungoje teisė į privatumą ir asmens duomenų apsaugą yra saugoma Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 str. nuostatomis bei BDAR reguliavimu. Kadangi teisė į privatumą ir asmens duomenų apsaugą yra laiduojama visiems asmenims, Europos Sąjunga turi užtikrinti, kad šios teisės būtų įgyvendinamos tvarkant asmens duomenis ne tik jos teritorijoje, bet ir perduodant už jos ribų.

Transatlantiniai duomenų srautai tarp Europos Sąjungos ir JAV yra greičiausi ir didžiausi pasaulyje, bei sudaro daugiau nei pusę Europos duomenų srautų ir apie pusę JAV duomenų srautų, todėl JAV ir Europos Sąjunga yra ne tik vienos didžiausių rinkų, bet ir svarbiausios komercinės partnerės skaitmeninių paslaugų srityje[498]. Dėl to teisine ir faktine prasme aktualiausios teisės į privatumą apsaugos problemos kyla iš asmens duomenų perdavimo būtent tarp Europos Sąjungos ir JAV teisinių sistemų.

Teisės į privatumą apsaugos apimties klausimas, jį derinant su valstybės nacionalinio saugumo ar nusikaltimų prevencijos interesais, nėra lengvai nustatomas net ir vienos teisinės sistemos kontekste. Tai patvirtina daugybė ginčų ir didelio atgarsio sulaukę sprendimai, kuriuos priėmė Europos Sąjungos Teisingumo Teismas nagrinėdamas bylas dėl Europos Sąjungos pagrindinių teisių chartijos taikymo, Europos Žmogaus Teisių Teismas – dėl Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos taikymo teisės į privatumą ir asmens duomenų apsaugą srityse.

Autoriaus vertinimu, ši teisės į privatumą apsaugos apimties nustatymo užduotis reikšmingai pasunkėja, kai jį būtina suderinti ne vienos, o kelių teisinių sistemų atžvilgiu. Teisės į privatumą apsauga pagal Europos Sąjungos iškeltą aukštą apsaugos standartą yra sudėtingai suderinama su JAV teisine sistema bei privatumo samprata joje, pirmiausiai, dėl pamatinių JAV teisinės sistemos skirtumų su Europos Sąjungos teisine sistema. Pavyzdžiui, JAV teisėje taikoma trečiosios šalies doktrina[499], pagal kurią, fiziniai asmenys neturi pagrįsto intereso į teisės į privatumą apsaugą tų duomenų atžvilgiu, kuriuos valdo ne jie patys, o tretieji asmenys (pavyzdžiui, bankai, elektroninių ryšių paslaugų teikėjai ir pan.). Todėl JAV teisėsaugos ar žvalgybos institucijos gali

[498] Daniel S. Hamilton ir Joseph P. Quinlan, *The Transatlantic Economy 2020: Annual Survey Of Jobs, Trade And Investment Between The United States And Europe* (2020), 8.

[499] Simon Stern, „The Third-Party Doctrine and the Third Person", *New Criminal Law Review* 16, 3 (2013): 101.

gauti šiuos duomenis iš esmės netaikant jokių apsaugos priemonių. Taip pat, pagal JAV Aukščiausiojo Teismo *Clapper* byloje suformuotą praktiką, asmenys negali kreiptis į teismą dėl privatumo apsaugos, jei jie negali įrodyti, kad stebėjimas jų atžvilgiu buvo taikytas[500]. Atsižvelgiant į tai, kad stebėjimo priemonės taikomos slaptai, apie tai nepranešant asmenims (kurių atžvilgiu jos yra taikomos), toks suformuotas precedentas padarė reikšmingą neigiamą poveikį asmenų galimybei ginti savo pažeidžiamas teises.

Be reikšmingų pamatinių požiūrio į teisės į privatumą apimties ir teisinių sistemų skirtumų tarp Europos Sąjungos ir JAV, svarbūs ir kiti veiksniai, susiję su faktine teisės į privatumą apsaugą JAV. JAV prezidentų Bušo ir Obamos administracijos vykdė prieštaringas nacionalinio saugumo programas, įskaitant tikslinių nužudymų, kankinimų ir asmenų stebėjimo srityse, kurių slaptumas atėmė iš visuomenės galimybę sužinoti tuos veiksmus ir taikomas priemones[501]. Dalį šių taikomų priemonių, jų taikymo mąstą ir reikšmę 2013 m. atskleidė pranešėjas (angl. *whistle blower*) Edvardas Snoudenas[502], tokiais savo veiksmais pasėjęs nepasitikėjimo sėklą privatumo apsauga JAV teisinėje sistemoje ir faktiškai taikomų stebėjimo priemonių teisėtumu. Šį nepasitikėjimo aspektą puikiai iliustruoja ir Lietuvos teisės doktrinoje pateikiami kritiniai privatumo apsaugos JAV teisinėje sistemoje vertinimai, kad „JAV vykdomas masinis asmens duomenų rinkimas elektroninėje erdvėje yra analogiškas XIII a. galiojusiai antikonstitucine pripažintai teisei Karūnos įgaliotiems asmenims bent kada įsibrauti į bent kurio iš Didžiosios Britanijos valdose esančio asmens namus“[503].

Šios teisinės sistemos sąveikauja, kai asmens duomenys yra perduodami tarp skirtingų subjektų, priklausančių šioms teisinėms sistemoms. Asmens duomenų perdavimas iš Europos Sąjungos subjektams į trečiąsias šalis reguliuojamas BDAR V skyriuje. Jame prioriteto tvarka yra įtvirtinti skirtingi asmens duomenų perdavimo pagrindai iš Europos Sąjungos į trečiąsias šalis (ar tarptautinėms organizacijoms): Europos Komisijos sprendimas dėl tinkamumo, duomenų valdytojo ar tvarkytojo taikomos tinkamos apsaugos priemonės, nukrypti leidžiančios nuostatos. Visi šie duomenų perdavimo pagrindai taikomi siekiant to paties tikslo – užtikrinti, kad nebūtų

[500] „Clapper v. Amnesty International“, CaseText, žiūrėta 2021 m. rugpjūčio 5 d., https://casetext.com/case/clapper-v-amnesty-intl-usa-7.

[501] Sudha N. Setty, *National Security Secrecy: Comparative Effects on Democracy and the Rule of Law* (Cambridge University Press, 2017), 3.

[502] Jordi Pujol, „Is This the End of Privacy? Snowden and the Power of Conscience“, *Church, Communication and Culture* 5, 1 (2020): 140-44.

[503] Sigutė Stankevičiūtė, „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas“ (daktaro disertacija, Mykolo Romerio Universitetas, 2020), 113 psl., prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka: 9.

pakenkta BDAR garantuojamam fizinių asmenų apsaugos lygiui.

Kadangi JAV yra trečioji šalis, remiantis BDAR 45 str. teisiniu reguliavimu, paprasčiausias bei palankiausias sprendimas sureguliuoti asmens duomenų perdavimą tarp Europos Sąjungos ir JAV yra Europos Komisijos sprendimas dėl trečiojoje šalyje (t. y. JAV) užtikrinamos tinkamo lygio privatumo apsaugos.

Europos Komisija tokį sprendimą JAV atžvilgiu (t. y. *Safe Harbour* susitarimą) priėmė 2000-aisiais metais. Dėl Edvardo Snoudeno 2013 m. atskleistų JAV vykdomų stebėjimo programų kilo ne tik daug pasipiktinimo, tačiau ir teisinių ginčų. *Safe Harbour* susitarimo teisėtumą ir pagrįstumą 2015 m. vertino Europos Sąjungos Teisingumo Teismas ir jį panaikino[504].

Europos Sąjungos Teisingumo Teismui panaikinus *Safe Harbour* susitarimą, skubiai buvo pradėtos derybos dėl galimo naujo susitarimo sudarymo, kurios baigėsi sėkmingai, 2016 m. sudarius *Privacy Shield* susitarimą. Tačiau laikas parodė, jog *Privacy Shield* susitarimas taip pat turėjo reikšmingų trūkumų, nes Europos Sąjungos Teisingumo Teismas 2020 m. jį taip pat panaikino, kaip neužtikrinantį adekvačios teisės į privatumą apsaugos JAV teisinėje sistemoje[505].

Tokiu būdu, atsižvelgiant į kategoriškas Europos Sąjungos Teisingumo Teismo padarytas išvadas apie teisės į privatumą apsaugos JAV teisinėje sistemoje nepakankamumą, lyginant su Europos Sąjungos teisinėje sistemoje garantuojamu privatumo apsaugos lygiu, vėl atsirado teisinis neapibrėžtumas dėl asmens duomenų perdavimo teisinio pagrindų taikymo. Minėto Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje reikšmė yra itin didelė, kadangi joje yra konstatuojami pamatiniai privautmo apsaugos JAV teisinėje sistemoje trūkumai, kurių, autoriaus vertinimu, duomenų valdytojai ar tvarkytojai negali ištaisyti. Tai yra trūkumai, susiję su teisėsaugos institucijų prieiga prie JAV tvarkomų asmens duomenų. Todėl naudojimasis kitu BDAR V skyriuje įtvirtintu asmens duomenų perdavimo teisiniu pagrindu, tikėtina, siekiant perduoti duomenis iš Europos Sąjungos į JAV taip pat yra negalimas, nes bendras asmens duomenų perdavimo principas bei tikslas (užtikrinti, kad nebūtų pakenkta BDAR garantuojamam fizinių asmenų apsaugos lygiui) negalės būti įgyvendintas dėl

---

[504] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems“, InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3390590.

[505] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II“)“, InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=8508220193825AFC3D98FABEA15645EC?text=&docid=228677&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3350436.

konstatuotų JAV teisinės sistemos asmens duomenų apsaugos trūkumų.

Kitas Europos Sąjungos Teisingumo Teismo sprendime konstatuotas, tačiau iš esmės neplėtotas argumentas yra tas, kad išimtis dėl BDAR netaikymo, siejant su valstybių narių nacionalinio saugumo interesų apsauga, netaikoma trečiųjų šalių atžvilgiu. T. y. priešingai nei Europos Sąjungos valstybės narės, trečiosios šalys (įskaitant ir JAV), su kuriais sudaromi duomenų perdavimo susitarimai, privalo taikyti BDAR reguliavimą asmens duomenų, gaunamų iš Europos Sąjungos, tvarkymui, net kai jis atliekamas ir nacionalinio saugumo interesais. Ši Europos Sąjungos Teisingumo Teismo pozicija ne tik dėl asmens duomenų perdavimo besiderančius subjektus (pvz., Europos Sąjungą ir JAV) pastato į nelygiavertes pozicijas, tačiau ir sukuria reikšmingas kliūtis sėkmingam susitarimo dėl asmens duomenų perdavimo pasiekimui, nes trečiąją šalį *de facto* reikalauja atsisakyti savo nacionalinio saugumo apsaugos interesų įgyvendinimo iš Europos Sąjungos gaunamų asmens duomenų atžvilgiu.

Dėl nurodytų aplinkybių, šiame darbe siekiama išanalizuoti asmens duomenų perdavimo elektroninėje erdvėje problemas, sąveikaujant Europos Sąjungos ir JAV teisinėms sistemoms – galimų asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinių pagrindų sąlygas, atsižvelgiant į nacionalinio saugumo interesų apsaugą ir Europos Sąjungos Teisingumo Teismo suformuotą praktiką šiuo aspektu.

