GENERALINIO ADVOKATO
HENRIK SAUGMANDSGAARD ØE IŠVADA,
pateikta 2019 m. gruodžio 19 d.[1]

Byla C-311/18

Data Protection Commissioner
prieš
Facebook Ireland Limited,
Maximilian Schrems,
dalyvaujant:
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

(*High Court* (Aukštasis Teismas, Airija) pateiktas prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Fizinių asmenų apsauga tvarkant asmens duomenis – Reglamentas (ES) 2016/679 – 2 straipsnio 2 dalis – Taikymo sritis – Asmens duomenų perdavimas komerciniais tikslais į Jungtines Amerikos Valstijas – Jungtinių Amerikos Valstijų valdžios institucijų atliekamas perduotų duomenų tvarkymas nacionalinio saugumo tikslais – 45 straipsnis – Trečiojoje šalyje užtikrinamo apsaugos lygio tinkamumo vertinimas – 46 straipsnis – Duomenų valdytojo užtikrinamos tinkamos apsaugos priemonės – Standartinės apsaugos sąlygos – 58 straipsnio 2 dalis – Nacionalinių priežiūros institucijų įgaliojimai – Sprendimas 2010/87/ES – Galiojimas – Įgyvendinimo sprendimas (ES) 2016/1250 – JAV ir ES „privatumo skydas“ – Galiojimas – Europos Sąjungos pagrindinių teisių chartijos 7, 8 ir 47 straipsniai“

Turinys

I. Įvadas 3

II. Teisinis pagrindas 5

A. Direktyva 95/46/EB 5

B. BDAR 6

C. Sprendimas 2010/87 10

1 Originalo kalba: prancūzų.

D. Sprendimas dėl „privatumo skydo“ 15

III. Pagrindinė byla, prejudiciniai klausimai ir procesas Teisingumo Teisme 15

IV. Analizė 24

A. Įvadinės pastabos 24

B. Dėl prašymo priimti prejudicinį sprendimą priimtinumo 25

1. Dėl Direktyvos 95/46 taikytinumo „ratione temporis“ 25

2. Dėl DPC išreikštų abejonių negalutinio pobūdžio 26

3. Dėl neaiškumų, susijusių su faktinių aplinkybių nustatymu 27

C. Dėl Sąjungos teisės taikytinumo asmens duomenų perdavimui komerciniais tikslais į trečiąją valstybę, kuri gali juos tvarkyti nacionalinio saugumo tikslais (pirmasis klausimas) 28

D. Dėl apsaugos lygio, reikalaujamo perduodant duomenis remiantis standartinėmis sutarčių sąlygomis (šeštojo prejudicinio klausimo pirma dalis) 29

E. Dėl Sprendimo 2010/87 galiojimo atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius (septintasis, aštuntasis ir vienuoliktasis prejudiciniai klausimai) 31

1. Dėl duomenų valdytojams tenkančių įpareigojimų 32

2. Dėl priežiūros institucijoms tenkančių įpareigojimų 34

F. Dėl būtinybės atsakyti į kitus prejudicinius klausimus ir nagrinėti sprendimo dėl „privatumo skydo“ galiojimą nebuvimo 37

1. Dėl to, kad Teisingumo Teismo atsakymai nėra reikalingi, atsižvelgiant į pagrindinės bylos dalyką 38

2. Dėl priežasčių, kodėl Teisingumo Teismas, nagrinėdamas šią bylą, neturėtų atsižvelgti į DPC vykdomos procedūros dalyką 40

G. Papildomos pastabos, susijusios su sprendimo dėl „privatumo skydo“ padariniais ir galiojimu 42

1. Dėl sprendimo dėl „privatumo skydo“ poveikio, priežiūros institucijai nagrinėjant skundą dėl sutartinėmis garantijomis grindžiamo duomenų perdavimo teisėtumo 42

2. Dėl sprendimo dėl „privatumo skydo“ galiojimo 43

a) Patikslinimai, susiję su sprendimo dėl tinkamumo galiojimo analizės turiniu 44

1) Dėl lyginimo sąlygų, leidžiančių įvertinti, ar apsaugos lygis yra „iš esmės toks pats“ .. 44

2) Dėl būtinybės užtikrinti tinkamą duomenų apsaugos lygį duomenų perdavimo etapu 49

3) Dėl atsižvelgimo į Komisijos ir prašymą priimti prejudicinį sprendimą pateikusio teismo konstatuotas faktines aplinkybes, susijusias su JAV teise 50

4) Dėl „esminio tapatumo“ reikalavimo taikymo srities 52

b) Dėl sprendimo dėl „privatumo skydo“ galiojimo atsižvelgiant į teisę į privataus gyvenimo gerbimą ir teisę į asmens duomenų apsaugą 53

1) Dėl ribojimų buvimo 53

2) Dėl to, ar ribojimai yra „numatyti įstatymo“ 54

3) Dėl poveikio pagrindinių teisių esmei nebuvimo 56

4) Dėl teisėto tikslo siekimo 59

5) Dėl ribojimų būtinumo ir proporcingumo 60

c) Dėl sprendimo dėl „privatumo skydo“ galiojimo atsižvelgiant į teisę į veiksmingą teisinę gynybą 63

1) Dėl JAV teisėje numatytų teisminių teisių gynimo priemonių veiksmingumo 64

2) Dėl ombudsmeno institucijos poveikio teisės į veiksmingą teisinę gynybą apsaugos lygiui 67

V. Išvada 69

I. Įvadas

1. Nesant bendrų pasauliniu lygmeniu taikomų garantijų asmens duomenų apsaugos srityje kyla grėsmė, kad, siunčiant šių duomenų srautus tarp valstybių, nebebus užtikrinamas Sąjungoje suteikiamas duomenų apsaugos lygis. Siekdamas palengvinti šiuos srautus ir apriboti šią grėsmę Sąjungos teisės aktų leidėjas nustatė tris mechanizmus, kuriuos taikant asmens duomenys gali būti perduodami iš Sąjungos į trečiąją valstybę.

2. Pirma, asmens duomenys gali būti perduodami į trečiąją valstybę remiantis sprendimu, kuriuo Europos Komisija nustato, kad atitinkama trečioji valstybė užtikrina į ją perduodamų duomenų „tinkamo lygio apsaugą“ [2]. Antra, jeigu tokio sprendimo nėra, duomenis perduoti leidžiama, jei taikomos „tinkamos apsaugos priemonės“ [3]. Šios apsaugos priemonės gali būti duomenų eksportuotojo ir duomenų importuotojo sudaryta sutartis, į kurią įtrauktos Komisijos priimtos standartinės duomenų apsaugos sąlygos. Trečia, BDAR numatytos tam tikros leidžiančios nukrypti nuostatos, grindžiamos, be kita ko, duomenų subjekto sutikimu, pagal kurias duomenis į trečiąją valstybę leidžiama perduoti net nesant sprendimo dėl tinkamumo ar tinkamų apsaugos priemonių [4].

2 Žr. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016, p. 1) (toliau – BDAR) 45 straipsnį.

3 Žr. BDAR 46 straipsnį.

4 Žr. BDAR 49 straipsnį.

3. *High Court* (Aukštasis Teismas, Airija) pateiktas prašymas priimti prejudicinį sprendimą susijęs su antruoju iš šių mechanizmų. Kalbant konkrečiau, jis susijęs su Sprendimo 2010/87/ES[5], kuriuo Komisija nustatė sutarčių standartines sąlygas kai kurioms perduodamų duomenų kategorijoms, atsižvelgiant į Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7, 8 ir 47 straipsnius.

4. Šis prašymas buvo pateiktas nagrinėjant *Data Protection Commissioner* (Duomenų apsaugos komisaras, Airija, toliau – DPC), *Facebook Ireland Ltd* ir Maximillian Schrems ginčą. Šis asmuo padavė skundą DPC dėl bendrovės *Facebook Ireland* perduotų jo asmens duomenų jos patronuojančiajai bendrovei *Facebook Inc.*, įsteigtai Jungtinėse Amerikos Valstijose (toliau – JAV). DPC nuomone, šio skundo nagrinėjimas priklauso nuo to, ar Sprendimas 2010/87 galioja. Šiomis aplinkybėmis jis kreipėsi į prašymą priimti prejudicinį sprendimą pateikusį teismą, prašydamas pateikti Teisingumo Teismui prašymą priimti prejudicinį sprendimą šiuo klausimu.

5. Pirmiausia reikėtų nurodyti, kad, mano nuomone, prejudicinių klausimų analizė neatskleidė jokios informacijos, kuri turėtų poveikį Sprendimo 2010/87 galiojimui.

6. Prašymą priimti prejudicinį sprendimą pateikęs teismas taip pat iškėlė kelias abejones, iš esmės susijusias su JAV užtikrinamo apsaugos lygio tinkamumu, atsižvelgiant į JAV žvalgybos institucijų taikomus asmenų, kurių duomenys perduodami į šią trečiąją valstybę, pagrindinių teisių įgyvendinimo ribojimus. Šiomis abejonėmis netiesiogiai kvestionuojami Komisijos vertinimai, kuriuos ji pateikė šiuo klausimu Įgyvendinimo sprendime (ES) 2016/1250[6]. Nors siekiant išspręsti pagrindinėje byloje kilusį ginčą Teisingumo Teismui nėra būtinybės nagrinėti šio klausimo, todėl siūlau jo nenagrinėti, papildomai nurodysiu priežastis, dėl kurių man kyla klausimų dėl šio sprendimo galiojimo.

7. Visa mano analizė bus grindžiama siekiu surasti pusiausvyrą tarp, viena vertus, būtinybės laikytis „pagrįstai pragmatiško požiūrio, kad būtų įmanoma sąveika su likusiu pasauliu“[7], ir, kita vertus, būtinybės įtvirtinti pagrindines vertybes, pripažįstamas Sąjungos ir jos valstybių narių teisės sistemose, visų pirma Chartijoje.

5 2010 m. vasario 5 d. Komisijos sprendimas dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas (OL L 39, 2010, p. 5), iš dalies pakeistas 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimu (ES) 2016/2297 (OL L 344, 2016, p. 100) (toliau – Sprendimas 2010/87).

6 2016 m. liepos 12 d. Komisijos sprendimas dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal [Direktyvą 95/46] (OL L 207, 2016, p. 1; toliau – sprendimas dėl „privatumo skydo“).

7 Žr. buvusio Europos asmens duomenų apsaugos priežiūros pareigūno (EDAPP) P. Hustinx diskursą „Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données“, p. 49, pateikiamas adresu https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf

II. Teisinis pagrindas

A. Direktyva 95/46/EB

8. Direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo [8] 3 straipsnio 2 dalyje buvo nurodyta:

„Ši direktyva netaikoma tvarkant asmens duomenis:

– kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, kaip antai veikla, kuri numatyta Europos Sąjungos sutarties V ir VI dalyse, taip pat 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;

<…>“

9. Šios direktyvos 13 straipsnio 1 dalis buvo suformuluota taip:

„Valstybės narės gali priimti teisines priemones, kad apribotų 6 straipsnio 1 dalyje, 10 straipsnyje, 11 straipsnio 1 dalyje bei 12 ir 21 straipsniuose numatytų prievolių ir teisių mastą, kai toks apribojimas yra reikalinga apsaugos priemonė norint užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

d) kriminalinių nusikaltimų bei reglamentuojamų profesijų etikos pažeidimų prevenciją, tyrimą, išaiškinimą ir persekiojimą;

e) svarbius ekonominius ar finansinius valstybės narės ar Europos Sąjungos interesus, įskaitant ir monetarinius, biudžeto ar mokesčių klausimus;

f) kontrolės, tikrinimo ar taisyklių nustatymo funkciją, kuri susijusi, bent atsitiktinai, su įgaliojimų vykdymu c, d ir e punktuose nurodytais atvejais;

g) duomenų subjekto apsaugą arba kitų asmenų teisių ir laisvių apsaugą.“

10. Minėtos direktyvos 25 straipsnyje buvo nurodyta:

„1. Valstybės narės numato, kad asmens duomenys, kurie yra tvarkomi arba kuriuos juos perdavus ketinama tvarkyti, gali būti perduodami į trečiąją šalį tik tuo atveju, jeigu nepažeidžiant nacionalinių nuostatų, priimtų pagal kitas šios direktyvos nuostatas, ši trečioji šalis užtikrina adekvatų apsaugos lygį.

8 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k., 13 sk., 15 t., p. 355), iš dalies pakeista 2003 m. rugsėjo 29 d. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 1882/2003 (OL L 284, 2003, p. 1; 2004 m. specialusis leidimas lietuvių k., 1 sk., 4 t., p. 447), toliau – Direktyva 95/46.

2. Apsaugos, kurią suteikia trečioji šalis, lygio adekvatumas įvertinamas atsižvelgiant į [visas] duomenų perdavimo operacijos ar operacijų grupės aplinkybes; ypatingas dėmesys atkreipiamas į duomenų pobūdį, siūlomos tvarkymo operacijos ar operacijų tikslą ir trukmę, duomenų kilmės bei paskirties valstybę ar valstybes, bendrųjų ir atskiriems sektoriams taikomų įstatymų, galiojančių trečiojoje šalyje, nuostatas, taip pat profesines taisykles ir saugumo priemones, kurių laikomasi toje valstybėje.

<…>

6. 31 straipsnio 2 dalyje nurodyta tvarka Komisija gali išsiaiškinti, kad adekvatų apsaugos lygį, kaip numatyta šio straipsnio 2 dalyje, trečioji šalis užtikrina savo šalies įstatymais arba tarptautiniais įsipareigojimais, kuriuos ji yra prisiėmusi, ypač po 5 dalyje nurodytų derybų dėl asmenų privataus gyvenimo ir pagrindinių laisvių bei teisių apsaugos.

Valstybės narės imasi reikalingų priemonių, kad būtų laikomasi Komisijos sprendimo.“

11. Tos pačios direktyvos 26 straipsnio 2 ir 4 dalyse buvo numatyta:

„2. Nepažeisdama šio straipsnio 1 dalies nuostatų, valstybė narė gali leisti perduoti asmens duomenis į trečiąją šalį, kuri neužtikrina adekvataus apsaugos lygio pagal 25 straipsnio 2 dalį, jeigu domenų valdytojas pateikia adekvačias apsaugos priemones asmenų privatumui ir pagrindinėms teisėms bei laisvėms apsaugoti ir atitinkamoms teisėms įgyvendinti; tokios apsaugos priemonės gali būti išdėstytos atitinkamuose sutarčių punktuose.

<…>

4. Jei <…> Komisija nusprendžia kad atitinkami standartiniai sutarčių punktai numato pakankamas apsaugos priemones, kaip reikalauja šio straipsnio 2 dalies nuostatos, valstybės narės imasi reikalingų priemonių, kad būtų laikomasi Komisijos sprendimo.“

12. Direktyvos 95/46 28 straipsnio 3 dalis buvo suformuluota taip:

„Kiekvienai valdžios institucijai suteikiami:

<…>

– įgaliojimai veiksmingai įsikišti, pavyzdžiui, įgaliojimai pareikšti nuomonę, iš anksto įvertinus tvarkymo operacijas pagal 20 straipsnį, ir užtikrinti, kad tokios nuomonės būtų tinkamu būdu skelbiamos viešai, taip pat įgaliojimai nurodyti blokuoti, ištrinti arba sunaikinti duomenis, laikinai arba visiškai uždrausti tvarkyti duomenis, įspėti arba papeikti duomenų valdytoją arba įgaliojimai perduoti klausimą nacionaliniams parlamentams ar kitoms politinėms institucijoms svarstyti,

<…>“

B. BDAR

13. Pagal BDAR 94 straipsnio 1 dalį šiuo reglamentu Direktyva 95/46 buvo panaikinta nuo 2018 m. gegužės 25 d., kai pagal jo 99 straipsnio 2 dalį pradėtas taikyti šis reglamentas.

14. BDAR 2 straipsnio 2 dalyje nurodyta:

„Šis reglamentas netaikomas asmens duomenų tvarkymui, kai:

a) duomenys tvarkomi vykdant veiklą, kuriai Sąjungos teisė netaikoma;

b) duomenis tvarko valstybės narės, vykdydamos veiklą, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius;

<…>

d) duomenis tvarko kompetentingos valdžios institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už jas, baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais.“

15. To paties reglamento 4 straipsnio 2 punkte duomenų tvarkymas apibrėžiamas kaip „bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas“.

16. BDAR 23 straipsnyje numatyta:

„1. Sąjungos ar valstybės narės teise, kuri taikoma duomenų valdytojui arba duomenų tvarkytojui, teisėkūros priemone gali būti apribotos 12–22 straipsniuose ir 34 straipsnyje, taip pat 5 straipsnyje tiek, kiek jo nuostatos atitinka 12–22 straipsniuose numatytas teises ir prievoles, nustatytos prievolės ir teisės, kai tokiu apribojimu gerbiama pagrindinių teisių ir laisvių esmė ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

d) užtikrinti nusikalstamų veikų prevenciją, tyrimą, atskleidimą, baudžiamąjį persekiojimą už jas, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir šių grėsmių prevenciją, arba bausmių vykdymą;

e) kitus Sąjungos ar valstybės narės svarbius tikslus, susijusius su bendrais viešaisiais interesais, visų pirma svarbiu ekonominiu ar finansiniu Sąjungos ar valstybės narės interesu <…>;

<…>

2. Visų pirma visose 1 dalyje nurodytose teisėkūros priemonėse pateikiamos konkrečios nuostatos, susijusios tam tikrais atvejais bent su:

a) duomenų tvarkymo tikslais arba duomenų tvarkymo kategorijomis,

b) asmens duomenų kategorijomis,

c) nustatytų apribojimų apimtimi,

d) apsaugos priemonėmis, kuriomis siekiama užkirsti kelią piktnaudžiavimui arba neteisėtam susipažinimui su duomenimis ar jų perdavimui,

e) duomenų valdytojo arba duomenų valdytojų kategorijų apibūdinimu,

f) saugojimo laikotarpiais ir taikytinomis apsaugos priemonėmis, atsižvelgiant į duomenų tvarkymo arba duomenų tvarkymo kategorijų pobūdį, aprėptį ir tikslus,

g) pavojais duomenų subjektų teisėms ir laisvėms, ir

h) duomenų subjektų teise būti informuotiems apie apribojimą, nebent tai pakenktų apribojimo tikslui.“

17. Šio reglamento 44 straipsnyje „Bendras duomenų perdavimo principas“ nurodyta:

„Asmens duomenys, kurie yra tvarkomi arba kuriuos ketinama tvarkyti juos perdavus į trečiąją valstybę arba tarptautinei organizacijai, perduodami tik tuo atveju, jei duomenų valdytojas ir duomenų tvarkytojas, laikydamiesi kitų šio reglamento nuostatų, laikosi šiame 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. Visos šio skyriaus nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui.“

18. Šio reglamento 45 straipsnyje „Duomenų perdavimas remiantis sprendimu dėl tinkamumo“ nustatyta:

„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

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.

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 numatomas periodinės peržiūros, atliekamos bent kas ketverius metus, kuria atsižvelgiama į visus atitinkamus pokyčius trečiojoje valstybėje ar tarptautinėje organizacijoje, mechanizmas. <…>

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] 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. <…>

6. Komisija pradeda konsultacijas su trečiąja valstybe arba tarptautine organizacija, siekdama, kad padėtis, dėl kurios buvo priimtas sprendimas pagal 5 dalį, būtų ištaisyta.

<…>

9. Sprendimai, kuriuos Komisija priėmė remdamasi [Direktyvos 95/46] 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.“

19. To paties reglamento 46 straipsnis „Duomenų perdavimas taikant tinkamas apsaugos priemones“ suformuluotas taip:

„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.

2. 1 dalyje nurodytos tinkamos apsaugos priemonės, nereikalaujant specialaus priežiūros institucijos leidimo, gali būti nustatomos:

<…>

c) standartinėmis duomenų apsaugos sąlygomis, kurias Komisija priima laikydamasi 93 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros;

<…>

5. Leidimai, kuriuos valstybė narė arba priežiūros institucija suteikė remdamasi [Direktyvos 95/46] 26 straipsnio 2 dalimi, lieka galioti tol, kol ta priežiūros institucija prireikus juos iš dalies pakeis, pakeis naujais leidimais arba panaikins. Sprendimai, kuriuos Komisija priėmė remdamasi [Direktyvos 95/46] 26 straipsnio 4 dalimi, lieka galioti tol, kol Komisijos sprendimu, priimtu pagal šio straipsnio 2 dalį, jie bus prireikus iš dalies pakeisti, pakeisti naujais sprendimais arba panaikinti.“

20. BDAR 58 straipsnio 2, 4 ir 5 dalyse nurodyta:

„2. Kiekviena priežiūros institucija turi visus šiuos įgaliojimus imtis taisomųjų veiksmų:

a) įspėti duomenų valdytoją arba duomenų tvarkytoją, kad numatomomis duomenų tvarkymo operacijomis gali būti pažeistos šio reglamento nuostatos;

b) pareikšti papeikimus duomenų valdytojui arba duomenų tvarkytojui, kai duomenų tvarkymo operacijomis buvo pažeistos šio reglamento nuostatos;

c) nurodyti duomenų valdytojui arba duomenų tvarkytojui patenkinti duomenų subjekto prašymus pasinaudoti savo teisėmis pagal šį reglamentą;

d) nurodyti duomenų valdytojui arba duomenų tvarkytojui suderinti duomenų tvarkymo operacijas su šio reglamento nuostatomis, tam tikrais atvejais – nustatytu būdu ir per nustatytą laikotarpį;

e) nurodyti duomenų valdytojui pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą;

f) nustatyti laikiną arba galutinį duomenų tvarkymo apribojimą, įskaitant tvarkymo draudimą;

<…>

i) skirti administracinę baudą pagal 83 straipsnį, kartu taikydama šioje dalyje nurodytas priemones arba vietoj jų, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes;

j) nurodyti sustabdyti duomenų srautus duomenų gavėjui trečiojoje valstybėje arba tarptautinei organizacijai.

<…>

4. Naudojimuisi pagal šį straipsnį priežiūros institucijai suteiktais įgaliojimais taikomos atitinkamos apsaugos priemonės, įskaitant veiksmingą apskundimą teismine tvarka ir tinkamą procesą, kaip nustatyta Sąjungos ir valstybės narės teisėje, laikantis Chartijos.

5. Kiekviena valstybė narė teisės aktais nustato, kad jos priežiūros institucija turi įgaliojimus atkreipti teisminių institucijų dėmesį į šio reglamento pažeidimus ir tam tikrais atvejais pradėti teismo procesą arba kitaip dalyvauti teismo procese siekiant užtikrinti šio reglamento nuostatų vykdymą.“

C. Sprendimas 2010/87

21. Pagal Direktyvos 95/46 26 straipsnio 4 dalį Komisija priėmė tris sprendimus, jais konstatavo, kad juose nustatytos sutarčių standartinės sąlygos užtikrina tinkamas apsaugos priemones ginant asmenų privatų gyvenimą ir pagrindines asmens teises ir laisves, susijusias su atitinkamų teisių įgyvendinimu (toliau – sprendimai dėl SSS) [9].

9 2001 m. birželio 15 d. Komisijos sprendimas 2001/497/EB dėl sutarčių, susijusių su asmens duomenų perdavimu trečiosioms šalims, tipinių punktų, atsižvelgiant į [Direktyvą 95/46] (OL L 181, 2001, p. 19; 2004 m. specialusis leidimas lietuvių k., 13 sk., 26 t., p. 347); 2004 m. gruodžio 27 d. Komisijos sprendimas 2004/915/EB, iš dalies keičiantis Sprendimą [2001/497] dėl sutarčių, susijusių su asmens duomenų perdavimu trečiosioms šalims, tipinių punktų (OL L 385, 2004, p. 74) ir Sprendimas 2010/87.

22. Vienas iš jų yra Sprendimas 2010/87, jo 1 straipsnyje nustatyta, kad „priede pateiktos standartinės sutarčių sąlygos laikomos užtikrinančiomis tinkamas apsaugos priemones pagal [Direktyvos 95/46] 26 straipsnio 2 dalies reikalavimus, ginant privatumo teisę ir pagrindines asmens teises ir laisves, susijusias su atitinkamų teisių įgyvendinimu“.