**Ištirtumas.** Bendrąja prasme, asmens teisė į privatumą yra populiari tema tiek tarp Lietuvos, tiek tarp užsienio teisės mokslininkų. Teisės doktrinoje teigiama, kad mokslininkų susidomėjimui asmens duomenų apsauga žvalgybos ir teisėsaugos srityje įtaką daro į viešumą nutekinama informacija apie asmens duomenų rinkimo mastus ir jų (ne)teisėtą panaudojimą[506]. Tokiai prielaidai turi būti pritariama, atsižvelgiant į teisinio reguliavimo ir teisės doktrinos pokytį asmens duomenų apsaugos srityje po Edvardo Snoudeno 2013 m. nutekintos informacijos apie JAV taikomas asmenų stebėjimo programas.

Viena iš populiarių teisės į privatumą tyrimo sričių buvo asmens santykis su valstybe asmens duomenų apsaugos srityje. Mokslininkai koncentravosi į Edvardo Snoudeno atskleistą informaciją apie valstybių taikomas stebėjimo priemones ir jų san-

[506] Stankevičiūtė, *supra note*, 6: 10.

tykį su teise į privatumą[507].

Kita populiari mokslinių tyrimų sritis atsivėrė po Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje, kuriuo buvo panaikintas *Safe Harbour* susitarimas. Tuomet teisės į privatumą apsaugos skirtingų teisės sistemų sąveikoje tema įgavo platesnį susidomėjimą. Pasirodė mokslininkų darbai apie duomenų perdavimo iš Europos Sąjungos į JAV galimybes ir teisėtumą[508].

Tarp šios srities tyrimų paminėtinos reikšmingi tyrimai, skirtos sisteminei asmens duomenų perdavimo tarp Europos Sąjungos ir JAV teisinei problematikai analizuoti[509]. Douglas M. Mcleod ir Dhavan V. Shah knygoje *News Frames and National Security. Covering Big Brother*[510] analizuojama įtampos tarp nacionalinio saugumo ir pilietinių laisvių įtampos prigimtis ir esmė. Ji padėjo tiksliau identifikuoti nacionalinio saugumo prigimtį, sampratą ir prasmę JAV teisinėje sistemoje. Svantesson, Dan Jerker B., ir Dariusz Kloza knygoje *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*[511] analizuojamas tarpvalstybinis duomenų srautų režimas, kuris grindžiamas Europos Sąjungos teisinio reguliavimo priemonėmis, tokiomis kaip BDAR, *Safe Harbour* ir daro įtaką kasdieniam duomenų apdorojimui abipus Atlanto bei kaip jie riboja duomenų operacijų apimtį. Ši knyga padėjo suprasti skirtingą Europos ir JAV teisės mokslininkų požiūrį į asmens duomenų perdavimo teisinį reguliavimą vadovaujantis *Safe Harbour* susitarimu, kuris neteko galios 2015 m. Patrick Birkinshaw knyga

[507] Zygmunt Bauman ir kt., „After Snowden: Rethinking the Impact of Surveillance“, *International Political Sociology* 8, 2 (2014): 122; Kevin Macnish, „Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World“, *Journal of Applied Philosophy* 35, 2 (2016): 417-32; Debora Halbert ir Stefan Larsson, „By Policy or Design? Privacy in the US in a Post-Snowden World“, *Journal of Law, Technology and Public Policy* 1, 2 (2015): 1; Sören Preibusch, „Privacy Behaviors after Snowden“, *Communications of the ACM* 58, 5 (2015): 48-55.; David Lyon, „Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique“, *Big Data & Society* 1, 2 (2014): 205395171454186; Nora Ni Loidean, „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era“, *Media and Communication (Lisboa)* 3, 2 (2015): 53-62.; Maria Helen Murphy, „The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe?“, *Information & Communications Technology Law* 23, 3 (2014): 192-219.

[508] Christina Lam, „Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner“, *Boston College International and Comparative Law Review* 40, 3 (2017): 1.

[509] David C. Gray ir Stephen E. Henderson, *The Cambridge Handbook of Surveillance Law* (Cambridge University Press, 2017); Dan Jerker B. Svantesson ir Dariusz Kloza. *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, 2017); Russell A. Miller, *Privacy and Power* (Cambridge: Cambridge University Press, 2017); Austin Sarat, *A World without Privacy* (New York: Cambridge University Press, 2014).

[510] Douglas M. McLeod ir Dhavan V Shah, „News Frames and National Security“, *Communication, Society and Politics* (Cambridge University Press, 2014).

[511] Dan Jerker B. Svantesson ir Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, 2017).

*Freedom of Information: The Law, the Practice, and the Ideal*[512] suteikė platesnę galimybę suprasti istorinį vyriausybių santykį su duomenų apsauga ir jų prigimtinį interesą prieigai prie asmens duomenų, kaip būtiną reikalavimą, užtikrinant visuomenės saugumą. James Carr ir Patricia Bellia knygoje *The Law of Electronic Surveillance*[513] apžvelgiamas teisinis JAV federalinio lygio asmens duomenų rinkimo el. erdvėje reglamentavimas. Ši knyga padėjo suprasti, kaip JAV teisinėje sistemoje veikia stebėjimo priemonių taikymo mechanizmas.

Tarp Lietuvos teisės mokslininkų teisės į privatumo apsaugą analizė taip pat laikytina populiaria tema. Tarp aktualių darbų pirmiausiai paminėtina šio tyrimo rengimo metu apginta S. Stankevičiūtės disertacija tema „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas“[514]. Joje mokslininkė analizuoja bendrosios ir kontinentinės teisės tradicijų šalių bei supranacionalinio lygmens asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo ypatumus dėl teisės į asmens duomenų apsaugą užtikrinimo. Šiame darbe, kaip ir apžvalginėje studijoje apie privatumo apsaugą JAV[515] bei aukščiau minėtose knygose, pateikiama detali JAV teisinio reguliavimo analizė apie asmens duomenų rinkimą teisėsaugos ir žvalgybos tikslais. Tačiau atsižvelgiant į šio tyrimo temą, joje nėra jokios analizės, nukreiptos į šių skritingų teisinių sistemų sąveikos problemas privatumo apsaugos kontekste bei galimus jų sprendimo būdus. Paulius Pakutinskas savo disertacijoje „Elektroninių komunikacijų teisinio reguliavimo modeliai“[516] analizavo elektroninių komunikacijų teisinio reguliavimo modelius, tačiau šio tyrimo atlikimui ji tiesiogiai nėra aktuali, nes joje taip pat neatskleidžiama skritingų teisinių sistemų sąveikos problema. Juliaus Zaleskio monografijoje „Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“[517] analizuojamas bendrasis BDAR teisinis reguliavimas kaip teisinės taisyklės, skirtos apsaugoti asmenis nuo pa-

---

512 Patrick Birkinshaw, *Freedom of Information: The Law, the Practice, and the Ideal. Fourth ed.* (Cambridge University Press, 2010).

513 James Carr ir Patricia Bellia, *The Law of Electronic Surveillance*, 2017-2 Ed., 1 dalis, (Clark Boardman Callaghan, 2017).

514 Stankevičiūtė, *supra note*, 6: 2 skyrius.

515 Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens“, European Parliament, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.

516 Paulius Pakutinskas, „Elektroninių Komunikacijų Teisinio Reguliavimo Modeliai“ (daktaro disertacija, Mykolo Romerio Universitetas, 2009), Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.

517 Julius Zaleskis, *Europos Sąjungos Bendrasis Duomenų Apsaugos Reglamentas Ir Asmens Duomenų Apsaugos Teisė: Monografija* (Vilnius: Registrų Centras, 2019).

vojų, kuriuos kelia duomenų tvarkymas. J. Zaleskio monografijoje aiškinamas BDAR reguliavimas, tačiau nėra analizuojama BDAR sąveikos su JAV teisine sistema problematika. Ilonos Petraitytės 2013 m. apgintoje disertacijoje[518] nagrinėti asmens duomenų apsaugos principai, tačiau ji prarado reikšmingą dalį aktualumo 2018 m., įsigaliojus BDAR ir iš esmės gali būti naudinga atliekant istorinę ir lyginamąją asmens duomenų apsaugos reguliavimo analizę.

Kita šiam tyrimui iš dalies aktuali Lietuvos mokslininkų analizuota asmens duomenų apsaugos teisės sritis, susijusi su teisės į privatumą ribojimais, atliekamais baudžiamojo persekiojimo metu (ikiteisminio tyrimo ar kriminalinės žvalgybos priemonių taikymo metu). Pirmiausiai šiuo aspektu paminėtinas Aurelijaus Gutausko mokslinis straipsnis, kuriame analizuojama Lietuvos Aukščiausiojo Teismo praktika, susijusi kriminalinės žvalgybos naudojamomis priemonės ir teisėtu jų skverbimusi į privatų žmogaus gyvenimą[519]. Jame pateikiamos įžvalgos, aktualios kriminalinės žvalgybos taikymo priemonių atveju, tačiau šio tyrimo objektas yra privatumo apsaugos problemos skritingų teisinių sistemų sąveikoje, ypač atsižvelgiant į aktualią problematiką dėl skirtingų valstybių nacionalinio saugumo interesų užtikrinimo. Susijusia tema pasisakė ir Rima Ažubalytė, kuri savo moksliniame straipsnyje analizavo Baudžiamojo proceso kodekso ir Kriminalinės žvalgybos įstatymo spragas dėl asmens duomenų rinkimo el. erdvėje, išryškėjusias Lietuvos teismų praktikoje[520]. Taip pat savo darbuose Gintaras Goda nagrinėjo procesinių prievartos priemonių (tame tarpe ir susijusių su teisės į privatumą ribojimu) Baudžiamojo proceso kodekse sampratas[521], kurios nėra teisioginis šio tyrimo objektas.

Nemažai Lietuvos mokslininkų darbų skirta pamatinių sampratų, susijusių su teise į privatumą ir asmens duomenų apsauga, analizei ir aiškinimui. Mindaugas Civilka ir Lina Šlapimaitė straipsnyje nagrinėjo asmens duomenų sampratą elektroninėje erdvėje[522], Ilona Petraityte savo straipsnyje analizavo asmens duomenų apsaugos sam-

---

518 Ilona Petraitytė, „Asmens Duomenų Teisinės Apsaugos Principai“ (daktaro disertacija, Vilniaus Universitetas, 2013), Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.

519 Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas“, *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

520 Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema“, *Jurisprudencija* 26, 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02.

521 Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys“, *Teisė* (2000): 17-27. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija* (Vilnius: Registrų centras, 2014).

522 Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė*, 96 (2015): 126-148.

pratą ir santykį su teise į privatumą[523]. Keli Lietuvos mokslininkų darbai[524] nukreipti į teisinius aspektus, susijusius su konkrečių techninių priemonių naudojimą kriminalinės žvalgybos tikslais. Nors šie teisės į privatumą kvalifikavimo aspektai ir aktualūs, tačiau atsižvelgiant į tai, kad jie atskleisti Lietuvos teisės doktrinoje minėtuose darbuose, šiame tyrime dėl to išsamiau nėra nagrinėjami.

**Mokslinis naujumas ir reikšmė**. Šiame tyrime siekiama išanalizuoti asmens duomenų apsaugos elektroninėje erdvėje problemas, atsirandančias sąveikaujant skirtingoms teisinėms sistemoms. Todėl jame ne tik pateikiama Europos Sąjungos teisinėje sistemoje aktualių asmens duomenų perdavimo į kitas teisines sistemas pagrindų, įtvirtintų BDAR, analizė, tačiau ir atliekamas Europos Sąjungos bei JAV sudarytų asmens duomenų perdavimo susitarimų *Safe Harbour* bei *Privacy Shield* vertinimas, atsižvelgiant į Europos Sąjungos Teisingumo Teismo suformuotą praktiką šioje srityje bei Europos Sąjungos bei JAV teisinių sistemų reguliavimą.