23. Šio sprendimo 3 straipsnyje nurodyta:

„Šio sprendimo tikslais taikomos šios apibrėžtys:

<…>

c) „duomenų eksportuotojas“ – duomenų valdytojas, kuris perduoda asmens duomenis;

d) „duomenų importuotojas“ – trečiojoje šalyje įsikūręs duomenų tvarkytojas, sutinkantis iš duomenų eksportuotojo gauti asmens duomenis ir gautus duomenis tvarkyti duomenų eksportuotojo vardu, laikydamasis jo duotų nurodymų bei šio sprendimo sąlygų, ir nepriklausantis trečiosios šalies tinkamos apsaugos užtikrinimo sistemai, kaip nustatyta [Direktyvos 95/46] 25 straipsnio 1 dalyje;

<…>

f) „taikytina duomenų apsaugos teisė“ – teisės aktai, ginantys pagrindines asmenų teises ir laisves (ypač jų teisę į privatų gyvenimą) tvarkant asmens duomenis, kurių turi laikytis duomenų valdytojas toje valstybėje narėje, kurioje įsikūręs duomenų eksportuotojas;

<…>“

24. Minėto sprendimo pirminės redakcijos 4 straipsnio 1 dalyje buvo numatyta:

„Nepažeidžiant valstybių narių kompetentingų institucijų teisės imtis veiksmų, kad būtų užtikrintas nacionalinių nuostatų, priimtų įgyvendinant [Direktyvos 95/46] II, III, V ir VI skyrių reikalavimus, vykdymas, jos gali pasinaudoti joms suteiktomis teisėmis uždrausti ar sustabdyti duomenų srautus į trečiąsias šalis, siekiant apsaugoti asmenis, kurių asmens duomenys yra tvarkomi. Šiomis teisėmis minėtosios institucijos gali pasinaudoti[, jeigu]:

a) nustatoma, kad teisės aktu, kurio turi laikytis duomenų importuotojas arba pagalbinis duomenų tvarkytojas, jam keliami reikalavimai verčia nukrypti nuo taikomos duomenų apsaugos teisės ir tie reikalavimai viršija [Direktyvos 95/46] 13 straipsnyje nustatytus apribojimus, reikalingus demokratinėje visuomenėje, jei tie reikalavimai gali ypač neigiamai paveikti taikytiname duomenų apsaugos teisėje ar standartinėse sutarčių sąlygose nustatytas garantijas;

b) kompetentinga institucija nustato, kad duomenų importuotojas arba pagalbinis duomenų tvarkytojas nevykdo priede pateiktų standartinių sutarčių sąlygų; arba

c) yra reali tikimybė, kad priede pateiktos standartinės sutarčių sąlygos yra nevykdomos arba bus nevykdomos ir kad toliau perduodant duomenis duomenų subjektams iškils didelės žalos grėsmė.“

25. To paties sprendimo aktualios redakcijos (po Sprendimo 2010/87 pakeitimo Įgyvendinimo sprendimu (ES) 2016/2297[10]) 4 straipsnyje nurodyta, kad „kai valstybių narių kompetentingos institucijos įgyvendina savo įgaliojimus pagal [Direktyvos 95/46] 28 straipsnio 3 dalį ir dėl šios priežasties sustabdomi arba neribotam laikui uždraudžiami duomenų srautai į trečiąsias šalis, kad apsaugotų asmenis atsižvelgiant į jų asmens duomenų tvarkymą, atitinkama valstybė narė nedelsdama informuoja Komisiją, kuri šią informaciją perduoda kitoms valstybėms narėms“.

26. Sprendimo 2010/87 priede pateikiamos visos standartinės sutarčių sąlygos. Visų pirma šio priedo 3 sąlygoje „Trečiosios šalies naudos gavėjos sąlyga“ numatyta:

„1. Duomenų subjektas gali iškelti ieškinį duomenų eksportuotojui kaip trečiajai šaliai naudos gavėjai pagal šią sąlygą, 4 sąlygos b–i punktus, 5 sąlygos a–e ir g–j punktus, 6 sąlygos 1–2 dalis, 7 sąlygą, 8 sąlygos 2 dalį ir 9–12 sąlygas.

2. Duomenų subjektas gali iškelti ieškinį duomenų importuotojui pagal šią sąlygą, 5 sąlygos a–e ir g punktus, 6 sąlygą, 7 sąlygą, 8 sąlygos 2 dalį ir 9–12 sąlygas tais atvejais, kai duomenų eksportuotojas yra faktiškai dingęs, teisiškai nutraukė savo veiklą arba tapo nemokus, išskyrus atvejus, kai visus duomenų eksportuotojo teisinius įsipareigojimus sutartimi arba teisiniais veiksmais perėmė veiklos tęsėjas. Jis prisiima duomenų eksportuotojo teises ir įsipareigojimus, ir tokiu atveju duomenų subjektas gali iškelti tokiai įstaigai ieškinį.

<…>“

27. Minėto priedo 4 sąlygoje „Duomenų eksportuotojo įsipareigojimai“ nurodyta:

„Duomenų eksportuotojas sutinka ir užtikrina, kad:

a) asmens duomenų tvarkymas, įskaitant jų perdavimą, yra ir bus vykdomas laikantis susijusių taikytinos duomenų apsaugos teisės nuostatų (ir, jei taikytina, apie jį pranešta atitinkamoms valstybės narės, kurioje įsikūręs duomenų eksportuotojas, institucijoms) ir juo nepažeidžiamos atitinkamos tos valstybės nuostatos;

b) jis davė nurodymus duomenų importuotojui ir visą asmens duomenų tvarkymo paslaugų laikotarpį duos nurodymus tvarkyti perduotus asmens duomenis tik duomenų eksportuotojo vardu ir laikantis taikytinos duomenų apsaugos teisės ir šių sąlygų;

c) duomenų importuotojas suteiks pakankamas garantijas, susijusias su techninėmis ir organizacinėmis saugumo priemonėmis, nustatytas šios sutarties 2 priedėlyje;

d) įvertinus taikytinos duomenų apsaugos teisės reikalavimus apsaugos priemonės yra tinkamos, kad asmens duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo arba nuo atsitiktinio praradimo, pakeitimo, nesankcionuoto atskleidimo arba nesankcionuotos prieigos prie jų, ypač tais atvejais, kai tvarkymo proceso metu duomenys perduodami tinklu, taip pat nuo visų kitų neteisėtų tvarkymo formų, ir kad šiomis priemonėmis užtikrinamas tinkamas apsaugos lygis atsižvelgiant į riziką, susijusią su tvarkymu, ir saugotinų duomenų pobūdį ir atsižvelgiant į tų priemonių modernumą bei jų įgyvendinimo išlaidas;

e) užtikrins saugumo priemonių laikymąsi;

10 2016 m. gruodžio 16 d. Komisijos sprendimas, kuriuo iš dalies keičiami sprendimai [2001/497] ir [2010/87] dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosioms šalims ir tokiose šalyse įsikūrusiems tvarkytojams pagal [Direktyvos 95/46] nuostatas (OL L 344, 2016, p. 100).

f) ypatingų kategorijų duomenų perdavimo atveju duomenų subjektui buvo pranešta arba bus pranešta prieš arba kuo greičiau po duomenų perdavimo, kad jo duomenys gali būti perduoti trečiajai šaliai, neužtikrinančiai reikiamos apsaugos pagal [Direktyvą 95/46];

g) persiųs bet kokį pranešimą, gautą iš duomenų importuotojo arba pagalbinio duomenų tvarkytojo pagal 5 sąlygos b punktą ir 8 sąlygos 3 dalį duomenų apsaugos priežiūros institucijai, jeigu duomenų eksportuotojas nusprendžia tęsti perdavimą arba nutraukti sustabdymą;

h) pagal pageidavimą pateiks duomenų subjektui šių sąlygų kopiją (išskyrus 2 priedėlį ir saugumo priemonių aprašymo santrauką) ir bet kokios sutarties dėl pagalbinio tvarkymo paslaugų, kuri buvo sudaryta laikantis šių sąlygų, kopiją, išskyrus atvejus, kai sąlygose arba sutartyje yra komercinės informacijos; tokiu atveju jis gali pašalinti tokią komercinę informaciją;

i) pagalbinio tvarkymo atveju tvarkymo veiklą pagal 11 sąlygą vykdo pagalbinis duomenų tvarkytojas, užtikrinantis bent tokį patį asmens duomenų ir duomenų subjekto teisių apsaugos lygį, kokį užtikrina duomenų importuotojas pagal šias sąlygas; ir

j) užtikrins atitiktį 4 sąlygos a–i punktams.“

28. To paties priedo 5 sąlygoje „Duomenų importuotojo įsipareigojimai([1])“ nurodyta:

„Duomenų importuotojas sutinka ir užtikrina, kad:

a) tvarkys asmens duomenis tik duomenų eksportuotojo vardu ir laikysis jo nurodymų ir šių sąlygų; jeigu jis dėl bet kokių priežasčių negali užtikrinti atitikties, jis sutinka kuo skubiau pranešti duomenų importuotojui apie tai, kad jis negali užtikrinti atitikties, ir tokiu atveju duomenų eksportuotojas turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį;

b) neturi pagrindo manyti, kad pagal jam taikytiną teisę jis negalės vykdyti iš duomenų eksportuotojo gautų nurodymų ir savo įsipareigojimų pagal sutartį, o jeigu ši teisė pakeičiama ir šie pakeitimai turi didelį neigiamą poveikį pagal šias sąlygas teikiamoms garantijoms ir prisiimtiems įsipareigojimams, jis kuo greičiau praneš apie šiuos pasikeitimus duomenų eksportuotojui, kai tik apie juos sužinos, o duomenų eksportuotojas tokiu atveju turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį;

c) prieš pradėdamas tvarkyti perduotus asmens duomenis jis įgyvendino 2 priedėlyje nustatytas technines ir organizacines saugumo priemones;

d) kuo greičiau praneš duomenų eksportuotojui apie:

   i) bet kokį teisiškai įpareigojantį teisėsaugos institucijų prašymą atskleisti asmens duomenis, išskyrus atvejus, kai tai draudžiama, pvz., draudimas pagal baudžiamąją teisę, kuriuo siekiama užtikrinti teisėsaugos institucijų vykdomo tyrimo konfidencialumą;

   ii) bet kokią atsitiktinę arba nesankcionuotą prieigą prie duomenų; ir

   iii) bet kokius tiesioginius duomenų subjektų prašymus, neatsakydamas į juos, išskyrus atvejus, kai jis turi leidimą tai daryti;

e) greitai ir tinkamai atsakys į visas duomenų eksportuotojo užklausas, susijusias su jo vykdomu perduoti skirtų asmens duomenų tvarkymu, ir laikysis priežiūros institucijos rekomendacijų, susijusių su perduotų duomenų tvarkymu;

f) duomenų eksportuotojo prašymu leis atlikti savo duomenų tvarkymo priemonių auditą, kiek tai susiję su šių sąlygų apimama duomenų tvarkymo veikla, kurį atliks duomenų eksportuotojas arba tikrinimo grupė, sudaryta iš nepriklausomų narių, kurie turi reikiamą profesinę kvalifikaciją, yra saistomi pasižadėjimo saugoti konfidencialumą ir kuriuos atrinko duomenų eksportuotojas, kai taikytina, suderinęs tai su priežiūros institucija;

<…>“

29. Sprendimo 2010/87 priede esančios 5 sąlygos 1 išnašoje nurodyta:

„Duomenų importuotojui taikytini privalomi nacionalinių teisės aktų reikalavimai, kurie, atsižvelgiant į [Direktyvos 95/46] 13 straipsnio 1 dalį, neviršija demokratinėje visuomenėje reikalingų apribojimų, t. y. jeigu jie yra būtina priemonė užtikrinti nacionalinį saugumą, gynybą, visuomenės saugumą, baudžiamųjų nusikaltimų bei reglamentuojamų profesijų etikos pažeidimų prevenciją, tyrimą, išaiškinimą ir persekiojimą, svarbius valstybės ekonominius bei finansinius interesus, apsaugoti duomenų subjektą arba kitų asmenų teises ir laisves, neprieštarauja standartinėms sutarčių sąlygoms. Tokių privalomų reikalavimų, kurie neviršija demokratinėje visuomenėje reikalingų apribojimų, yra, *inter alia*, tarptautiniu mastu pripažintos sankcijos, mokestinių ataskaitų reikalavimai arba pinigų plovimo prevencijos ataskaitų reikalavimai.“

30. Šiame priede esanti 6 sąlyga „Atsakomybė“ suformuluota taip:

„1. Šalys susitaria, kad bet koks duomenų subjektas, kuriam bet kuri šalis arba pagalbinis duomenų tvarkytojas padarė žalą, nes neįvykdė 3 arba 11 sąlygoje nustatytų įsipareigojimų, turi teisę gauti kompensaciją iš duomenų eksportuotojo dėl patirtos žalos.

2. Jeigu duomenų subjektas negali reikalauti kompensacijos, kaip nustatyta 1 dalyje, iš duomenų eksportuotojo dėl duomenų importuotojo arba jo pagalbinio duomenų tvarkytojo padaryto bet kurio iš jų įsipareigojimų, įvardytų 3 arba 11 sąlygose, pažeidimo dėl to, kad duomenų eksportuotojas yra faktiškai dingęs, teisiškai nutraukė savo veiklą arba tapo nemokus, duomenų importuotojas sutinka, kad duomenų subjektas gali iškelti ieškinį duomenų importuotojui, tarytum jis būtų duomenų eksportuotojas, išskyrus atvejį, kai visus duomenų eksportuotojo teisinius įsipareigojimus sutartimi arba teisiniais veiksmais perėmė veiklos tęsėjas; tokiais atvejais duomenų subjektas gindamas savo teises gali iškelti ieškinį tokiam tęsėjui.

<…>“

31. Šiame priede esančioje 7 sąlygoje „Tarpininkavimas ir jurisdikcija“ nurodyta:

„1. Duomenų importuotojas sutinka, kad jeigu duomenų subjektas prieš jį pasinaudoja trečiosios šalies naudos gavėjos teisėmis ir (arba) pareikalauja kompensuoti žalą pagal šias sąlygas, duomenų importuotojas sutiks su duomenų subjekto sprendimu:

a) kreiptis dėl ginčo į tarpininką, kurio vaidmenį atliktų nepriklausomas asmuo arba, kai taikytina, priežiūros institucija;

b) kreiptis dėl ginčo į valstybės narės, kurioje įsisteigęs duomenų eksportuotojas, teismą.

2. Šalys sutinka, kad duomenų subjekto pasirinkimas nepažeis jo esminių arba procedūrinių teisių imtis teisių gynimo priemonių pagal kitas nacionalinės arba tarptautinės teisės nuostatas.“

32. To paties priedo 9 sąlygoje „Reglamentuojantys teisės aktai“ numatyta, kad standartinės sutarčių sąlygos reglamentuojamos valstybės narės, kurioje įsikūręs duomenų eksportuotojas, teisės.

D. Sprendimas dėl „privatumo skydo“

33. Komisija, remdamasi Direktyvos 95/46 25 straipsnio 6 dalimi, iš eilės priėmė du sprendimus, jais konstatavo, kad JAV užtikrina tinkamą asmens duomenų, perduodamų JAV įsteigtoms įmonėms, pareiškusioms, kad, taikydamos autosertifikavimo procedūrą, laikysis šiuose sprendimuose įtvirtintų principų, apsaugos lygį.

34. Pirmiausia Komisija priėmė Sprendimą 2000/520/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“ [11]. 2015 m. spalio 6 d. Sprendime *Schrems* [12] Teisingumo Teismas pripažino šį sprendimą negaliojančiu.

35. Po šio Teisingumo Teismo sprendimo Komisija priėmė sprendimą dėl „privatumo skydo“.

36. Šio sprendimo 1 straipsnyje nurodyta:

„1. Atsižvelgdamos į [Direktyvos 95/46] 25 straipsnio 2 dalį, Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos pagal ES ir JAV „privatumo skydą“ Sąjunga perdavė Jungtinių Amerikos Valstijų organizacijoms, apsaugos lygį.

2. ES ir JAV „privatumo skydą“ sudaro 2016 m. liepos 7 d. JAV komercijos departamento paskelbti privatumo principai, kurie išdėstyti II priede ir oficialiuose pareiškimuose ir įsipareigojimuose, kurie pateikti I, III–VII prieduose nurodytuose dokumentuose.

3. Pagal šio straipsnio 1 dalį asmens duomenys perduodami pagal ES ir JAV „privatumo skydą“ tais atvejais, kai jie iš Sąjungos perduodami Jungtinių Amerikos Valstijų organizacijoms, įrašytoms į „privatumo skydo“ sąrašą, kurį pagal II priede išdėstytų privatumo principų I ir III skirsnius tvarko ir viešai skelbia JAV komercijos departamentas.“

37. Šio sprendimo III priedo A priede „ES ir JAV „privatumo skydo“ ombudsmeno mechanizmas dėl signalų žvalgybos“, pridėtame prie tuometinio *Secretary of State* (JAV valstybės sekretorius) 2016 m. liepos 7 d. John Kerry rašto, yra memorandumas, jame apibūdinama nauja ombudsmeno procedūra, pavedant valstybės sekretoriui paskirti „Tarptautinės informacinių technologijų diplomatijos vyresnįjį koordinatorių“ (toliau – ombudsmenas).

38. Kaip nurodyta šiame memorandume, ši procedūra buvo nustatyta tam, „kad palengvintų prašymų dėl prieigos prie duomenų, perduotų pagal [Sąjungos] ir JAV „privatumo skydą“, standartines sutarčių sąlygas, privalomas įmonių taisykles, išimtis arba galimas būsimas išimtis nacionalinio saugumo tikslais, nagrinėjimą pasinaudojant Jungtinių Amerikos Valstijų taikomuose įstatymuose ir politikoje nustatytais būdais ir šių prašymų patenkinimą“.

III. Pagrindinė byla, prejudiciniai klausimai ir procesas Teisingumo Teisme

39. Austrijoje gyvenantis Austrijos pilietis M. Schrems yra socialinio tinklo *Facebook* naudotojas. Visų Sąjungos teritorijoje gyvenančių asmenų, norinčių naudotis šiuo socialiniu tinklu, per registracijos procedūrą prašoma pasirašyti sutartį su *Facebook Ireland*, Jungtinėse Amerikos Valstijose įsikūrusios patronuojančiosios bendrovės *Facebook Inc.* patronuojamąja bendrove. Šių naudotojų asmens duomenys (visi arba jų dalis) perduodami į JAV teritorijoje esančius *Facebook Inc.* priklausančius serverius ir ten tvarkomi.

11 2000 m. liepos 26 d. Sprendimas dėl [Direktyvos 95/46] (OL L 215, 2000, p. 7; 2004 m. specialusis leidimas lietuvių k., 16 sk., 1 t., p. 119) (toliau – Sprendimas dėl „saugaus uosto“).

12 C-362/14, EU:C:2015:650, toliau – Sprendimas *Schrems*.

40. 2013 m. birželio 25 d. M. Schrems pateikė skundą DPC, jame iš esmės prašė uždrausti *Facebook Ireland* perduoti jo asmens duomenis į JAV. Minėtame skunde jis nurodė, kad pagal šios trečiosios šalies teisę ir praktiką jos teritorijoje laikomi asmens duomenys nėra pakankamai apsaugoti nuo ribojimų, atsirandančių dėl šios šalies viešosios valdžios institucijų vykdomos stebėjimo veiklos. Šiuo klausimu M. Schrems rėmėsi Edward Snowden atskleista informacija apie JAV žvalgybos tarnybų, visų pirma *National Security Agency* (Nacionalinė saugumo agentūra, toliau – NSA), veiklą.

41. Šis skundas buvo atmestas motyvuojant, be kita ko, tuo, kad kiekvienas klausimas, susijęs su JAV užtikrinamos apsaugos tinkamumu, turi būti sprendžiamas vadovaujantis sprendimu dėl „saugaus uosto“. Tame sprendime Komisija nustatė, kad ši trečioji šalis užtikrina tinkamą jos teritorijoje esančioms įmonėms perduodamų asmens duomenų apsaugos lygį, laikydamasi minėtame sprendime įtvirtintų principų.

42. M. Schrems apskundė sprendimą atmesti jo skundą *High Court* (Aukštasis teismas). Šis teismas nusprendė, kad nors M. Schrems formaliai neginčijo sprendimo dėl „saugaus uosto“ galiojimo, iš tikrųjų savo skunde jis nesutiko su šiame sprendime nustatytos tvarkos teisėtumu. Tokiomis aplinkybėmis minėtas teismas pateikė Teisingumo Teismui klausimus, kuriais iš esmės siekiama išsiaiškinti, ar valstybių narių valdžios institucijoms, atsakingoms už duomenų apsaugą (toliau – priežiūros institucijos), gavusioms skundą dėl asmens teisių ir laisvių tvarkant jo asmens duomenis, kurie buvo perduoti į trečiąją valstybę, apsaugos, yra privalomos išvados dėl šios trečiosios valstybės užtikrinamo apsaugos lygio tinkamumo, kurias Komisija padarė pagal Direktyvos 95/46 25 straipsnio 6 dalį, nors skundo pateikėjas ginčija šias išvadas.

43. Sprendimo *Schrems* 51 ir 52 punktuose konstatavęs, kad sprendimas dėl tinkamumo yra privalomas priežiūros institucijoms, kol nėra pripažintas negaliojančiu, Teisingumo Teismas šio sprendimo 63 ir 65 punktuose nurodė:

„63. <…> jei asmuo, kurio asmens duomenys buvo arba galėjo būti perduoti į pagal Direktyvos 95/46 25 straipsnio 6 dalį priimtame Komisijos sprendime nurodytą trečiąją šalį, pateikia nacionalinei priežiūros institucijai prašymą dėl jo teisių ir laisvių apsaugos tvarkant šiuos duomenis ir šiame prašyme ginčija <…> kad šis sprendimas suderinamas su privataus gyvenimo ir asmenų pagrindinių teisių ir laisvių apsauga, tokia institucija ypač kruopščiai turi išnagrinėti minėtą prašymą.

<…>

65. <…> kai minėta institucija mano, kad asmens, pateikusio jai prašymą dėl teisių ir laisvių apsaugos tvarkant jo asmens duomenis, pateikti kaltinimai pagrįsti, remdamasi Direktyvos 95/46 28 straipsnio 3 dalies pirmos pastraipos trečia įtrauka, siejama, be kita ko, su Chartijos 8 straipsnio 3 dalimi, ji turi galėti kreiptis į teismą. Šiuo atžvilgiu nacionalinis teisės aktų leidėjas turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis nacionaliniuose teismuose kaltinimais, kurie, jos nuomone, yra pagrįsti, tam, kad šie teismai, vertindami Komisijos sprendimo galiojimą, pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir priežiūros institucija, turėtų abejonių dėl šio sprendimo galiojimo.“

44. Minėtame sprendime Teisingumo Teismas taip pat nagrinėjo sprendimo dėl „saugaus uosto“ galiojimą atsižvelgiant į reikalavimus, kylančius iš Direktyvos 95/46, aiškinamos atsižvelgiant į Chartiją. Atlikęs šią analizę jis pripažino minėtą sprendimą negaliojančiu [13].

13 Žr. Sprendimą *Schrems* (106 punktas).

45. Po Sprendimo *Schrems* prašymą priimti prejudicinį sprendimą pateikęs teismas panaikino sprendimą, kuriuo DPC atmetė M. Schrems skundą, ir grąžino jį DPC nagrinėti iš naujo. DPC pradėjo tyrimą ir paprašė M. Schrems performuluoti savo skundą atsižvelgiant į sprendimo dėl „saugaus uosto“ pripažinimą negaliojančiu.

46. Šiuo tikslu M. Schrems paprašė *Facebook Ireland* nustatyti teisinius pagrindus, kuriais yra grindžiamas socialinio tinklo *Facebook* naudotojų asmens duomenų perdavimas iš Sąjungos į JAV. *Facebook Ireland*, nepateikdama visų teisinių pagrindų, kuriais remiasi, nurodė susitarimą dėl duomenų perdavimo ir tvarkymo (*data transfer processing agreement*), sudarytą tarp jos pačios ir *Facebook Inc.*, taikytiną nuo 2015 m. lapkričio 20 d., ir rėmėsi Sprendimu 2010/87.