Atlikdamas šį tyrimą, aktualioje Europos Sąjungos Teisingumo Teismo *Schrems II* byloje, autorius užčiuopė kertinį probleminį teisės į privatumą ir asmens duomenų apsaugos aspektą, susijusį su trečiosios šalies nacionalinio saugumo intereso įgyvendinimu. Remiantis Europos Sąjungos Teisingumo Teismo išaiškinimais, trečiosios šalies interesas turėti prieigą prie iš Europos Sąjungos subjektų gaunamų asmens duomenų, ginant savo nacionalinį saugumą, yra vertinamas pagal žymiai griežtesnius kriterijus, nei pačių Europos Sąjungos valstybių narių ir, autoriaus vertinimu, yra iš esmės paneigiamas.

Todėl šiame tyrime vertinami galimo naujo susitarimo tarp Europos Sąjungos ir JAV kontūrai, atsižvelgiant į Europos Sąjungos Teisingumo Teismo suformuotą praktiką minėtose bylose, ryšiumi su trečiosios šalies interesu užtikrinti savo nacionalinį saugumą.

Iš pristatytos teisės doktrinos privatumo apsaugos srityje apžvalgos, darytina išvada, kad joje dažniausiai analizuojamos temos, susijusios su (i) bendrąja teisės į privatumą ir asmens duomenų apsaugą samprata; (ii) asmens duomenų perdavimo tarp

---

523 Ilona Petraitytė, „Asmens Duomenų Apsauga Ir Teisė į Privatų Gyvenimą“, *Teisė* 80 (2011): 163-74.

524 Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“, *Teisės problemos* 1, 91 (2016): 25-51; Darius Štitilis ir Marius Laurinaitis, „IP telefonija - iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui“, *Socialinių mokslų studijos* 1 (2009): 205–221; Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas“, *Jurisprudencija : mokslo darbai* 29 (2002): 72–85; Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė* (2017): 84–99, doi:10.15388/Teise.2017.105.11114.

Europos Sąjungos ir JAV pagrindais; (iii) jų (ne)teisėtumu remiantis jau pasenusia Europos Sąjungos Teisingumo Teismo praktika *Schrems* byloje, (iv) asmens teisės į privatumą ir asmens duomenų apsaugą ribojimas ikiteisminio tyrimo priemonėmis bei keitimasis šiais duomenimis. Autoriui nepavyko rasti nė vieno mokslinio darbo, kuriame būtų analizuojami asmens duomenų perdavimo į kitą teisinę sistemą teisiniai pagrindai, atsižvelgiant į nacionalinio saugumo intereso įgyvendinimą, jo ribas ar santykį su asmenų teise į privatumą bei asmens duomenų apsaugą kitoje teisinėje sistemoje.

Atliktas tyrimas ir jo rezultatai gali būti naudingi, siekiant įvertinti Europos Sąjungos subjektų atliekamo asmens duomenų perdavimo pagrindų į JAV teisinę sistemą teisėtumą ir pagrįstumą bei atliekant galimo naujo Europos Komisijos sprendimo dėl tinkamos asmens duomenų apsaugos JAV teisinėje sistemoje užtikrinimo lyginamąją analizę.

**Tyrimo objektas**. Šios disertacijos tyrimo objektas yra asmens teisės į privatumą ir asmens duomenų apsaugą ribos elektroninėje erdvėje skirtingose teisinėse sistemose, atsižvelgiant į probleminį teisinių sistemų sąveikos aspektą – valstybių interesą užtikrinti savo nacionalinį saugumą.

**Mokslinė problema**. Disertacijos mokslinė problema formuluojama šiais klausimais:

1. Kokia yra nacionalinio saugumo samprata ir ar jis turi ribas?

2. Ar Europos Sąjungos Teisingumo Teismas sprendimais *Schrems* ir *Schrems II* bylose užkirto kelią susitarimui dėl asmens duomenų perdavimo tarp Europos Sąjungos ir kitos teisinės sistemos (tame tarpe ir JAV) sudarymo?

3. Ar remiantis proporcingumo principu galima pateisinti teisės į privatumą ir asmens duomenų apsaugą ribojimą, taikomą trečios šalies nacionalinio saugumo užtikrinimo tikslais?

4. Ar asmens duomenų perdavimas iš Europos Sąjungos į JAV gali būti laikomas teisėtu taikant standartinių duomenų apsaugos sąlygų institutą pagal BDAR 46 str., kai Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje JAV teisinį reguliavimą pripažino neužtikrinančiu adekvačios teisės į privatumą ir asmens duomenų apsaugos?

5. Kokie yra būtini pokyčiai JAV teisinėje sistemoje, susiję su asmens teisės į privatų gyvenimą ir asmens duomenų apsauga, siekiant galimo susitarimo dėl asmens duomenų perdavimo tarp Europos Sąjungos ir JAV?

**Tyrimo tikslas**. Ištirti asmens duomenų perdavimo iš Europos Sąjungos į JAV

teisinius pagrindus ir atsižvelgiant į Europos Sąjungos Teisingumo Teismo praktikoje suformuotą kritiką JAV teisinei sistemai, nustatyti, kokiomis sąlygomis asmens duomenų perdavimas į JAV galėtų būti laikomas teisėtu.

**Tyrimo uždaviniai**. Siekiant nurodyto tikslo, formuluojami tokie uždaviniai:

1. Įvertinti galimus asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinius pagrindus pagal BDAR ir išanalizuoti jų tarpusavio santykį bei priklausomybę;

2. Išanalizuoti Europos Sąjungos Teisingumo Teismo praktiką, susijusią su asmens teisės į privatumą ir asmens duomenų apsauga ir nustatyti reikšmingas privatumo apsaugos JAV teisinėje sistemoje problemas, užkertančias kelią sėkmingam asmens duomenų perdavimui iš Europos Sąjungos į JAV;

3. Išanalizuoti nacionalinio saugumo sampratą ir nustatyti galimas jos ribas pagal Lietuvos, JAV teisinį reguliavimą bei Europos Žmogaus Teisių Teismo praktiką bylose dėl teisės į privatumą pažeidimo;

4. Identifikuoti proporcingumo principo, kaip pagrindinio teisinio testo, taikomo vertinant asmens teisės į privatumą ir asmens duomenų apsaugą ribojimų teisėtumą, kriterijus bei nustatyti, ar jį taikant gali būti išsprendžiama asmens duomenų perdavimo iš Europos Sąjungos į JAV teisėtumo problema;

5. Įvertinus pamokas iš Europos Sąjungos Teisingumo Teismo praktikos, nustatyti kokios yra galimo teisėto asmens duomenų perdavimo iš Europos Sąjungos į JAV sąlygos.

**Ginamieji teiginiai**:

1. Kai panaikinamas asmens duomenų perdavimo iš Europos Sąjungos į trečiąją šalį pagrindas, taikytas pagal BDAR V skyriaus teisinį reguliavimą, nepakitus asmens duomenų apsaugos lygiui trečiojoje šalyje, asmens duomenų perdavimas į tą pačią trečiąją šalį negali būti teisėtas remiantis kitu BDAR V skyriuje įtvirtintu teisiniu pagrindu.

2. Pagrindinis JAV teisinės sistemos trūkumas, kuris užkerta kelią JAV teisės į privatumą ir asmens duomenų apsaugos reguliavimą pripažinti adekvačiu BDAR V skyriaus prasme, yra susijęs su JAV nacionalinio saugumo intereso įgyvendinimu.

3. Asmens teisės į privatumą ir asmens duomenų apsaugą ribojimo pagrindas, susijęs su valstybės nacionalinio saugumo interesų įgyvendinimu, neturi teisiškai apibrėžtų ribų.

4. Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje netiesiogiai verčia trečiąją šalį, kuri pageidauja būti pripažinta užtikrinančia adekvatų teisės

į privatumą ir asmens duomenų apsaugą lygį, atsisakyti savo nacionalinio saugumo interesų įgyvendinimo iš Europos Sąjungos gaunamų duomenų atžvilgiu.

**Metodologija.** Skirtingi mokslinių tyrimų yra naudojami ir derinami tarpusavyje, siekiant tyrimo tikslo ir uždavinių įgyvendinimo.

Duomenys tyrimui buvo renkami remiantis *mokslinės literatūros, teisinių dokumentų analizės, nestruktūruoto ekspertų interviu metodais*. Tyrimui aktualūs duomenys buvo apdorojami *naudojantis sisteminės ir loginės analizės, lingvistiniu, lyginamuoju ir istoriniais metodais*.

*Teisinių dokumentų analizės* bei *lyginamasis metodai* naudoti viso tyrimo metu. Jie turėjo reikšmingą įtaką rengiant antrąjį darbo skyrių, kuriame tiriami asmens duomenų perdavimo į trečiąsias šalis teisiniai pagrindai, įtvirtinti BDAR V skyriuje. Šių metodo taikymas leido atskleisti asmens duomenų perdavimo į trečiąsias šalis teisinių pagrindų skirtumus, tarpusavio priklausomybę ir santykį siekiant jiems visiems suformuoto bendro taikymo tikslo.

*Istorinis tyrimo metodas* turėjo svarbų vaidmenį viso tyrimo atlikimui. Remiantis juo buvo analizuota nacionalinio saugumo sampratos kilmė ir raida JAV teisinėje sistemoje bei Europos Žmogaus Teisių Teismo praktikoje. *Lyginamasis metodas* sudarė galimybes įvertinti nacionalinio saugumo sampratos ir teisinio reglamentavimo Lietuvos, JAV teisinėse sistemose bei pagal Europos Žmogaus Teisių Teismo praktiką, skirtumus.

*Loginės, sisteminės analizės* tyrimo metodai buvo naudojami viso tyrimo metu. Remiantis jais nuosekliai buvo tiriama tyrimui aktuali medžiaga. Jie buvo labiausiai reikšmingi analizuojant Europos Sąjungos Teisingumo Teismo praktiką dėl asmens teisės į privatumą ribojimų teisėtumo bei identifikuojant proporcingumo principo, kaip pagrindinio teisinio testo, taikomo vertinant asmens teisės į privatumą ir asmens duomenų apsaugą, taikymo sąlygas ir ribas. Kartu su šiais metodais aktyviai naudotas *lingvistinis* metodas, siekiant nustatyti sąvokų skirtumus, galinčius atsirasti dėl vertinių skirtingų sampratų lietuvių ir anglų kalbomis. Šių metodų taikymo tikslas – ištirti buvusį ir esamą asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinį reglamentavimą; teisės į privatumą ribojimo pagrindų teisinį reglamentavimą Europos Sąjungoje ir JAV.

Taikant *teleologinį tyrimo metodą* analizuota ir aiškinta Europos Sąjungos Teisingumo Teismo praktika. Šis metodas naudotas siekiant įvertinti teismo suformuotų išaiškinimų svarbą, atskleisti jų prasmę bei kontekstą ir šias įžvalgas pritaikyti aktua-

liam teisiniam reguliavimui bei darant išvadas dėl būtinų asmens duomenų perdavimo modelio pakeitimų. Šis metodas buvo itin reikšmingas atskleidžiant Europos Sąjungos Teisingumo Teismo išaiškinimų turinį ir pagrindinę mintį.

*Mokslinės literatūros analizės metodas* naudojamas siekiant atskleisti Europos Sąjungos, JAV ir Lietuvos mokslininkų požiūrį dėl teisės į privatumą ir asmens duomenų apsaugos ribojimų teisėtumo ir jų atliktų mokslinių tyrimų rezultatus. Šio metodo taikymas leido atskleisti tarp JAV mokslininkų dominuojantį kritišką požiūrį į Europos Sąjungos Teisingumo Teismo išaiškinimus *Schrems II* byloje, suprasti jį pagrindžiančias pozicijas bei kodėl šis teismas kaltinamas dviveidiškumu.

Asmens teisės į privatumą apsauga elektroninėje erdvėje pasižymi greitais pokyčiais dėl technologinės elektroninių ryšių ir technologijų raidos. Šiuos pokyčius lemia netikėčiausi, tačiau visuomenėms itin reikšmingi įvykiai, pavyzdžiui pranešėjų (angl. *whistle-blowers*) paviešinama informacija (Edvardo Snoudeno atveju), ar net atskirų ūkio subjektų sprendimai, darantys įtaką jų produktų ar paslaugų vartotojams visame pasaulyje (pvz., įmonės kaip *Facebook*, *Apple*, *Google* etc.). Todėl *stebėsenos* metodas taikomas siekiant tyrimo tema turėti aktualią informaciją, gebėti suprasti konkrečių sprendimų motyvus ar užsienio mokslininkų pozicijas, prognozuoti būsimus teisinio reguliavimo pokyčius arba tų pokyčių poreikį, dar nepasirodžius teisės aktų pakeitimams ar mokslininkų publikacijoms aktualiais klausimais[525].

*Nestruktūrizuoto interviu metodas* taikomas teisinio reglamentavimo problematikos, atsižvelgiant Europos Sąjungos Teisingumo Teismo išaiškinimus, nustatymui ir atskleidimui. Autorius tyrimo tema diskutavo su prof. Lietuvos Aukščiausiojo Teismo baudžiamųjų bylų skyriaus pirmininku Aurelijumi Gutausku, stažuotės Lenkijoje metu – su prof. Dorota Lis-Staranowicz, prof. Marcin Dabrowski, taip pat su kitais Varmijos ir Mazūrijos universiteto mokslininkais seminarų metu. Interviu metu visiems ekspertams buvo pateikiami nevienodi klausimai, suformuoti atsižvelgiant į kiekvieno eksperto pateiktą informaciją ir mokslinių tyrimų sritį.

---

[525] Pavyzdžiui, tyrimo rengimo metus stebėtos JAV mokslininko Daniel Justin Solove publikacijos, teisinis tinklaraštis *TeachPrivacy* (https://www.youtube.com/channel/UCqODltywqZCuxprcz72kc-Q), socialinio tinklo LinkedIn grupė *Schrems II – Lawful Data Transfer* ir t.t.

# IŠVADOS

1. Vadovaujantis atlikta analize, darytina išvada, kad nacionalinio saugumo sąvoka Lietuvos, Europos Sąjungos ar JAV teisės sistemose nėra apibrėžta. Visų šių teisės sistemų reguliavimo analizė atskleidžia, kad jos stokoja aiškios indikacijos apie galimas nacionalinio saugumo sampratos ribas. Ypač riba tarp žvalgybos veiklos (kuria saugomas nacionalinis saugumas) ir kriminalinės žvalgybos (kurios pagrindu kovojama su nusikalstamumu) yra neaiški, nes visuotinai sutariama, kad, pavyzdžiui, kova su terorizmu yra vedina valstybių tiek nacionalinio saugumo apsaugos, tiek nusikaltimų prevencijos tikslais. Todėl valstybės, siekdamos riboti asmenų teisę į privatumą ir pateisinti prieigą prie asmens duomenų gali tai daryti skirtingais teisiniais pagrindais ir pagal skirtingas taisykles – arba pagal nacionalinio saugumo apsaugos teisinį mechanizmą, arba nusikaltimų prevencijos tikslais. Nesant koncepcinių nacionalinio saugumo sampratos ribų, teisėsaugos ir žvalgybos institucijos gali piktnaudžiauti joms prieinamais teisės į privatumą ribojimo pagrindais. Siekiant minimizuoti šią riziką, siūlytina Lietuvos teisiniame reguliavime įtvirtinti konkrečius kriterijus, kurie leistų identifikuoti visuomeninio reiškinio priskyrimą nacionalinio saugumo apsaugos sričiai ir įgalintų brėžti ribas tarp žvalgybos ir kriminalinės žvalgybos veiklų.

2. Dėl teisės į privatumą apsaugos skirtingų sistemų sąveikoje, atsižvelgiant į asmens duomenų perdavimo teisinius pagrindus pagal BDAR, jų tarpusavio santykį bei priklausomybę:

2.1. duomenų valdytojai ar tvarkytojai, pageidaujantys perduoti duomenis į JAV (trečiąją šalį), kai Europos Sąjungos Teisingumo Teismas panaikino *Privacy Shield* susitarimą, patys negali duomenų subjektams užtikrinti „iš esmės lygiaverčio apsaugos lygio, koks garantuojamas Europos Sąjungoje“, nes jie negali suteikti jokių teisių ar garantijų duomenų subjektams, kurios galėtų „pagerinti“ duomenų subjektų padėtį ryšium su JAV valdžios institucijų neribota prieiga prie jų asmens duomenų ir masinio asmens duomenų rinkimo.

2.2. nepaisant prieštaringo BDAR preambulės 107 p. ir 44 str. reguliavimo, asmens duomenų perdavimas iš Europos Sąjungos į trečią šalį, teritoriją ar tarptautinę organizaciją negali būti laikomas teisėtu, jei ankstesnis asmens duomenų perdavimo teisinis pagrindas vienu iš V skyriuje įtvirtintų pagrindų (pvz., *Privacy Shield* susitarimas, sudarytas BDAR 45 str. 3 d. pagrindu) buvo panaikintas dėl priežasčių, kurių ištaisymas nepriklauso nuo trečiojoje šalyje veikiančio duomenų valdytojo ar tvarkytojo

ir jų galimų taikyti pavyzdinių tinkamų apsaugos priemonių BDAR V skyriaus prasme.

3. Dėl Europos Sąjungos Teisingumo Teismo praktikos, susijusios su asmens teisės į privatumą ir asmens duomenų apsauga ir reikšmingų JAV teisinio reguliavimo kliūčių, užkertančių kelią sėkmingam asmens duomenų perdavimui iš Europos Sąjungos į JAV:

3.1. Europos Sąjungos Teisingumo Teismo sprendimo *Digital Rights Ireland* byloje analizė leidžia daryti išvadą, kad elektroninių ryšių subjektų pareiga numatytą laikotarpį (*Digital Rights Ireland* bylos atveju – 6 – 24 mėn.) saugoti turimus srauto ir vietos nustatymo duomenis nusikaltimų prevencijos, atskleidimo, tyrimo arba patraukimo už juos atsakomybėn, taip pat valstybės saugumo užtikrinimo tikslais, yra neproporcinga ir neteisėta. Tačiau šis teismo sprendimas neleidžia daryti aiškios išvados, ar tokie veiksmai apskritai gali būti teisėti, esant kitokiam teisiniam reguliavimui ir galiojant papildomoms teisės į privatumą ir asmens duomenų apsaugą užtikrinimo priemonėms, kuriomis duomenų subjektai galėtų pasinaudoti.

3.2. Europos Sąjungos Teisingumo Teismo sprendimo *Schrems* byloje analizė leidžia daryti išvadą, kad susitarimas tarp Europos Sąjungos ir JAV (*Schrems* bylos atveju – *Safe Harbour* susitarimas) negali būti laikomas užtikrinančiu adekvačią asmenų teisės į privatumą ir asmens duomenų apsaugą JAV teisinėje sistemoje, kai susitarime įtvirtinti teisės į privatumą apsaugos principai apskritai netaikomi JAV valdžios įstaigoms arba kai JAV teisėsaugos ir žvalgybos institucijoms suteikiama prieiga prie JAV subjektams perduodamų Europos Sąjungos vartotojų asmens duomenų, o jie neturi procedūrinių garantijų apginti savo galimai pažeidžiamas teises JAV teritorijoje.

3.3. Europos Sąjungos Teisingumo Teismo sprendimo *Schrems II* byloje analizė leidžia daryti išvadą, kad BDAR yra taikomas asmens duomenų perdavimui, atliktam valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, jei atliekant šį perdavimą ar po jo šios trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais. Todėl didžiausią iššūkį galimiems susitarimams dėl duomenų perdavimo tarp Europos Sąjungos ir JAV kelia būtent JAV taikomų nacionalinį saugumą užtikrinančių priemonių (pvz. vykdomo masinio sekimo) atitikties vertinimas BDAR atžvilgiu.

4. Dėl proporcingumo principo, kaip pagrindinės teisės ribojimo teisėtumo įvertinimo kriterijaus taikymo sprendžiant teisės į privatumą apsaugos skirtingų teisinių sistemų sąveikoje problemą:

4.1. Europos Sąjungos teisės kontekste, proporcingumo principas yra vienas

reikšmingiausių teisinių konceptų, galinčių padėti nustatyti protingą pusiausvyrą tarp viešųjų interesų konkurencijos (pvz. teisės į privatumą ir nacionalinio saugumo apsaugos). Todėl jis gali būti laikomas raktu į teisingą sprendimą dėl asmens teisės į privatumą apsaugos ribojimų teisėtumo nustatymo, tame tarpe ir pateisinant teisės į privatumą ir asmens duomenų apsaugą ribojimą, taikomą trečios šalies nacionalinio saugumo užtikrinimo tikslais.

4.2. Pagal Europos Sąjungos Teisingumo Teismo sprendimą byloje *Schrems II*, kad pats *Privacy Shield* susitarimas pažeidžia pagrindinės teisės į privatumą esmę. Tokio (t. y. teisės į privatumą esmės) pažeidimo nustatymas eliminuoja būtinybę taikyti proporcingumo principą ir atlikti konkuruojančių interesų analizę ir teisingo jų balanso paiešką. Konstatavus teisės į privatumą ir duomenų apsaugą esmės pažeidimą, JAV teisės sistemoje galiojančių teisės į privatumą ribojimų neproporcingumas negali būti švelninamas net ir atsižvelgiant į veiksmingas teisių gynimo priemones, jei tokios Europos Sąjungos duomenų subjektams ir būtų suteiktos JAV *Privacy Shield* susitarimo pagrindu.

4.3. Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje dėl Privacy Shield susitarimo panaikinimo netiesiogiai verčia JAV ar kitą trečiąją šalį, kuri pageidauja būti pripažinta užtikrinančia adekvatų teisės į privatumą ir asmens duomenų apsaugą lygį BDAR V skyriaus prasme, atsisakyti savo nacionalinio saugumo interesų įgyvendinimo iš Europos Sąjungos gaunamų duomenų atžvilgiu. Todėl Europos Sąjungos Teisingumo Teismas sprendimu *Schrems II* byloje užkirto kelią susitarimo dėl asmens duomenų perdavimo tarp Europos Sąjungos ir kitos teisinės sistemos (tame tarpe ir JAV) sudarymui, trečiai šaliai neatsisakant savo nacionalinio saugumo intereso įgyvendinimo iš Europos Sąjungos gaunamų duomenų atžvilgiu.