47. Performuluotame skunde M. Schrems nurodo, pirma, kad šio susitarimo sąlygos neatitinka Sprendimo 2010/87 priede nustatytų sutarčių standartinių sąlygų. Antra, M. Schrems teigia, kad šios standartinės sutarčių sąlygos bet kuriuo atveju negalėjo būti pagrindas perduoti jo asmens duomenis į JAV. Taip yra, nes pagal JAV teisę *Facebook Inc.* privalo pateikti naudotojų asmens duomenis JAV valdžios institucijoms, kaip antai NSA ir *Federal Bureau of Investigation* (FBI) (Federalinis tyrimų biuras, JAV), pagal stebėjimo programas, kuriomis kliudoma įgyvendinti Chartijos 7, 8 ir 47 straipsniuose užtikrinamas teises. M. Schrems teigimu, nė viena teisių gynimo priemonė neleidžia duomenų subjektams remtis savo teisėmis į privataus gyvenimo gerbimą ir asmens duomenų apsaugą. Tokiomis aplinkybėmis M. Schrems prašo DPC sustabdyti šį duomenų perdavimą pagal Sprendimo 2010/87 4 straipsnį.

48. DPC atliekant tyrimą *Facebook Ireland* pripažino, kad toliau perduoda Sąjungoje gyvenančių socialinio tinklo *Facebook* naudotojų asmens duomenis į JAV ir kad šiuo tikslu ji daugiausia remiasi Sprendimo 2010/87 priede esančiomis standartinėmis sutarčių sąlygomis.

49. DPC tyrimu buvo siekiama nustatyti, pirma, ar JAV užtikrina tinkamą Sąjungos piliečių asmens duomenų apsaugą, ir, antra, jeigu ne, ar sprendimai dėl SSS suteikia tinkamas apsaugos priemones, kiek tai susiję su šių asmenų laisvių ir pagrindinių teisių apsauga.

50. Šiuo klausimu sprendimo projekte (*draft decision*) DPC laikinai nusprendė, kad pagal JAV teisę Sąjungos piliečiams, kurių duomenys perduodami į JAV, kur JAV agentūros gali juos tvarkyti nacionalinio saugumo tikslais su Chartijos 7 ir 8 straipsniais nesuderinamu būdu, nesuteikiamos veiksmingos teisių gynimo priemonės, kaip tai suprantama pagal Chartijos 47 straipsnį. Sprendimų dėl SSS priede esančiose sąlygose numatytos apsaugos priemonės šios spragos nepanaikintų, nes jos nėra privalomos JAV valdžios institucijoms ar agentūroms ir suteikia duomenų subjektams tik sutartyje numatytas teises duomenų eksportuotojo ir (arba) importuotojo atžvilgiu.

51. Tokiomis aplinkybėmis DPC konstatavo, kad negali priimti sprendimo dėl M. Schrems skundo, kol Teisingumo Teismas nėra išnagrinėjęs sprendimų dėl SSS galiojimo klausimo. Taigi DPC, atsižvelgdamas į tai, kas nurodyta Sprendimo *Schrems* 65 punkte, kreipėsi į prašymą priimti prejudicinį sprendimą pateikusį teismą, prašydamas jo, jeigu jis pritartų DPC iškeltoms abejonėms, pateikti Teisingumo Teismui prašymą priimti prejudicinį sprendimą dėl šių sprendimų galiojimo.

52. JAV vyriausybė, *Electronic Privacy Information Centre* (EPIC) (Elektroninio privatumo informacijos centras), *Business Software Alliance* (BSA) (Komercinės programinės įrangos aljansas) ir *Digitaleurope* buvo leista įstoti į bylą prašymą priimti prejudicinį sprendimą pateikusiame teisme.

53. Siekdamas nustatyti, ar pritaria DPC iškeltoms abejonėms dėl sprendimų dėl SSS galiojimo, *High Court* (Aukštasis Teismas) gavo ginčo šalių pateiktus įrodymus ir išklausė jų bei įstojusių į bylą šalių argumentus. Visų pirma ekspertai pateikė įrodymų dėl JAV teisės nuostatų. Pagal Airijos teisę užsienio teisė laikoma fakto klausimu, kuris turi būti įrodytas pateikiant įrodymų, kaip ir bet kuri kita faktinė aplinkybė. Remdamasis šiais įrodymais, prašymą priimti prejudicinį sprendimą pateikęs teismas įvertino JAV teisės nuostatas, pagal kurias valdžios institucijoms ir agentūroms leidžiama vykdyti

stebėjimą, dviejų viešai pripažintų stebėjimo programų (PRISM ir *Upstream*) veikimą, įvairias teisių gynimo priemones, suteikiamas privatiems asmenims, kurių teisės buvo pažeistos stebėjimo priemonėmis, taip pat sistemines apsaugos priemones ir priežiūros mechanizmus. Minėtas teismas šio vertinimo rezultatus pateikė 2017 m. spalio 3 d. sprendime, pridėtame prie jo nutarties dėl prašymo priimti prejudicinį sprendimą (toliau – 2017 m. spalio 3 d. *High Court* (Aukštasis Teismas) sprendimas).

54. Tame sprendime prašymą priimti prejudicinį sprendimą pateikęs teismas kaip vieną iš teisinių pagrindų, leidžiančių JAV žvalgybos tarnyboms perimti užsienio komunikaciją, nurodė *Foreign Intelligence and Surveillance Act* (FISA) (Įstatymas dėl užsienio žvalgybos informacijos stebėjimo) ir *Executive Order 12333* (Prezidento vykdomasis įsakymas Nr. 12333, toliau – EO 12333).

55. Kaip nustatyta minėtame teismo sprendime, pagal FISA 702 straipsnį *Attorney General* (JAV generalinis prokuroras) ir *Director of National Intelligence* (DNI) (JAV nacionalinės žvalgybos vadovas) kartu gali duoti leidimą vienus metus stebėti asmenis, kurie nėra JAV piliečiai ir nuolat negyvena JAV (toliau – ne JAV asmenys), siekiant gauti informaciją užsienio žvalgybos srityje, jeigu yra pagrindo manyti, kad šie asmenys yra už JAV teritorijos ribų [14]. Kaip nurodyta FISA, sąvoka „užsienio žvalgyba“ reiškia informaciją, susijusią su vyriausybės gebėjimu apsisaugoti nuo užsienio išpuolių, terorizmo, masinio naikinimo ginklų platinimo ir informaciją, susijusią su JAV užsienio reikalų tvarkymu [15].

56. Šiuos metinius leidimus, taip pat numatomų stebėti asmenų tikslingo pasirinkimo procedūras ir surinktos informacijos tvarkymą (angl. *minimisation*) [16] turi patvirtinti *Foreign Intelligence Surveillance Court* (FISC) (Užsienio žvalgybos priežiūros teismas, JAV). Nors vykdant „tradicinį“ stebėjimą remiantis kitomis FISA nuostatomis reikalaujama, kad būtų nustatytas „tikėtinas pagrindas“, leidžiantis įtarti, kad stebimi asmenys priklauso užsienio valdžiai ar yra jos agentai, o stebėjimo veiklai, vykdomai pagal FISA 702 straipsnį, nereikalaujama nei nustatyti tokio „tikėtino pagrindo“, nei kad FISC patvirtintų numatomų stebėti konkrečių asmenų tikslingą pasirinkimą. Be to, kaip konstatavo prašymą priimti prejudicinį sprendimą pateikęs teismas, minimalios informacijos procedūros netaikomos ne JAV asmenims, esantiems už JAV ribų.

57. Praktiškai, kai FISC duoda leidimą, NSA siunčia JAV įsteigtiems elektroninių ryšių paslaugų teikėjams nurodymus su paieškos kriterijais, kurie vadinami „selektoriais“ ir yra siejami su tiksliniais asmenimis (pavyzdžiui, telefono numeris arba e. pašto adresas). Taigi šie paslaugų teikėjai privalo perduoti selektorius atitinkančius duomenis NSA ir saugoti paslaptį dėl jiems skirtų nurodymų. Jie gali pareikšti ieškinį FISC dėl NSA nurodymų pakeitimo arba netaikymo. FISC sprendimas gali būti skundžiamas *Foreign Intelligence Surveillance Court of Review* (FISCR) (Užsienio žvalgybos informacijos stebėjimo apeliacinis teismas, JAV).

58. *High Court* (Aukštasis Teismas) konstatavo, kad FISA 702 straipsnis yra programų PRISM ir *Upstream* teisinis pagrindas.

59. Pagal programą PRISM elektroninių ryšių paslaugų teikėjai turi perduoti NSA visus pranešimus, „išsiunčiamus iš“ NSA nurodyto selektoriaus arba „skirtus“ jam. Dalis šių pranešimų būtų siunčiama FBI ir *Central Intelligence Agency* (CIA) (Centrinė žvalgybos agentūra, JAV). 2015 m. buvo stebimi 94 386 asmenys, o 2011 m. JAV vyriausybė pagal šią programą gavo, kaip teigiama, daugiau kaip 250 mln. pranešimų.

14 50 U.S.C. 1881 (a).

15 50 U.S.C. 1881 (e).

16 Prašymą priimti prejudicinį sprendimą pateikęs teismas konstatavo, kad numatomų stebėti asmenų tikslingo pasirinkimo procedūros susijusios su tuo, kaip vykdomoji valdžia nustato, jog yra pagrįsta manyti, kad konkretus asmuo yra už JAV ribų esantis ne JAV asmuo ir kad šio asmens stebėjimas gali leisti gauti informaciją užsienio žvalgybos srityje. Minimalios informacijos procedūros apima visos viešai neskelbiamos informacijos apie JAV asmenį, gautos pagal FISA 702 straipsnį, gavimą, saugojimą, naudojimą ir sklaidą.

60. Programa *Upstream* grindžiama įmonių, naudojančių „dorsale“ (kabelių, perjungiklių ir maršrutizatorių tinklas), per kurį perduodami telefonu ir internetu siunčiami pranešimai, privalomai teikiama pagalba. Šios įmonės privalo leisti NSA kopijuoti ir filtruoti interneto duomenų srautą siekiant gauti pranešimus, „išsiunčiamus iš“ šios agentūros nurodyme paminėto selektoriaus, šiam selektoriui „skirtus“ pranešimus arba pranešimus, „susijusius su“ šios agentūros nurodyme paminėtu selektoriumi. Pranešimai, „susiję su“ selektoriumi, yra tie, kuriuose nurodomas šis selektorius ir su šiuo selektoriumi nebūtinai siejamas ne JAV asmuo. Nors pagal 2017 m. balandžio 26 d. FISC nuomonę nuo šios datos Amerikos vyriausybė neberenka ir nebegauna pranešimų, „susijusių su“ selektoriumi, šioje nuomonėje nenurodyta, kad NSA nustojo kopijuoti ir filtruoti per jos taikomą stebėjimo mechanizmą pereinančių pranešimų srautą. Vadinasi, tai reiškė, kad vykdant programą *Upstream* NSA gauna ir metaduomenis, ir pranešimų turinį. Nuo 2011 m. NSA pagal programą *Upstream* gaudavo beveik 26,5 mln. pranešimų per metus, bet tai tik nedidelė dalis pranešimų, kuriems pagal šią programą buvo taikomas filtravimas.

61. Be to, kaip nustatė *High Court* (Aukštasis Teismas), pagal EO 12333 elektroninius pranešimus leidžiama stebėti ir už JAV teritorijos ribų, leidžiant užsienio žvalgybos tikslais gauti duomenis, kurie „perduodami“ per šią teritoriją arba ją „kerta“ ir nėra skirti tvarkyti joje, taip pat rinkti ir saugoti šiuos duomenis. EO 12333 sąvoka „užsienio žvalgyba“ apibrėžiama kaip apimanti informaciją, susijusią su užsienio valdžios, užsienio organizacijų ar užsieniečių galimybėmis, ketinimais ar veikla [17].

62. Pagal EO 12333 NSA buvo suteikta teisė naudotis Atlanto vandenyno dugne esančiais povandeniniais kabeliais, kuriais duomenys perduodami iš Sąjungos į JAV, dar prieš šiems duomenims pasiekiant JAV, vadinasi, prieš pradedant jiems taikyti FISA nuostatas. Vis dėlto nėra jokių įrodymų, kad pagal šį prezidento įsakymą būtų vykdoma kokia nors programa.

63. Nors EO 12333 numatyti informacijos rinkimo, saugojimo ir sklaidos apribojimai, šie apribojimai netaikomi ne JAV asmenims. Pastariesiems taikomos tik tos apsaugos priemonės, kurios nurodytos *Presidential Policy Directive 28* (Prezidento politikos direktyva Nr. 28, toliau – PPD 28), taikomoje visai elektromagnetinės kilmės informacijos užsienio žvalgybos srityje rinkimo ir naudojimo veiklai. PPD 28 nurodyta, kad privataus gyvenimo gerbimas yra vienas iš motyvų, į kuriuos atsižvelgtina planuojant šią veiklą, kad informacija turi būti renkama vieninteliu tikslu gauti informaciją užsienio žvalgybos ir kontršnipinėjimo srityje ir kad ši veikla turi būti „kuo tikslingesnė“.