5. Dėl būtinų privatumo apsaugos pokyčių JAV teisės sistemoje, siekiant teisėto asmens duomenų perdavimo iš Europos Sąjungos į JAV:

5.1. Atsižvelgiant į tai, kad JAV institucijoms suteikiant neribotą prieigą prie iš Europos Sąjungos subjektų gaunamų duomenų, yra pažeidžiama teisės į privatumą ir asmens duomenų apsaugą esmė, siekiant ilgalaikį sudaryti susitarimą dėl asmens duomenų perdavimo tarp Europos Sąjungos ir JAV, JAV teisinėje sistemoje turėtų būti apribota teisėsaugos ir žvalgybos institucijų prieiga prie skirtingų kategorijų duomenų, pavyzdžiui, suteikiant prieigą tik prie asmenų, siejamų su sunkiais nusikaltimais ar keliančių tiesioginį ir pagrįstą pavojų nacionalinio saugumo užtikrinimui, duomenų.

5.2. Atsižvelgiant į tai, kad teisės į privatumą ribojimo proporcingumas gali pri-

klausyti nuo duomenų subjektams prieinamų procedūrinių apsaugos priemonių egzistavimo, priimtinas efektyvios asmenų teisių pažeidimų apsaugos modelis yra galimas JAV teisinėje sistemoje įgyvendinant šiuos pagrindinius pakeitimus: (i) praplečiant nepriklausomo subjekto (pvz., ombudsmeno, kuris buvo numatytas pagal *Privacy Shield* susitarimą) galias ir įgaliojant priimti teisėsaugos ir žvalgybos tarnyboms privalomus sprendimus (įskaitant ir susijusius su JAV Prezidento nurodymu Nr. 12333), (ii) numatant nepriklausomo subjekto aiškias nepriklausomumo nuo vykdomosios valdžios garantijas, (iii) įtvirtinant asmenų skundų nagrinėjimo modelį, pasižymintį bent ribotu rungimosi principu, pavyzdžiui, asmeniui neatskleidžiant jo atžvilgiu surinktos informacijos turinio ir apimties, tačiau užtikrinant, kad kompetentingas ir nepriklausomas subjektas galėtų nešališkai ir pagrįstai išnagrinėti asmens skundą dėl teisėsaugos ar žvalgybos institucijų veiksmų pagrįstumo.

**Publikacijos disertacijos tema**

1. „*E. Privatumo direktyvos įgyvendinimo problemos ir jų sprendimai e. Privatumo reglamento projekte*“. Žurnalas Teisė, 2019, Vol. 113, pp. 139–154.;

2. “*Restrictions of Criminal Intelligence Measures in Law Enforcement Directive and Law on Criminal Intelligence of Lithuania*“. SOCRATES Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law, 2020, Nr. 3 (18);

3. „*Efektyvi teisės į privatų gyvenimą apsauga taikant kriminalinės žvalgybos priemones*”, Vytauto Didžiojo Universiteto žurnalas „Teisės apžvalga“, 2021, Nr. 1 (23).

**Pranešimai konferencijose disertacijos tema**

2020-11-23 skaitytas pranešimas “*Efficiency of Criminal Intelligence Measures in the Context of Privacy*” in Ukrainos Yaroslav Mudryi Nacionalinio teisės universiteto konferencijoje „Legal Autumn“. Taip pat išspausdintas pranešimas tarptautinės mokslo konferencijos „Legal Autumn“ žurnale skaityto pranešimo tema;

2020-10-14 skaitytas pranešimas MRU tarptautinėje konferencijoje „Tvarumas pasaulinės krizės akivaizdoje“ tema „*Criminal Intelligence vs Right to Private Life*“;

**Mokslinė stažuotė**

2021-05-10 – 2021-05-21 – mokslinė stažuotė Lenkijos Varmijos ir Mazūrijos universitete (UWM) Olštyne.

## Gyvenimo aprašymas

**Išsilavinimas**

2015–2021 m. doktorantūros studijos Mykolo Romerio universiteto Teisės mokykloje

2008 m. įgytas teisės magistro laipsnis (Vilniaus universitetas)

**Darbo patirtis**

Nuo 2017 m. viešųjų pirkimų skyriaus vadovas Vilniaus universitete

2014–2017 m. viešųjų pirkimų skyriaus vadovas Vilniaus universiteto Santaros klinikose

MYKOLAS ROMERIS UNIVERSITY

**Edgaras Markevičius**

# LEGAL ISSUES OF PERSONAL DATA TRANSFER IN CYBERSPACE BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA

Summary of Doctoral Thesis
Social Sciences, Law (S 001)

Vilnius, 2022

The doctoral dissertation has been prepared in 2015–2021, defended at Mykolas Romeris University according to the right to perform PhD studies given to Mykolas Romeris University and Vytautas Magnus University by Order No. V-160 of the Minister of Education, Science and Sport of the Republic of Lithuania, dated 22nd February 2019.

*Scientific supervisor:*
Prof. Dr. Darijus Beinoravičius (Mykolas Romeris University, Social Sciences, Law, S 001).

The doctoral dissertation is going to be defended before the Defence Board in the Field of the Science of Law of Mykolas Romeris University and Vytautas Magnus University:

*Chairperson:*
Prof. Dr. Toma Birmontienė (Mykolas Romeris University, Social Sciences, Law, S 001).

*Members:*
Prof. Dr. Vida Davidavičienė (Vilnius Gediminas Technical University, Social Sciences, Management, S 003);
Prof. Dr. Aurelijus Gutauskas (Vilniaus University, Social Sciences, Law, S 001);
Hab. Dr. Dorota Lis-Staranowicz (University of Warmia and Mazury in Olsztyn, Poland, Social Sciences, Law, S 001);
Assoc. Prof. Dr. Juozas Valčiukas (Mykolas Romeris University, Social Sciences, Law, S 001).

The doctoral dissertation will be defended in a public meeting of the Defence Board in the Field of the Science of Law in Room I-414 at Mykolas Romeris University on September 5th, 2022 at 14 pm.
Address: Ateities g. 20, LT-08303 Vilnius, Lithuania.

The summary of the doctoral dissertation was sent out on August 5th, 2022.

The doctoral dissertation can be accessed in Martynas Mažvydas National Library of Lithuania (Gedimino pr. 51, Vilnius), in the library of Mykolas Romeris University (Ateities g. 20, Vilnius) and in the library of Vytautas Magnus University (K. Donelaičio g. 52, Kaunas).

**Edgaras Markevičius**

# LEGAL ISSUES OF PERSONAL DATA TRANSFER IN CYBERSPACE BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA

## SUMMARY OF DOCTORAL THESIS

**Relevance of the topic**. The last decades have been characterized by extremely rapid technological progress, which has changed many areas of everyday life. One of the most affected areas includes the social life of individuals - means and habits of joint work, mutual communication. Currently, it has become common to hold teleconferences instead of live meetings; call no longer via GSM connection, but communicate via video (e.g. with the help of *Viber*, *Facebook Messenger*, *FaceTime* apps), etc.

This technological progress leads to the ever-increasing use of electronic communication networks and cloud technologies by individuals, companies and organizations to provide innovative communication services, store and manage records in the electronic space. The increasing use of these communications provides an unprecedented opportunity to systematically collect and use various data (including personal data) for different purposes. With the help of technology, information and data are collected, processed and used not only for the purposes of meeting the needs of communicating natural and legal persons, but also for various other purposes.

In the context of extremely widespread collection and use of personal data, ensuring a person's right to private life becomes problematic in a legal sense. Although individuals are guaranteed the right to privacy, other interests for which this data may be used cannot be ignored. These interests include both private and public interests - prevention and pretrial investigation of serious crimes (for example, terrorism, drug smuggling and transportation, human trafficking, etc.), ensuring the national security of states, providing public administration services by electronic means, etc.

In terms of legal analysis, a difficult question is always related to the competition of two interests - the individual's right to privacy and the collective interest of society's

security - and determining the proportional balance of these interests. This issue becomes even more complex when the protection of privacy needs to be reconciled not only with respect to competing interests, but also between different legal systems where both privacy and society's collective security interests are understood and interpreted differently.

In the European Union, the right to privacy and protection of personal data is protected by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union provisions and GDPR. Since the right to privacy and protection of personal data is guaranteed to all individuals, the European Union must ensure that these rights are implemented when processing personal data not only within its territory, but also when transferring it outside its borders.

Transatlantic data flows between the European Union and the United States of America are the fastest and largest in the world, accounting for more than half of European data flows and about half of United States of America data flows, making the United States of America and the European Union not only one of the largest markets, but also the most important commercial partners in digital services[526]. As a result, in a legal and factual sense, the most pressing problems of protecting the right to privacy arise from the transfer of personal data between the legal systems of the European Union and the United States of America.

The question of the scope of protection of the right to privacy, when combined with the state's national security or crime prevention interests, is not easily determined even in the context of a single legal system. This is confirmed by the many controversial and high-profile decisions made by the Court of Justice of the European Union in cases regarding the application of the Charter of Fundamental Rights of the European Union, the practice of the European Court of Human Rights in the application of the European Convention for the Protection of Human Rights and Fundamental Freedoms in the areas of the right to privacy and personal data protection.

In the author's opinion, this task of determining the scope of protection of the right to privacy becomes significantly more difficult when it is necessary to harmonize it with respect to not one, but several legal systems. The protection of the right to privacy according to the high standard of protection afforded by the European Union is not easily compatible with the American legal system and the concept of privacy in it,

[526] Daniel S. Hamilton ir Joseph P. Quinlan, *The Transatlantic Economy 2020: Annual Survey Of Jobs, Trade And Investment Between The United States And Europe* (2020), 8.

primarily due to fundamental differences between the American legal system and the European Union legal system. For example, the third-party doctrine applied in American law[527], according to which, natural persons do not have a reasonable interest in the protection of the right to privacy with respect to data that is not controlled by them, but by third parties (for example, banks, electronic communication service providers, etc.). Therefore, American law enforcement or intelligence agencies can obtain this data with essentially no safeguards in place. Also, according to the practice established by the United States of America Supreme Court in the *Clapper* case, individuals cannot sue for privacy protection if they cannot prove that surveillance has been applied to them[528]. Taking into account the fact that surveillance measures are applied secretly, without notifying the individuals (in relation to whom they are applied), such established precedent has a significant negative impact on the ability of individuals to defend their vulnerable rights.

In addition to significant fundamental differences in the scope and legal frameworks of the approach to the right to privacy between the European Union and the United States of America, other factors related to the actual protection of the right to privacy in the United States of America are also important. The administrations of United States of America presidents Bush and Obama pursued controversial national security programs, including targeted killings, torture and surveillance, the secrecy of which prevented the public from learning about those actions and the measures taken[529]. Some of these applied measures, the rationale and significance of their application wer revealed by whistleblower Edward Snowden in 2013 [530], by which he sowed the seeds of distrust in the protection of privacy in the American legal system and in the legality of the surveillance measures actually in place. This aspect of mistrust is perfectly illustrated by the critical evaluations of privacy protection in the American legal system in the Lithuanian legal doctrine that "mass collection of personal data in the US is analogous to the 13th century right of persons authorized by the Crown to enter at any

---

527 Simon Stern, „The Third-Party Doctrine and the Third Person", *New Criminal Law Review* 16, 3 (2013): 101.

528 „Clapper v. Amnesty International", CaseText, žiūrėta 2021 m. rugpjūčio 5 d., https://casetext.com/case/clapper-v-amnesty-intl-usa-7.

529 Sudha N. Setty, *National Security Secrecy: Comparative Effects on Democracy and the Rule of Law* (Cambridge University Press, 2017), 3.

530 Jordi Pujol, „Is This the End of Privacy? Snowden and the Power of Conscience", *Church, Communication and Culture* 5, 1 (2020): 140-44.

time the house of any person in the domain of the Great Britain"[531].

These legal systems interact when personal data is transferred between different entities belonging to these legal systems. The transfer of personal data from European Union entities to third countries is regulated in Chapter V of GDPR. It establishes, in order of priority, the different grounds for the transfer of personal data from the European Union to third countries (or international organizations): the decision of the European Commission on suitability, appropriate protection measures applied by the data controller or processor, derogating provisions. All these grounds for data transfer are applied to achieve the same goal, which is to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

As United States of America is a third country, pursuant to Art. 45 of the GDPR, the simplest and most favorable solution to regulate the transfer of personal data between the European Union and the United States of America is the decision of the European Commission on the adequate level of privacy protection ensured in a third country (i.e. the United States of America).

The European Commission adopted such a decision in relation to the United States of America (i.e. *Safe Harbor Agreement*) in the year 2000. The revelations of Edward Snowden in 2013 regarding surveillance programs applied in the United States of America have sparked not only outrage but also legal disputes. Legality and validity of the *Safe Harbor Agreement* in 2015 was evaluated by the Court of Justice of the European Union and it was annulled[532].

Following the annulment of the *Safe Harbor Agreement* by the Court of Justice of the European Union, negotiations on a possible new agreement were urgently launched, which ended successfully in 2016 by signing the *Privacy Shield Agreement*. However, time has shown that the *Privacy Shield Agreement* also had significant flaws, as the Court of Justice of the European Union in 2020 also struck it down as not providing adequate privacy protections in the American legal system[533].

---

[531] Sigutė Stankevičiūtė, „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas" (daktaro disertacija, Mykolo Romerio Universitetas, 2020), 113 psl., prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka: 9.

[532] „Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 Schrems", InfoCuria, **žiū**rėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3390590.

[533] „Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje Nr. C-311/18 Facebook Ireland ir Schrems („Shrems II")", InfoCuria, žiūrėta 2021 m. rugpjūčio 2 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=8508220193825AFC3D98FABEA15645EC?text=&docid=228677&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=3350436.

Therefore, taking into account the categorical conclusions reached by the Court of Justice of the European Union about the insufficiency of the protection of the right to privacy in the American legal system, compared to the level of privacy protection guaranteed in the European Union legal system, legal uncertainty regarding the application of the legal basis for the transfer of personal data has arisen once again. The significance of the above-mentioned decision of the European Court of Justice in the *Schrems II* case is extremely high, as it states the fundamental shortcomings of privacy protection in the American legal system, which, in the author's opinion, can hardly be corrected by data controllers or processors. These are flaws related to law enforcement access to personal data processed in the United States of America. Therefore, the use of another legal basis for the transfer of personal data enshrined in Chapter V of the GDPR is likely to be impossible in order to transfer data from the European Union to the United States, as the general principle and purpose of the transfer of personal data (to ensure that the level of protection of natural persons guaranteed by the GDPR) will not be able to be used to be implemented due to the established shortcomings of the personal data protection of the American legal system.

Another argument mentioned in the decision of the Court of Justice of the European Union, but largely undeveloped, is that the exception for non-application of the GDPR, in connection with the protection of national security interests of member states, does not apply to third parties. I. e. in contrast to the member states of the European Union, third countries (including the United States of America) with which data transfer agreements are concluded, must apply GDPR regulation to the processing of personal data received from the European Union, even when it is carried out in the interests of national security. This position of the Court of Justice of the European Union not only places the entities negotiating on the transfer of personal data (such as the European Union and the United States of America) in unequal positions, but also creates significant obstacles to the successful achievement of an agreement on the transfer of personal data, as it *de facto* requires the third party to give up its national security in relation to the implementation of protection of national security interests in relation to personal data received from the European Union.

Due to these circumstances, this thesis aims to analyze the problems of personal data transfer in the cyberspace, in the interaction of the legal systems of the European Union and the United States of America - the conditions and possible legal grounds for the transfer of personal data from the European Union to the United States of America,

taking into account the protection of national security interests and the practice formed by the Court of Justice of the European Union in this regard aspect.

**Research of the topic in the doctrine.** Generally, the individual's right to privacy is a popular topic with both Lithuanian and foreign legal scholars. It is accepted by the scholars that the interest of scientists in the protection of personal data in the field of intelligence and law enforcement is influenced by information leaked to the public about the extent of personal data collection and their (i)legal use[534]. Such an assumption must be supported, taking into account the change in legal regulation and legal doctrine in the field of personal data protection after Edward Snowden leaked information about surveillance programmes in United States of America in 2013.

One of the popular research areas of the right to privacy has been the relationship between the individual and the state in the area of personal data protection. Researchers focused on Edward Snowden's revelations about state surveillance measures and their relationship to the right to privacy[535].

Another popular area of research opened up after the European Court of Justice's decision in the *Schrems* case, which overturned the *Safe Harbor Agreement*. Then the topic of privacy protection in the interaction of different legal systems gained wider interest. The works of scientists appeared on the possibility and legality of data transfer from the European Union to the United States of America[536].

Among the researches in this area, significant studies aimed at analyzing the legal issues of the systematic transfer of personal data between the European Union and

---

534 Stankevičiūtė, *supra note*, 6: 10.

535 Zygmunt Bauman ir kt., „After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology* 8, 2 (2014): 122; Kevin Macnish, „Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World", *Journal of Applied Philosophy* 35, 2 (2016): 417-32; Debora Halbert ir Stefan Larsson, „By Policy or Design? Privacy in the US in a Post-Snowden World", *Journal of Law, Technology and Public Policy* 1, 2 (2015): 1; Sören Preibusch, „Privacy Behaviors after Snowden", *Communications of the ACM* 58, 5 (2015): 48-55.; David Lyon, „Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique", *Big Data & Society* 1, 2 (2014): 205395171454186; Nora Ni Loidain, „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era", *Media and Communication (Lisboa)* 3, 2 (2015): 53-62.; Maria Helen Murphy, „The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe?", *Information & Communications Technology Law* 23, 3 (2014): 192-219.

536 Christina Lam, „Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner", *Boston College International and Comparative Law Review* 40, 3 (2017): 1.

the United States of America should be mentioned[537]. Douglas M. Mcleod and Dhavan V. Shah book *News Frames and National Security. Covering Big Brother*[538] analyses the nature and essence of the tension between national security and civil liberties. It has helped to better identify the nature, concept, and meaning of national security in the American legal system. Svantesson, Dan Jerker B., ir Dariusz Kloza book *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*[539] analyses the cross-border data flow regime, which is based on European Union legal regulatory measures such as GDPR, *Safe Harbor Agreement* and affects the day-to-day data processing on both sides of the Atlantic and how they limit the scope of data transactions. This book helped to understand the different views of European and US legal scholars on the legal regulation of the transfer of personal data under the *Safe Harbor Agreement*, which was anulled in 2015. Patrick Birkinshaw book *Freedom of Information: The Law, the Practice, and the Ideal*[540] provided a broader understanding of governments' historical relationship with data protection and their inherent interest in access to personal data as a necessary requirement for public safety. James Carr ir Patricia Bellia book *The Law of Electronic Surveillance*[541] reviews the legal framework for the collection of personal data in cyberspace at the United States of America at federal level. This book helped to understand how the surveillance mechanisms work in the American legal system.

Analysis of the right to privacy protection can also be considered a popular topic among Lithuanian legal scholars. Among the relevant works, the thesis of S. Stankevičiūtė, which was defended during the preparation of this thesis, on the topic of "Regulation of the collection of personal data in the electronic space for law enforcement and intelligence purposes"[542] should be mentioned first. In it, the researcher analyses the collection of personal data in countries with common and continental

---

537 David C. Gray ir Stephen E. Henderson, *The Cambridge Handbook of Surveillance Law* (Cambridge University Press, 2017); Dan Jerker B. Svantesson ir Dariusz Kloza. *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, 2017); Russell A. Miller, *Privacy and Power* (Cambridge: Cambridge University Press, 2017); Austin Sarat, *A World without Privacy* (New York: Cambridge University Press, 2014).

538 Douglas M. McLeod ir Dhavan V Shah, „News Frames and National Security", *Communication, Society and Politics* (Cambridge University Press, 2014).

539 Dan Jerker B. Svantesson ir Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, 2017).

540 Patrick Birkinshaw, *Freedom of Information: The Law, the Practice, and the Ideal. Fourth ed.* (Cambridge University Press, 2010).

541 James Carr ir Patricia Bellia, *The Law of Electronic Surveillance*, 2017-2 Ed., 1 dalis, (Clark Boardman Callaghan, 2017).

542 Stankevičiūtė, *supra note*, 6: 2 skyrius.

law traditions at the supranational level for law enforcement and intelligence purposes, the peculiarities of legal regulation on ensuring the right to personal data protection. In this paper, as well as in a review study of privacy protection in the United States of America[543] and the above-mentioned books, a detailed analysis of US legal regulation on the collection of personal data for law enforcement and intelligence purposes is provided. However, given the topic of this study, it does not contain any analysis directed at the interaction problems of these overlapping legal systems in the context of privacy protection and possible ways of solving them. P. Pakutinskas in his thesis "Models of legal regulation of electronic communications"[544] analyzed models of legal regulation of electronic communications, but it is not directly relevant for the purpose of this study, as it also does not reveal the problem of the interaction of overlapping legal systems. Julius Zaleskis monography „European Union General Data Protection Regulation and Personal Data Protection Law"[545] analyses general GDPR legal regulation as legal rules to protect individuals from the risks posed by data processing. J. Zaleskis's monograph explains GDPR regulation, but does not analyze the issue of interaction between GDPR and the American legal system. Ilona Petraitytė 2013 thesis[546] is dedicated to the analysis of personal data protection principles, however, it lost a significant part of its relevance in 2018 with the entry into force of the GDPR, and in principle can be useful for historical and comparative analysis of personal data protection regulation.

Another area of personal data protection law analyzed by Lithuanian researchers that is partly relevant for this study is related to the restrictions on the right to privacy carried out during criminal prosecution (pre-trial investigation or during the application of criminal intelligence measures). First of all, in this aspect, the scientific article of Aurelijus Gutauskas should be mentioned, which analyses the practice of the Supreme Court of Lithuania, related to the means used by criminal intelligence and their legal penetration into the private life of a person[547]. It provides insights that are

[543] Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens", European Parliament, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.

[544] Paulius Pakutinskas, „Elektroninių Komunikacijų Teisinio Reguliavimo Modeliai" (daktaro disertacija, Mykolo Romerio Universitetas, 2009), Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.

[545] Julius Zaleskis, *Europos Sąjungos Bendrasis Duomenų Apsaugos Reglamentas Ir Asmens Duomenų Apsaugos Teisė: Monografija* (Vilnius: Registrų Centras, 2019).

[546] Ilona Petraitytė, „Asmens Duomenų Teisinės Apsaugos Principai" (daktaro disertacija, Vilniaus Universitetas, 2013), Prieiga per ELABa – Nacionalinė Lietuvos Akademinė Elektroninė Biblioteka.

[547] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas", *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

relevant in the case of criminal intelligence application measures, but it does not cover the subject of this thesis – privacy protection issues in the interaction of overlapping legal systems, especially considering the current issue of ensuring the national security interests of different states. Rima Ažubalytė also spoke on a related topic, who in her scientific article analysed the loopholes in the Code of Criminal Procedure and the Law on Criminal Intelligence regarding the collection of personal data in cyberspace, which emerged in the practice of Lithuanian courts[548]. Also in his works, Gintaras Goda examined the concepts of procedural coercive measures (including those related to restricting the right to privacy) in the Code of Criminal Procedure[549], which are not direct subject of this thesis.