64. Kaip nurodo prašymą priimti prejudicinį sprendimą pateikęs teismas, NSA veikla, grindžiama EO 12333, kurį JAV prezidentas gali bet kada iš dalies pakeisti ar panaikinti, nėra reglamentuota įstatymo, jai netaikoma teismų kontrolė ir dėl jos nėra galimybės pareikšti ieškinio teisme.

65. Konstatavęs šias aplinkybes, minėtas teismas laikosi pozicijos, kad JAV masiškai ir be jokios atrankos tvarko asmens duomenis, todėl gali būti pažeistos duomenų subjektų teisės, kurias jie turi pagal Chartijos 7 ir 8 straipsnius.

66. Minėtas teismas taip pat nurodo, kad Sąjungos piliečiams nėra prieinamos tos pačios kaip ir JAV piliečiams teisminės teisių gynimo priemonės dėl JAV valdžios institucijų atliekamo neteisėto jų asmens duomenų tvarkymo. JAV Konstitucijos Ketvirtoji pataisa, kurioje numatyta didžiausia apsauga nuo neteisėto stebėjimo, netaikytina Sąjungos piliečiams, neturintiems savanoriško reikšmingo ryšio su JAV. Nors jiems suteikiamos tam tikros kitos teisių gynimo priemonės, jie susiduria su didelėmis kliūtimis.

17 EO 12333, 3.5 punkto e papunktis.

67. Visų pirma pagal JAV Konstitucijos III straipsnį kiekvienas suinteresuotasis asmuo, norėdamas pareikšti ieškinį federaliniuose teismuose, turi įrodyti savo teisę pareikšti ieškinį (*standing*). Teisė pareikšti ieškinį suteikiama, jeigu, be kita ko, šis asmuo įrodo patyręs realią žalą, kuri, pirma, yra konkreti ir individuali ir, antra, esama arba neišvengiama. Remdamasis, be kita ko, *Supreme Court of the United States* (JAV Aukščiausiasis Teismas) sprendimu *Clapper v. Amnesty International US*[18], prašymą priimti prejudicinį sprendimą pateikęs teismas mano, kad praktiškai šią sąlygą pernelyg sunku įvykdyti, atsižvelgiant, be kitų aspektų, į tai, kad nėra jokios pareigos informuoti duomenų subjektus apie jiems taikomas sekimo priemones[19]. Be to, Sąjungos piliečiams prieinamų teisių gynimo priemonių daliai taikomos ir kitos ribojančios sąlygos, pavyzdžiui, būtinybė įrodyti turtinę žalą. Žvalgybos agentūroms pripažįstamas imunitetas ir atitinkamos informacijos įslaptinimas taip pat neleidžia pasinaudoti kai kuriomis teisių gynimo priemonėmis[20].

68. *High Court* (Aukštasis Teismas) taip pat nurodo įvairius žvalgybos agentūrų veiklos kontrolės ir priežiūros mechanizmus.

69. Tarp jų yra, pirma, FISC taikomas FISA 702 straipsniu grindžiamų programų metinio sertifikavimo mechanizmas, tačiau jį taikydamas FISC netvirtina atskirų selektorių. Be to, informacijos rinkimui užsienio žvalgybos srityje pagal EO 12333 netaikoma jokia išankstinė teisminė kontrolė.

70. Antra, prašymą priimti prejudicinį sprendimą pateikęs teismas nurodo kelis žvalgybos veiklos neteisminės priežiūros mechanizmus. Jis visų pirma mini *Inspectors General* (generaliniai inspektoriai, JAV), kurie kiekvienoje žvalgybos agentūroje yra atsakingi už stebėjimo veiklos priežiūrą, vaidmenį. Be to, *Privacy and Civil Liberties Oversight Board* (PCLOB) (Privataus gyvenimo ir pilietinių laisvių priežiūros valdyba, JAV) kaip nepriklausoma vykdomosios valdžios grandies agentūra gauna kiekvienoje agentūroje paskirtų pilietinių laisvių arba privatumo pareigūnų (*civil liberties or privacy officers*) ataskaitas. PCLOB reguliariai rengia ataskaitas parlamento komitetams ir prezidentui. Atitinkamos agentūros turi pranešti, be kita ko, DNI apie incidentus, susijusius su taisyklių ir procedūrų, reglamentuojančių užsienio žvalgybos informacijos rinkimą, pažeidimu. Apie šiuos incidentus pranešama ir FISC. JAV Kongresas per Atstovų rūmų ir Senato žvalgybos komitetus taip pat yra atsakingas už užsienio žvalgybos veiklos kontrolę.

71. Vis dėlto *High Court* (Aukštasis Teismas) pažymi esminį skirtumą tarp, pirma, taisyklių, kuriomis siekiama užtikrinti, kad duomenys būtų gaunami teisėtai ir kad po to, kai šie duomenys gaunami, naudojant juos nebūtų piktnaudžiaujama, ir, antra, teisių gynimo priemonių, kurios yra prieinamos pažeidus šias taisykles. Duomenų subjektų pagrindinių teisių apsauga užtikrinama tik veiksmingomis teisių gynimo priemonėmis, leidžiančiomis asmenims remtis savo teisėmis, jeigu minėtos taisyklės pažeidžiamos.

72. Tokiomis aplinkybėmis prašymą priimti prejudicinį sprendimą pateikęs teismas laiko pagrįstais DPC pateiktus argumentus, pagal kuriuos JAV teisėje nustatytais asmenų, kurių duomenys perduodami iš Sąjungos, teisės pareikšti ieškinį apribojimais nepaisoma Chartijos 47 straipsnyje užtikrinamos teisės esmės ir bet kuriuo atveju jais neproporcingai ribojamas šios teisės įgyvendinimas.

18 133 S.Ct. 1138 (2013).

19 Vis dėlto prašymą priimti prejudicinį sprendimą pateikęs teismas konstatavo, kad principui, pagal kurį nereikalaujama informuoti asmens, kuriam taikoma sekimo priemonė, taikoma išimtis, jeigu JAV vyriausybė ketina panaudoti pagal FISA 702 straipsnį surinktus duomenis prieš šį asmenį baudžiamojoje arba administracinėje byloje.

20 Visų pirma prašymą priimti prejudicinį sprendimą pateikęs teismas nurodė, kad nors pagal *Judicial Redress Act* (JRA) (Įstatymas dėl teisminės gynybos) *Privacy Act* (Įstatymas dėl privataus gyvenimo apsaugos) nuostatų taikymas išplėstas apimant Sąjungos piliečius (pagal jį fiziniams asmenims leidžiama gauti kai kurių agentūrų turimą informaciją apie juos, susijusią su kai kuriomis trečiosiomis šalimis), NSA nėra nurodyta JRA kaip viena iš tokių agentūrų.

73. Kaip teigia *High Court* (Aukštasis Teismas), tai, kad JAV vyriausybė numatė sprendime dėl „privatumo skydo“ apibūdintą ombudsmeno instituciją, neleidžia suabejoti šiuo vertinimu. Pažymėdamas, kad ši ombudsmeno institucija yra prieinama Sąjungos piliečiams, pagrįstai manantiems, kad jų duomenys buvo perduoti pagal sprendimus dėl SSS [21], šis teismas nurodė, kad ombudsmenas nėra teismas, atitinkantis Chartijos 47 straipsnio reikalavimus, visų pirma jis nėra nepriklausomas nuo vykdomosios valdžios [22]. Minėtas teismas taip pat abejoja, ar ombudsmeno, kurio sprendimai negali būti skundžiami teismui, įtraukimas yra veiksminga teisių gynimo priemonė. Iš tiesų ombudsmeno įtraukimas neleidžia asmenims, kurių asmens duomenys buvo renkami, tvarkomi arba platinami neteisėtai, gauti žalos atlyginimo ar įpareigojimo nutraukti neteisėtus veiksmus, nes ombudsmenas nei patvirtina, nei paneigia, kad ieškovui buvo taikoma elektroninio stebėjimo priemonė.

74. Išdėstęs susirūpinimą jam keliančius klausimus, susijusius su tuo, ar JAV teisėje numatytos apsaugos priemonės ir iš Chartijos 7, 8 ir 47 straipsnių kylantys reikalavimai yra iš esmės tokie patys, prašymą priimti prejudicinį sprendimą pateikęs teismas klausė, ar sprendimuose dėl SSS numatytos standartinės sutarčių sąlygos, kurios pagal savo pobūdį nėra privalomos JAV valdžios institucijoms, vis dėlto gali užtikrinti duomenų subjektų pagrindinių teisių apsaugą. Tuo remdamasis minėtas teismas nusprendė, kad pritaria DPC abejonėms dėl šių sprendimų galiojimo.

75. Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas visų pirma mano, kad Direktyvos 95/46 28 straipsnio 3 dalies, į kurią Sprendimo 2010/87 4 straipsnyje daroma nuoroda, pripažįstant priežiūros institucijoms įgaliojimus sustabdyti arba uždrausti duomenų perdavimą, grindžiamą šiame sprendime numatytomis standartinėmis sutarčių sąlygomis, nepakanka šioms abejonėms išsklaidyti. Jo nuomone, šie įgaliojimai yra tik diskreciniai, be to, prašymą priimti prejudicinį sprendimą pateikęs teismas, atsižvelgdamas į Sprendimo 2010/87 11 konstatuojamąją dalį, kelia klausimą dėl galimybės jais pasinaudoti, jeigu nustatyti trūkumai nesusiję su konkrečiu ir išimtiniu atveju, o yra bendro ir sisteminio pobūdžio [23]. Taip pat, minėto teismo nuomone, rizika, kad skirtingose valstybėse narėse bus priimti skirtingi sprendimai, galėtų būti pagrindas prieštarauti, kad priežiūros institucijoms būtų pavesta konstatuoti tokius trūkumus.

76. Tokiomis aplinkybėmis *High Court* (Aukštasis Teismas) 2018 m. gegužės 4 d. sprendimu [24], kurį Teisingumo Teismas gavo 2018 m. gegužės 9 d., nutarė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui tokius prejudicinius klausimus:

„1. Ar tais atvejais, kai privati bendrovė perduoda asmens duomenis iš [Sąjungos] valstybės narės privačiai bendrovei trečiojoje šalyje komerciniais tikslais pagal [Sprendimą 2010/87], ir toje trečiojoje šalyje jos institucijos gali toliau tvarkyti tokius asmens duomenis ne tik nacionalinio saugumo tikslais, bet ir teisėsaugos bei trečiosios šalies užsienio politikos tikslais, tokių duomenų perdavimui taikoma Sąjungos teisė (įskaitant [Chartiją]), nepaisant ESS 4 straipsnio 2 dalies nuostatų dėl nacionalinio saugumo ir [Direktyvos 95/46] 3 straipsnio 2 dalies pirmos įtraukos nuostatų dėl visuomenės saugumo, gynybos ir valstybės saugumo?

21 Prašymą priimti prejudicinį sprendimą pateikęs teismas šiuo aspektu nurodo sprendimo dėl „privatumo skydo“ III priedo A priedą (žr. šios išvados 37 ir 38 punktus).

22 Prašymą priimti prejudicinį sprendimą pateikęs teismas nurodo 2005 m. sausio 27 d. Sprendimą *Denuit ir Cordenier* (C-125/04, EU:C:2005:69, 12 punktas).

23 Sprendimo 2010/87 11 konstatuojamojoje dalyje nurodyta: „įgyvendinant šį sutarčių mechanizmą valstybių narių priežiūros institucijoms tenka svarbus vaidmuo – jos užtikrina, kad po perdavimo asmens duomenys būtų tinkamai apsaugoti. Išskirtiniais atvejais, kai duomenų eksportuotojai atsisako ar negali duoti tinkamų nurodymų duomenų importuotojui, ir todėl duomenų subjektams iškyla didelės žalos grėsmė, standartinės sutarčių sąlygos turėtų leisti priežiūros institucijoms atlikti duomenų importuotojų ir pagalbinių duomenų tvarkytojų patikrinimus ir, tam tikrais atvejais, priimti duomenų importuotojus ir pagalbinius duomenų tvarkytojus įpareigojančius sprendimus. Priežiūros institucijoms turėtų būti suteikta teisė sutarčių standartinių sąlygų pagrindu uždrausti ar sustabdyti duomenų perdavimą ar kelis duomenų perdavimus tais išimtiniais atvejais, kai nustatoma, jog pagal sutartį atliekamas duomenų perdavimas gali labai neigiamai paveikti garantijas ir įsipareigojimus, kuriais suteikiama tinkama apsauga duomenų subjektui“.

24 *Facebook Ireland* apskundė prašymą priimti prejudicinį sprendimą pateikusio teismo sprendimą *Supreme Court* (Aukščiausiasis Teismas, Airija). Šis kasacinis skundas buvo atmestas 2019 m. gegužės 31 d. Sprendimu *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, Appeal nº2018/68 (toliau – 2019 m. gegužės 31 d. *Supreme Court* (Aukščiausiasis Teismas) sprendimas).

2. a) Ar norint nustatyti, ar perdavus duomenis iš [Sąjungos] į trečiąją šalį pagal Sprendimą [2010/87], kur jie gali būti toliau tvarkomi nacionalinio saugumo tikslais, buvo pažeistos asmens teisės, pagal [Direktyvą 95/46] svarbus lyginamasis teisės šaltinis yra:

   i) Chartija, ESS, SESV, [Direktyva 95/46], [Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, pasirašyta 1950 m. lapkričio 4 d. Romoje (toliau – EŽTK) (arba kuri nors kita [Sąjungos] teisės nuostata); ar

   ii) vienos arba daugiau valstybių narių nacionaliniai įstatymai?

   b) Jeigu svarbus lyginamasis teisės šaltinis yra nurodytas ii punkte, ar į jį turi būti įtraukta ir vienos arba daugiau valstybių narių taikoma su nacionalinio saugumo užtikrinimu susijusi praktika?

3. Ar norint įvertinti, ar trečioji šalis užtikrina pagal [Sąjungos] teisę reikalaujamą asmens duomenų, perduodamų į tą šalį pagal [Direktyvos 95/46] 26 straipsnį, apsaugos lygį, apsaugos lygis toje trečiojoje šalyje turėtų būti vertinamas atsižvelgiant į:

   a) toje trečiojoje šalyje taikomas jos nacionalinės teisės arba tarptautinių įsipareigojimų nuostatas ir tokių nuostatų laikymosi užtikrinimo praktiką, įskaitant profesines nuostatas ir saugumo priemones, kurių laikomasi toje trečiojoje šalyje;

   ar

   b) a punkte nurodytas nuostatas kartu su administracine, reguliavimo ir reikalavimų laikymosi užtikrinimo praktika bei politikos įgyvendinimo užtikrinimo priemonėmis, procedūromis, protokolais, priežiūros mechanizmais ir neteisminėmis gynybos priemonėmis, kurios yra taikomos trečiojoje šalyje?

4. Atsižvelgiant į *High Court* (Aukštasis Teismas) nustatytas faktines aplinkybes, susijusias su JAV teise, jeigu asmens duomenys pagal Sprendimą [2010/87] perduodami iš [Sąjungos] į JAV, ar taip pažeidžiamos Chartijos 7 ir (arba) 8 straipsniuose numatytos asmens teisės?

5. Atsižvelgiant į *High Court* (Aukštasis Teismas) nustatytas faktines aplinkybes, susijusias su JAV teise, jeigu asmens duomenys perduodami iš [Sąjungos] į JAV pagal Sprendimą [2010/87]:

   a) ar JAV suteikiama apsauga yra tokio lygio, kad ja užtikrinama asmens teisės pasinaudoti pagal Chartijos 47 straipsnį garantuojamomis teisminės gynybos priemonėmis, kai pažeidžiamos jo teisės į duomenų privatumą, esmė?

Jeigu atsakymas į a punkte pateiktą klausimą yra teigiamas:

   b) ar JAV teisėje numatyti asmens teisės pasinaudoti teisminės gynybos priemonėmis apribojimai, taikomi dėl JAV nacionalinio saugumo, yra proporcingi, kaip tai suprantama pagal Chartijos 52 straipsnį, ir jie neviršija to, kas būtina demokratinėje visuomenėje siekiant nacionalinio saugumo tikslų?

6. a) Kokio lygio apsaugą reikia užtikrinti asmens duomenims, perduodamiems į trečiąją šalį pagal sutarčių standartines sąlygas, nustatytas Komisijos sprendimu pagal 26 straipsnio 4 dalį, atsižvelgiant į [Direktyvos 95/46] nuostatas, visų pirma į jos 25 ir 26 straipsnius, aiškinamus atsižvelgiant į Chartiją?

b) Į kokias aplinkybes reikia atsižvelgti, kai vertinama, ar pagal Sprendimą [2010/87] į trečiąją šalį perduodamiems duomenims suteikiamos apsaugos lygis atitinka [Direktyvos 95/46] ir Chartijos reikalavimus?

7. Ar aplinkybė, kad duomenų eksportuotojo ir duomenų importuotojo tarpusavio santykiams taikomos sutarčių standartinės sąlygos, nesaistančios trečiosios šalies nacionalinės valdžios institucijų, kurios gali pareikalauti duomenų importuotojo pateikti pagal [Sprendime 2010/87] pateiktas sąlygas perduotus asmens duomenis toliau tvarkyti jos saugumo tarnyboms, reiškia, kad pagal šias sąlygas negali būti pateiktos adekvačios apsaugos priemonės, kaip numatyta [Direktyvos 95/46] 26 straipsnio 2 dalyje?

8. Ar, jeigu duomenų importuotojui iš trečiosios šalies taikomi stebėjimo įstatymai, kurie, duomenų apsaugos institucijos manymu, prieštarauja [Sprendimo 2010/87] priede pateiktoms sąlygoms arba [Direktyvos 95/46] 25 ir 26 straipsniams ir (arba) Chartijai, [priežiūros] institucija privalo įgyvendinti pagal [Direktyvos 95/46] 28 straipsnio 3 dalį jai suteiktus vykdymo užtikrinimo įgaliojimus, kad sustabdytų duomenų srautus, ar tokie įgaliojimai gali būti įgyvendinami tik išimtiniais atvejais, atsižvelgiant į [Sprendimo 2010/87] 11 konstatuojamąją dalį, ar [priežiūros] institucija gali pasinaudoti diskrecija nestabdyti duomenų srautų?

9. a) Ar, atsižvelgiant į [Direktyvos 95/46] 25 straipsnio 6 dalį, Sprendimas [dėl „privatumo skydo“] 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?

b) Jeigu taip nėra, kokią reikšmę Sprendimas dėl „privatumo skydo“ turi (jeigu iš viso turi), kai vertinamas apsaugos priemonių, taikomų pagal [Sprendimą 2010/87] į Jungtines Valstijas perduodamiems duomenims, tinkamumas?

10. Ar, atsižvelgiant į *High Court* (Aukštasis Teismas) nustatytas su JAV teise susijusias aplinkybes, „privatumo skydo“ ombudsmeno institucijos įsteigimas pagal Sprendimo dėl „privatumo skydo“ III priedo A priedą, vertinamą kartu su Jungtinėse Valstijose galiojančia sistema, užtikrina, kad JAV suteikia duomenų subjektams, kurių asmens duomenys perduodami į JAV pagal [Sprendimą 2010/87], teisių gynybos priemones, atitinkančias Chartijos 47 straipsnio reikalavimus?

11. Ar [Sprendimas 2010/87] pažeidžia Chartijos 7, 8 ir (arba) 47 straipsnius?“

77. Rašytines pastabas Teisingumo Teismui pateikė DPC, *Facebook Ireland*, M. Schrems, JAV vyriausybė, EPIC, BSA, *Digitaleurope*, Airija, Belgijos, Čekijos, Vokietijos, Nyderlandų, Austrijos, Lenkijos, Portugalijos ir Jungtinės Karalystės vyriausybės, Europos Parlamentas ir Komisija. DPC, *Facebook Ireland*, M. Schrems, JAV vyriausybei, EPIC, BSA, *Digitaleurope*, Airijos, Vokietijos, Prancūzijos, Nyderlandų, Austrijos ir Jungtinės Karalystės vyriausybėms, Parlamentui, Komisijai ir Europos duomenų apsaugos valdybai (*European Data Protection Board*, EDPB) buvo atstovaujama 2019 m. liepos 9 d. teismo posėdyje.

IV. Analizė

A. Įvadinės pastabos

78. Po to, kai Teisingumo Teismas Sprendimu *Schrems* pripažino sprendimą dėl „saugaus uosto“ negaliojančiu, asmens duomenys buvo toliau perduodami į JAV remiantis kitais teisiniais pagrindais. Visų pirma duomenis eksportuojančios bendrovės galėjo remtis sutartimis su duomenų importuotojais, į kurias buvo įtraukiamos Komisijos parengtos standartinės sąlygos. Šios sąlygos taip pat yra teisinis pagrindas perduoti duomenis į daugelį kitų trečiųjų šalių, dėl kurių Komisija nėra priėmusi sprendimo dėl tinkamumo [25]. Dabar pagal sprendimą dėl „privatumo skydo“ autosertifikuotoms įmonėms, patvirtinusioms, kad laikosi šiame sprendime nustatytų principų, leidžiama perduoti asmens duomenis į JAV netaikant jokių kitų formalumų.

79. Kaip aiškiai nurodyta nutartyje dėl prašymo priimti prejudicinį sprendimą ir kaip pažymėjo BSA, *Digitaleurope*, Airija, Austrijos ir Prancūzijos vyriausybės, Parlamentas ir Komisija, *High Court* (Aukštasis Teismas) nagrinėjamoje pagrindinėje byloje siekiama vienintelio tikslo – nustatyti, ar sprendimas, kuriame Komisija nustatė standartines sutarčių sąlygas, kuriomis grindžiamas M. Schrems skunde nurodytas duomenų perdavimas, t. y. Sprendimas 2010/87 [26] galioja.

80. Šis ginčas kilo dėl skundo, kuriuo DPC paprašė prašymą priimti prejudicinį sprendimą pateikusio teismo pateikti Teisingumo Teismui prejudicinį klausimą dėl Sprendimo 2010/87 galiojimo. Kaip nurodo prašymą priimti prejudicinį sprendimą pateikęs teismas, pagrindinė byla susijusi su naudojimusi teisių gynimo priemonėmis, kurias Teisingumo Teismas Sprendimo *Schrems* 65 punkte įpareigojo valstybes nares nustatyti.

81. Reikėtų priminti, jog minėto sprendimo 63 punkte Teisingumo Teismas konstatavo, kad priežiūros institucija turi ypač kruopščiai išnagrinėti skundą, kuriame asmuo, kurio asmens duomenys buvo arba galėjo būti perduoti į trečiąją šalį, dėl kurios buvo priimtas sprendimas dėl tinkamumo, ginčija šio sprendimo suderinamumą su Chartijoje įtvirtintomis pagrindinėmis teisėmis. Kaip nurodyta to paties sprendimo 65 punkte, jeigu minėta institucija mano, kad šiame skunde pateikti kaltinimai yra pagrįsti, ji pagal Direktyvos 95/46 28 straipsnio 3 dalies pirmą pastraipą (ją atitinka BDAR 58 straipsnio 5 dalis), aiškinamą atsižvelgiant į Chartijos 8 straipsnio 3 dalį, turi galėti kreiptis į teismą. Šiuo atžvilgiu nacionalinės teisės aktų leidėjas turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis šiais kaltinimais nacionaliniuose teismuose, tam, kad šie teismai pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir ši institucija, turėtų abejonių dėl nagrinėjamo sprendimo galiojimo.

82. Kaip ir prašymą priimti prejudicinį sprendimą pateikęs teismas, laikausi nuomonės, kad šios išvados pagal analogiją taikomos tuo atveju, kai priežiūros institucija, nagrinėdama jai paduotą skundą, turi abejonių ne dėl sprendimo dėl tinkamumo, o tokio sprendimo kaip Sprendimas 2010/87, kuriuo nustatomos standartinės sutarčių sąlygos, taikomos asmens duomenų perdavimui į trečiąsias šalis, galiojimo. Priešingai, nei teigia Vokietijos vyriausybė, nesvarbu, kad šios abejonės atitinka skundo pateikėjo šioje institucijoje iškeltus kaltinimus ar kad ši institucija pati savo iniciatyva kvestionuoja

25 BSA patvirtina, kad 70 % šiam aljansui priklausančių įmonių, atsakiusių į šiuo tikslu surengtą apklausą, pareiškė, kad rėmėsi standartinėmis sutarčių sąlygomis kaip svarbiausiu pagrindu perduoti asmens duomenis į trečiąsias šalis. *Digitaleurope* taip pat mano, kad standartinės sutarčių sąlygos yra pagrindinis teisinis dokumentas, kuriuo remiamasi kaip šio duomenų perdavimo pagrindu.