Many works of Lithuanian scientists are dedicated to the analysis and interpretation of fundamental concepts related to the right to privacy and personal data protection. In an article Mindaugas Civilka and Lina Šlapimaitė analysed the concept of personal data in the cyberspace[550], Ilona Petraityte analyzed the concept of personal data protection and the relationship with the right to privacy in her article[551]. Several works of Lithuanian scientists[552] address legal aspects related to the use of specific technical means for criminal intelligence purposes. Although these aspects of the qualification of the right to privacy are relevant, but given the fact that they are revealed in the Lithuanian legal doctrine in the aforementioned works, this study does not examine them in more detail.

**Scientific novelty and significance.** This thesis aims to analyze the problems of personal data protection in cyberspace that arise from the interaction of different legal systems. Therefore, it not only provides an analysis of the basis of the transfer of personal data to other legal systems relevant in the legal system of the European Union,

548 Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema“, *Jurisprudencija* 26, 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02.

549 Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys“, *Teisė* (2000): 17-27. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija* (Vilnius: Registrų centras, 2014).

550 Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė*, 96 (2015): 126-148.

551 Ilona Petraitytė, „Asmens Duomenų Apsauga Ir Teisė Į Privatų Gyvenimą“, *Teisė* 80 (2011): 163-74.

552 Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“, *Teisės problemos* 1, 91 (2016): 25-51; Darius Štitilis ir Marius Laurinaitis, „IP telefonija - iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui“, *Socialinių mokslų studijos* 1 (2009): 205–221; Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas“, *Jurisprudencija : mokslo darbai* 29 (2002): 72–85; Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė* (2017): 84–99, doi:10.15388/Teise.2017.105.11114.

enshrined in the GDPR, but also evaluates the *Safe Harbor* and *Privacy Shield* personal data transfer agreements concluded by the European Union and the United States of America, taking into account the European Court of Justice practice in this area and the regulation of the legal systems of the European Union and the United States of America.

In carrying out this research, in a significant case of the Court of Justice of the European Union, *Schrems II*, the author stumbled upon a key problematic aspect of the right to privacy and protection of personal data related to the implementation of the national security interest of a third country. According to the interpretations of the Court of Justice of the European Union, a third country's interest in having access to personal data obtained from the entities of the European Union, in defence of its national security, is evaluated according to much stricter criteria than those of the European Union member states themselves and, in the author's opinion, is essentially negated.

Therefore, this thesis evaluates the contours of a possible new agreement between the European Union and the United States of America, taking into account the practice formed by the Court of Justice of the European Union in the aforementioned cases, in relation to a third country's interest in ensuring its national security.

From the presented review of the legal doctrine in the field of privacy protection, it can be concluded that most analysed topics relate to (i) the general concept of the right to privacy and personal data protection; (ii) the basis of the transfer of personal data between the European Union and the United States; (iii) their (i)legality based on the outdated practice of the Court of Justice of the European Union in the *Schrems* case, (iv) limitation of a person's right to privacy and protection of personal data by means of pre-trial investigation and the exchange of this data. The author was not able to find any scientific works that analysed the legal basis of the transfer of personal data to another legal system, taking into account the implementation of the national security interest, its limits or the relationship with the right of individuals to privacy and the protection of personal data in another legal system.

The research conducted and its results can be useful in order to assess the legality and reasonableness of the basis for the transfer of personal data by European Union entities to the American legal system and in conducting a comparative analysis of a possible new decision of the European Commission on ensuring adequate protection of personal data in the American legal system.

**Object of the research.** The object of this dissertation is the limits of a person's

right to privacy and protection of personal data in cyberspace in different legal systems, taking into account the problematic aspect of the interaction of legal systems - the interest of states to ensure their national security.

**Scientific problem.** The scientific problem of the dissertation can be formulated by the following questions:

1. What is the concept of national security and does it have limits?

2. Did the Court of Justice of the European Union prevent the conclusion of an agreement on the transfer of personal data between the European Union and another legal system (including the United States of America) by decisions in cases *Schrems* and *Schrems II*?

3. Based on the principle of proportionality, can the restriction of the right to privacy and protection of personal data be justified for the purposes of ensuring the national security of a third country?

4. Can the transfer of personal data from the European Union to the United States be considered legal when applying the standard data protection conditions institute in accordance with GDPR Article 46, when the Court of Justice of the European Union recognized the United States of America legal regulation in the *Schrems II* case as not ensuring the adequate right to privacy and personal data protection?

5. What are the necessary changes in the American legal system related to the individual's right to privacy and the protection of personal data in order to achieve a possible agreement on the transfer of personal data between the European Union and the United States of America?

**The aim of the research.** To investigate the legal basis of the transfer of personal data from the European Union to the United States of America and, taking into account the criticism of the American legal system formed in the practice of the Court of Justice of the European Union, determine the conditions under which the transfer of personal data to the United States of America could be considered legal.

**The objectives of the research.** In order to achieve the specified aim of the research, the objectives tasks are formulated:

1. Assess the possible legal grounds for the transfer of personal data from the European Union to the United States of America in accordance with the GDPR and analyse their mutual relationship and dependence;

2. To analyse the practice of the Court of Justice of the European Union related to the right to privacy and the protection of personal data and to identify signifi-

cant privacy protection problems in the American legal system that prevent the lawful transfer of personal data from the European Union to the United States of America;

3. To analyse the concept of national security and determine its possible limits according to the legal regulation of Lithuania and the United States of America and the practice of the European Court of Human Rights in cases of violation of the right to privacy;

4. To identify application criteria of the principle of proportionality, as the main legal test used in assessing the legality of restrictions on a person's right to privacy and protection of personal data, and to determine whether its application can solve the problem of the legality of the transfer of personal data from the European Union to the United States of America;

5. After evaluating the lessons from the practice of the Court of Justice of the European Union, determine what the conditions are for the possible legal transfer of personal data from the European Union to the United States of America.

**Dissertation statements to be defended**:

1. When the basis for the transfer of personal data from the European Union to a third country, applied in accordance with the legal regulation of Chapter V of the GDPR, is abolished, without changing the level of protection of personal data in the third country, the transfer of personal data to the same third country cannot be legal based on another legal basis established in Chapter V of the GDPR.

2. The main shortcoming of the American legal system, which prevents the right to privacy and the regulation of personal data protection in the United States of America from being recognized as adequate within the meaning of Chapter V of the GDPR, is related to the implementation of the United States of America national security interest.

3. The basis for restricting a person's right to privacy and protection of personal data, related to the implementation of the state's national security interests, has no legally definable limits.

4. The decision of the Court of Justice of the European Union in *Schrems II* case indirectly forces a third party, which seeks to be recognized as ensuring an adequate level of the right to privacy and personal data protection, to waive the implementation of its national security interests in relation to data received from the European Union.

**Methodology.** Different scientific research methods are used and combined with each other in order to achieve the research goal and objectives.

Data for the study was collected based on the methods of scientific literature analysis of legal documents, and unstructured expert interviews. Data relevant to the study was processed using systematic and logical analysis, linguistic, comparative and historical methods.

Analysis and comparative methods of legal documents were used throughout the investigation. They had a significant influence on the preparation of the second work section, which examines the legal basis for the transfer of personal data to third countries, established in Chapter V of the GDPR. The application of this method made it possible to reveal the differences in the legal bases of the transfer of personal data to third countries, interdependence and the relationship in order to achieve the common goal of application formed for all of them.

The historical research method played an important role in the overall research. Based on it, the origin and development of the concept of national security in the American legal system and in the practice of the European Court of Human Rights were analysed. The comparative method made it possible to assess the differences between the concept of national security and legal regulation in the legal systems of Lithuania and the United States of America, as well the practice of the European Court of Human Rights.

Research methods of logical, systematic analysis were used throughout the study. Based on them, material relevant to the study was consistently studied. They were the most significant in analysing the practice of the Court of Justice of the European Union regarding the legality of restrictions on a person's right to privacy and in identifying the conditions and limits of the application of the principle of proportionality as the main legal test for assessing the right to privacy and protection of personal data. Together with these methods, the linguistic method was actively used in order to determine the differences in concepts that may arise due to the value of different concepts in the Lithuanian and English languages. The purpose of applying these methods is to investigate the former and current legal regulation of the transfer of personal data from the European Union to the United States; the legal regulation of the grounds for limiting the right to privacy in the European Union and the United States.

The practice of the Court of Justice of the European Union was analysed and explained using the teleological research method. This method was used in order to evaluate the importance of the interpretations formed by the court, to reveal their meaning and context, and to apply these insights to relevant legal regulation and to draw

conclusions about the necessary changes in the personal data transfer model. This method was extremely significant in revealing the content and main idea of the interpretations of the Court of Justice of the European Union.

The method of scientific literature analysis is used to reveal the views of European Union, American and Lithuanian scientists regarding the legality of restrictions on the right to privacy and personal data protection and the results of their research. The application of this method made it possible to reveal the dominant critical approach among American researchers regarding the interpretations of the Court of Justice of the European Union in the *Schrems II* case, to understand the positions supporting it and why this court is accused of being hypocritical.

The protection of an individual's right to privacy in cyberspace is characterized by rapid changes due to the technological development of electronic communications and technology. These changes are caused by unexpected, but extremely significant events for societies, such as the information disclosed by whistle-blowers (in the case of Edward Snowden), or even the decisions of individual economic entities that affect the users of their products or services around the world (e.g. companies like Facebook, Apple, Google, etc.). Therefore, the monitoring method is applied in order to have relevant information on the research topic, to be able to understand the reasons for specific decisions or the positions of foreign scientists, to forecast future changes in legal regulation or the need for those changes, before changes to legal acts or scientific publications on relevant issues appear.

The unstructured interview method is applied to the determination and disclosure of legal regulation issues, taking into account the interpretations of the Court of Justice of the European Union. The author discussed the research topic with prof. Aurelijus Gutauskas, Chairman of the Criminal Cases Department of the Supreme Court of Lithuania, during his internship in Poland - with prof. Dorota Lis-Staranowicz, prof. Marcin Dabrowski, as well as with other scientists from the University of Warmia and Mazury during seminars. During the interview, all experts were asked different questions, formed taking into account the information provided by each expert and the field of research.

## CONCLUSIONS

1. Based on the analysis performed, it can be concluded that the concept of national security is not defined in the legal systems of Lithuania, the European Union or the United States of America. A regulatory analysis of all these legal systems reveals that they lack a clear indication of the possible limits of the concept of national security. In particular, the line between intelligence activities (which protects national security) and criminal intelligence (which is based on the fight against crime) is unclear, as it is generally agreed that, for example, the fight against terrorism is conducted by states for the both purposes of protecting national security and preventing crime. Therefore, states, in order to limit individuals' right to privacy and justify access to personal data, may do so on different legal bases and according to different rules - either according to the legal mechanism of national security protection, or for the purposes of crime prevention. In the absence of conceptual boundaries to the concept of national security, law enforcement and intelligence agencies may abuse the grounds available to them for restricting the right to privacy. In order to minimize this risk, it is recommended to establish specific criteria in the legal regulation of Lithuania that would allow identification of the assignment of an activity to the area of national security protection and enable drawing boundaries between intelligence and criminal intelligence activities.

2. Regarding the protection of the right to privacy in the interaction of different legal systems, taking into account the legal bases of the transfer of personal data according to the GDPR, their mutual relationship and dependence:

2.1. data controllers or processors wishing to transfer data to United States of America (a third country) after the Court of Justice of the European Union annulled the *Privacy Shield Agreement* cannot themselves provide data subjects with a "substantially equivalent level of protection to that guaranteed in the European Union" because they cannot grant any rights or guarantees to data subjects that could "improve" the situation of data subjects in relation to American authorities' unrestricted access to their personal data and bulk collection of personal data.

2.2. despite the controversial regulation of GDPR preamble p. 107 and Article 44, the transfer of personal data from the European Union to a third country, territory or international organization cannot be considered legal if the previous legal basis for the transfer of personal data based one of the methods established in Chapter V (e.g. the *Privacy Shield Agreement*, concluded on the basis of Art. 45 d. 3 of GDPR) has been

annulled for reasons beyond the control of the data controller or processor operating in the third country and their possible application of exemplary adequate safeguards within the meaning of Chapter V of the GDPR.

3. Regarding the practice of the Court of Justice of the European Union related to the protection of the individual's right to privacy and personal data and significant legal regulatory obstacles in the American legal system that prevent the successful transfer of personal data from the European Union to the United States of America:

3.1. The analysis of the decision of the Court of Justice of the European Union in the case of *Digital Rights Ireland* allows us to conclude that the obligation of entities providing electronic communications to store available traffic and location data for the prescribed period (in *Digital Rights Ireland* case - 6 - 24 months) for the prevention, detection, investigation of crime, as well as for the purposes of ensuring state security, is disproportionate and illegal. However, this court decision does not allow us to draw a clear conclusion whether such actions can be legal in general, in the presence of a different legal regulation and in the presence of additional measures to ensure the right to privacy and protection of personal data, which data subjects could use.

3.2. The analysis of the decision of the Court of Justice of the European Union in the *Schrems* case allows us to conclude that the agreement between the European Union and the United States (in the case of the *Schrems* case - the *Safe Harbor Agreement*) cannot be considered to ensure adequate protection of individuals' right to privacy and protection of personal data in the US legal system, when the agreement establishes that the principled of right to privacy protection generally do not apply to United States of America government agencies or when American law enforcement and intelligence agencies are granted access to personal data of European Union users transferred to American entities without procedural safeguards to defend their potentially infringed rights on United States of America territory.

3.3. The analysis of the decision of the Court of Justice of the European Union in the *Schrems II* case leads to the conclusion that the GDPR applies to the transfer of personal data carried out by an economic entity established in a member state to another economic entity established in a third country, if during this transfer or after it the authorities of this third country can process this data for the purposes of public safety, defense and national security. Therefore, the greatest challenge to possible agreements on data transfer between the European Union and the United States of America is the assessment of the compliance of national security measures (e.g. mass surveillance)

applied by the United States of America with regard to the GDPR.

4. Regarding the application of the principle of proportionality as a criteria for assessing the legality of the limitation of the fundamental right when solving the problem of the protection of the right to privacy in the interaction of different legal systems:

4.1. In the context of European Union law, the principle of proportionality is one of the most significant legal concepts that can help establish a reasonable balance between the competition of public interests (e.g. the right to privacy and the protection of national security). Therefore, it can be considered to be the key to correct decision regarding the determination of the legality of restrictions on the protection of a person's right to privacy, including justifying the restriction of the right to privacy and protection of personal data, applied for the purposes of ensuring the national security of a third country.

4.2. According to the decision of the Court of Justice of the European Union in the *Schrems II* case, the *Privacy Shield Agreement* itself violates the essence of the fundamental right to privacy. Establishing such a violation (i.e. the essence of the right to privacy) eliminates the need to apply the principle of proportionality and perform an analysis of competing interests and the search for their correct balance. Having established a violation of the essence of the right to privacy and data protection, the disproportionality of the restrictions on the right to privacy in the American legal system cannot be mitigated even taking into account effective remedies, if such would be granted to European Union data subjects in the United States of America on the basis of the Privacy Shield Agreement.

4.3. With the decision of the Court of Justice of the European Union in the *Schrems II* case regarding the annulment of the *Privacy Shield Agreement*, the United States of America or any other third party that wishes to be recognized as ensuring an adequate level of the right to privacy and protection of personal data in the sense of Chapter V of the GDPR, is indirectly forced waive the implementation of its national security interests to the data received from the European Union. Therefore, in the *Schrems II* case, the Court of Justice of the European Union prevented the conclusion of an agreement on the transfer of personal data between the European Union and another legal system (including the United States of America), unless the third party renounces the implementation of its national security interest in relation to the data received from the European Union.

5. With regard to the necessary changes of right to privacy protection in the American legal system in order to legalize the transfer of personal data from the European Union to the United States of America:

5.1. Given the fact that giving American authorities unlimited access to data received from European Union entities violates the essence of the right to privacy and protection of personal data, in order to reach a long-term agreement on the transfer of personal data between the European Union and the United States of America, the American legal system should limit law access of law enforcement and intelligence agencies to different categories of data, for example by granting access only to the data of individuals linked to serious crimes or posing an immediate and reasonable threat to national security, rather than access to bulk data.

5.2. Given that the proportionality of restrictions to the right of privacy may depend on the existence of procedural safeguards available to data subjects, an acceptable model for effective protection of individual's rights violations is possible in the American legal system by implementing the following key changes: (i) expanding the role of an independent entity (e.g., an ombudsman, which was established under the *Privacy Shield Agreement*) powers and authorizing it to make binding decisions for law enforcement and intelligence services (including those related to Executive Order No. 12333), (ii) providing independent entity with clear guarantees of independence from the executive branch, (iii) consolidating individual complaints examination model characterized by at least a limited adversarial principle, for example, by not disclosing to a person the content and scope of information collected in relation to him, but ensuring that a competent and independent entity could impartially and reasonably examine a person's complaint about law enforcement or reasonableness of the actions of catering institutions.

**Publications on the topic of the dissertation**

1. „*E. Privatumo direktyvos įgyvendinimo problemos ir jų sprendimai e. Privatumo reglamento projekte*“. Journal “Law”, 2019, Vol. 113, pp. 139–154.;

2. “*Restrictions of Criminal Intelligence Measures in Law Enforcement Directive and Law on Criminal Intelligence of Lithuania*“. SOCRATES Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law, 2020, Nr. 3 (18);

3. „*Efektyvi teisės į privatų gyvenimą apsauga taikant kriminalinės žvalgybos priemones*“, Vytauto Magnus University Journal “Law Review“, 2021, Nr. 1 (23).

**Presentations at conferences on the topic of dissertation**

2020-11-23 presentation “*Efficiency of Criminal Intelligence Measures in the Context of Privacy*” in Ukraine Yaroslav Mudryi National University Faculty of Law conference “*Legal Autumn*“. A report on the subject of the presentation given was also printed in the journal of the international scientific conference “*Legal Autumn*”;

2020-10-14 presentation “*Criminal Intelligence vs Right to Private Life*“ in Mykolas Romeris University international conference “Sustainability in the presence of a global crisis”.

**Academic internship**

2021-05-10 – 2021-05-21 – academic internship in University of Warmia and Mazury in Olsztyn, Poland.

## Curriculum Vitae

**Education**

2015–2021 – doctoral studies in the Law School at Mykolas Romeris University
2008 – Master of Law (Vilnius University)

**Work experience**

From 2017 – Head of Public Procurement Department in Vilnius University
2014–2017 – Head of Public Procurement Department in Vilnius University Hospital Santaros Clinics

Markevičius, Edgaras

ASMENS DUOMENŲ PERDAVIMO ELEKTRONINĖJE ERDVĖJE TARP EUROPOS SĄJUNGOS IR JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINĖS PROBLEMOS: daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2022. P. 232.

Bibliogr. 160-185 p.

*Šis tyrimas yra skirtas išanalizuoti asmens duomenų perdavimo elektroninėje erdvėje problemas, sąveikaujant Europos Sąjungos ir JAV teisinėms sistemoms – galimų asmens duomenų perdavimo iš Europos Sąjungos į JAV teisinių pagrindų sąlygas, atsižvelgiant į nacionalinio saugumo interesų apsaugą ir Europos Sąjungos Teisingumo Teismo suformuotą praktiką šiuo aspektu. Atlikdamas šį tyrimą, Europos Sąjungos Teisingumo Teismo išaiškinimuose Schrems II byloje, autorius užčiuopė kertinį probleminį teisės į privatumą ir asmens duomenų apsaugos aspektą, susijusį su trečiosios šalies nacionalinio saugumo intereso įgyvendinimu. Remiantis Europos Sąjungos Teisingumo Teismo išaiškinimais, trečiosios šalies interesas turėti prieigą prie iš Europos Sąjungos subjektų gaunamų asmens duomenų, ginant savo nacionalinį saugumą, yra vertinamas pagal žymiai griežtesnius kriterijus, nei pačių Europos Sąjungos valstybių narių ir, autoriaus vertinimu, yra iš esmės paneigiamas. Todėl tyrime yra analizuojama nacionalinio saugumo samprata, ir, atsižvelgiant į, pirmiausiai, Europos Sąjungos Teisingumo Teismo išaiškinimus bylose Schrems ir Schrems II bei proporcingumo principo, kaip pagrindinio teisinio testo, taikomo vertinant asmens teisės į privatumą ir asmens duomenų apsaugą ribojimų teisėtumą, mėginama nustatyti, ar asmens duomenų perdavimo tarp Europos Sąjungos ir JAV gali būti laikomas teisėtu, ar ne. Galiausiai, tyrime yra pateikiami pasiūlymai dėl galimų JAV teisinio reguliavimo pakeitimų, siekiant užtikrinti asmens duomenų perdavimo tarp Europos Sąjungos ir JAV teisėtumą.*

*This study is intended to analyze the problems of personal data transfer in cyber space, in the interaction of the European Union and the American legal systems - the conditions of possible legal grounds for the transfer of personal data from the European Union to the United States of America, taking into account the protection of national security interests and the practice formed by the Court of Justice of the European Union in this aspect. In carrying out this research, in the interpretations of the Court of Justice of the European Union in the Schrems II case, the author identified a key problematic aspect*

*of the right to privacy and protection of personal data related to the implementation of the third country's national security interest. According to the interpretations of the Court of Justice of the European Union, third country's interest in having access to personal data obtained from the entities of the European Union, in defense of its national security, is evaluated according to much stricter criteria than those of the European Union member states themselves and, in the author's opinion, is essentially negated. Therefore, the study analyzes the concept of national security and, taking into account, first of all, the rulings of the Court of Justice of the European Union in cases Schrems and Schrems II and the principle of proportionality, as the main legal test for assessing the legality of restrictions on a person's right to privacy and protection of personal data, tries to determine, whether the transfer of personal data between the European Union and the United States can be considered legal or not. Finally, the study entails proposals for possible changes to legal regulation in the United States of America to ensure the legality of personal data transfer between the European Union and the United States of America.*

Edgaras Markevičius

# ASMENS DUOMENŲ PERDAVIMO ELEKTRONINĖJE ERDVĖJE TARP EUROPOS SĄJUNGOS IR JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINĖS PROBLEMOS

Daktaro disertacija
Socialiniai mokslai, teisė (S 001)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz.

Parengė spaudai Jovita Jankauskienė

Spausdino UAB „Šiaulių spaustuvė“
P. Lukšio g. 9G, 76200 Šiauliai
El. p. info@dailu.lt
https://siauliuspaustuve.lt