26 Nors prašymą priimti prejudicinį sprendimą pateikęs teismas nurodo, kad jo prašymas priimti prejudicinį sprendimą susijęs su trijų sprendimų dėl SSS galiojimu (šie sprendimai buvo nagrinėjami DPC sprendimo projekte ir 2017 m. spalio 3 d. sprendime), prejudiciniuose klausimuose nurodomas tik Sprendimas 2010/87. Būtent todėl šiame teisme *Facebook Ireland* nurodė šį sprendimą kaip Europoje esančių *Facebook* naudotojų duomenų perdavimo į JAV teisinį pagrindą. Taigi atliksiu analizę tik dėl šio sprendimo.

nagrinėjamo sprendimo galiojimą. Iš BDAR 58 straipsnio 5 dalies ir Chartijos 8 straipsnio 3 dalies kylantys reikalavimai, kuriais yra grindžiami Teisingumo Teismo motyvai, taikomi neatsižvelgiant į tai, koks duomenų perdavimo teisinis pagrindas nurodytas priežiūros institucijai pateiktame skunde, ir į priežastis, dėl kurių ši institucija, nagrinėdama šį skundą, suabejojo atitinkamo sprendimo galiojimu.

83. Atsižvelgiant į šiuos patikslinimus, DPC prašė prašymą priimti prejudicinį sprendimą pateikusio teismo pateikti Teisingumo Teismui klausimą dėl Sprendimo 2010/87 galiojimo tik todėl, kad jam atrodo, jog tam, kad būtų išnagrinėtas skundas, kuriuo M. Schrems prašo jo pasinaudoti jam pagal Direktyvos 95/46 28 straipsnio 3 dalies antrą įtrauką suteiktais įgaliojimais (kurie dabar jam suteikiami pagal BDAR 58 straipsnio 2 dalies f punktą) sustabdyti *Facebook Ireland* atliekamą jo asmens duomenų perdavimą *Facebook Inc.*, yra būtinas Teisingumo Teismo išaiškinimas.

84. Vadinasi, kadangi pagrindinėje byloje kilęs ginčas susijęs tik su Sprendimo 2010/87 galiojimu *in abstracto*, DPC vykdoma pirminė procedūra susijusi su šios institucijos įgaliojimų *konkrečiu atveju* imtis taisomųjų priemonių įgyvendinimu. Siūlysiu Teisingumo Teismui išnagrinėti pateiktus klausimus tiek, kiek to reikia sprendimui dėl Sprendimo 2010/87 galiojimo priimti, nes šio nagrinėjimo pakaks tam, kad prašymą priimti prejudicinį sprendimą pateikęs teismas galėtų išspręsti jam perduotą ginčą [27].

85. Prieš vertinant šio sprendimo galiojimą reikia atmesti kai kuriuos prieštaravimus dėl prašymo priimti prejudicinį sprendimą priimtinumo.

B. Dėl prašymo priimti prejudicinį sprendimą priimtinumo

86. Prašymo priimti prejudicinį sprendimą priimtinumas buvo ginčijamas dėl įvairių priežasčių, iš esmės susijusių su prejudiciniuose klausimuose nurodytos Direktyvos 95/46 netaikytinumu *ratione temporis* (1 dalis), su tuo, kad DPC vykdoma procedūra nėra pakankamai pažengusi, kad būtų pateisinamas jos tikslingumas (2 dalis), ir su neišsklaidytomis abejonėmis dėl prašymą priimti prejudicinį sprendimą pateikusio teismo nurodytų faktinių aplinkybių (3 dalis).

87. Šiuos nepriimtinumo pagrindus nagrinėsiu atsižvelgdamas į svarbos prezumpciją, taikomą Teisingumo Teismui pagal SESV 267 straipsnį pateiktiems klausimams. Pagal suformuotą jurisprudenciją Teisingumo Teismas gali atsisakyti priimti sprendimą dėl prašymo priimti prejudicinį sprendimą tik jeigu akivaizdu, kad prašomas Sąjungos teisės nuostatos išaiškinimas visiškai nesusijęs su pagrindinėje byloje nagrinėjamo ginčo aplinkybėmis ar dalyku, jeigu problema hipotetinė arba Teisingumo Teismas neturi informacijos apie faktines ir teisines aplinkybes, būtinos tam, kad naudingai atsakytų į jam pateiktus klausimus [28].

1. Dėl Direktyvos 95/46 taikytinumo „ratione temporis“

88. *Facebook Ireland* nurodo, kad prejudiciniai klausimai yra nepriimtini todėl, kad juose nurodoma Direktyva 95/46, nors nuo 2018 m. gegužės 25 d. ši direktyva buvo panaikinta ir pakeista BDAR [29].

89. Pritariu, kad Sprendimo 2010/87 galiojimas turi būti nagrinėjamas atsižvelgiant į BDAR nuostatas.

27 Žr. šios išvados 167–186 punktus.

28 Žr., be kita ko, 2018 m. gruodžio 10 d. Sprendimą *Wightman ir kt.* (C-621/18, EU:C:2018:999, 27 punktas ir jame nurodyta jurisprudencija) ir 2019 m. lapkričio 19 d. Sprendimą *A. K. ir kt.* (Aukščiausiojo Teismo Drausmės bylų kolegijos nepriklausomumas) (C-585/18, C-624/18 ir C-625/18, EU:C:2019:982, 98 punktas).

29 Žr. BDAR 94 straipsnio 1 dalį ir 99 straipsnio 1 dalį.

90. Pagal šio reglamento 94 straipsnio 2 dalį „nuorodos į panaikintą direktyvą laikomos nuorodomis į šį reglamentą“. Man atrodo, tai reiškia, kad Sprendimas 2010/87, kiek jame kaip teisinis pagrindas nurodoma Direktyvos 26 straipsnio 4 dalis, turi būti suprantamas kaip nurodantis BDAR 46 straipsnio 2 dalies c punktą, kuriame iš esmės pakartojamas minėtos direktyvos nuostatos turinys [30]. Taigi įgyvendinimo sprendimai, kuriuos prieš įsigaliojant BDAR Komisija priėmė pagal Direktyvos 95/46 26 straipsnio 4 dalį, turi būti aiškinami atsižvelgiant į šį reglamentą. Be to, prireikus ir jų galiojimas turi būti vertinamas remiantis šiuo reglamentu.

91. Šios išvados nepaneigia jurisprudencija, pagal kurią Sąjungos akto teisėtumas turi būti vertinamas atsižvelgiant į šio akto priėmimo dieną buvusias faktines ir teisines aplinkybes. Iš tiesų ši jurisprudencija susijusi su Sąjungos akto galiojimo nagrinėjimu atsižvelgiant į jo priėmimo metu buvusias reikšmingas faktines aplinkybes [31] arba jo priėmimą reglamentavusias procedūrines taisykles [32]. Vis dėlto Teisingumo Teismas jau daug kartų nagrinėjo antrinės teisės aktų galiojimą, remdamasis aukštesnės galios materialinės teisės normomis, įsigaliojusiomis po šių aktų priėmimo [33].

92. Vis dėlto, nors yra pateisinama performuluoti prejudicinius klausimus, kuriuose nurodomas *ratione temporis* nebetaikomas aktas, tai negali lemti jų nepriimtinumo [34]. Kaip teigia DPC ir M. Schrems, nuorodas į Direktyvą 95/46 prejudiciniuose klausimuose taip pat galima paaiškinti atsižvelgiant į šios bylos nagrinėjimo trukmę, nes šie klausimai buvo pateikti Teisingumo Teismui prieš įsigaliojant BDAR.

93. Bet kuriuo atveju BDAR nuostatose, kurios bus nagrinėjamos analizuojant prejudicinius klausimus, t. y. konkrečiai jo 45, 46 ir 58 straipsniuose, iš esmės pakartojamas (išplėtojamas atsižvelgiant į tam tikrus nedidelius skirtumus) Direktyvos 95/46 25, 26 ir 28 straipsnių turinys. Kiek tai susiję su jų aspektais, kurie yra reikšmingi priimant sprendimą dėl Sprendimo 2010/87 galiojimo, nematau jokio pagrindo šioms BDAR nuostatoms priskirti kitokią taikymo sritį nei atitinkamoms Direktyvos 95/46 nuostatoms [35].

2. Dėl DPC išreikštų abejonių negalutinio pobūdžio

94. Vokietijos vyriausybės teigimu, prašymas priimti prejudicinį sprendimą yra nepriimtinas todėl, kad Sprendimo *Schrems* 65 punkte nurodyta ieškinio pareiškimo procedūra reikalauja, kad priežiūros institucija būtų susidariusi galutinę nuomonę dėl ieškovo pateiktų prieštaravimų dėl nagrinėjamo sprendimo galiojimo, pagrįstumo. Taip nėra šioje byloje nagrinėjamu atveju, nes DPC išreiškė abejones dėl Sprendimo 2010/87 galiojimo (kurio, be to, M. Schrems neginčija) negalutiniame sprendimo projekte, nedarant poveikio galimam papildomų *Facebook Ireland* ir M. Schrems pastabų pateikimui.

30 Pažymiu, kad pagal BDAR 46 straipsnio 5 dalį sprendimai, kuriuos Komisija priėmė remdamasi Direktyvos 95/46 26 straipsnio 4 dalimi, lieka galioti tol, kol bus iš dalies pakeisti, pakeisti naujais sprendimais arba panaikinti.

31 Žr., be kita ko, 1979 m. vasario 7 d. Sprendimą *Prancūzija / Komisija* (15/76 ir 16/76, EU:C:1979:29, 7 punktas); 2001 m. gegužės 17 d. Sprendimą *IECC / Komisija* (C-449/98 P, EU:C:2001:275, 87 punktas) ir 2013 m. spalio 17 d. Sprendimą *Schaible* (C-101/12, EU:C:2013:661, 50 punktas).

32 Žr., be kita ko, 2015 m. balandžio 16 d. Sprendimą *Parlamentas / Taryba* (C-540/13, EU:C:2015:224, 35 punktas); 2015 m. balandžio 16 d. Sprendimą *Parlamentas / Taryba* (C-317/13 ir C-679/13, EU:C:2015:223, 45 punktas) ir 2016 m. rugsėjo 22 d. Sprendimą *Parlamentas / Taryba* (C-14/15 ir C-116/15, EU:C:2016:715, 48 punktas).

33 Sprendime *Schrems* Teisingumo Teismas vertino sprendimo dėl „saugaus uosto“ galiojimą, atsižvelgdamas į Chartijos, kuri buvo priimta vėliau nei šis sprendimas, nuostatas. Taip pat žr. 2011 m. kovo 17 d. Sprendimą *AJD Tuna* (C-221/09, EU:C:2011:153, 48 punktas) ir 2015 m. birželio 11 d. Sprendimą *Pfeifer & Langen* (C-51/14, EU:C:2015:380, 42 punktas).

34 Žr., be kita ko, 2010 m. liepos 15 d. Sprendimą *Pannon Gép Centrum* (C-368/09, EU:C:2010:441, 30–35 punktai); 2011 m. vasario 10 d. Sprendimą *Andersson* (C-30/10, EU:C:2011:66, 20 ir 21 punktai) ir 2018 m. spalio 25 d. Sprendimą *Roche Lietuva* (C-413/17, EU:C:2018:865, 17–20 punktai).

35 Šiuo klausimu žr. generalinio advokato M. Bobek išvadą byloje *Fashion ID* (C-40/17, EU:C:2018:1039, 87 punktas).

95. Mano nuomone, negalutinis DPC išreikštų abejonių pobūdis neturi poveikio prašymo priimti prejudicinį sprendimą priimtinumui. Prejudicinio klausimo priimtinumo kriterijai turi būti vertinami atsižvelgiant į ginčo dalyką, kurį yra apibrėžęs prašymą priimti prejudicinį sprendimą pateikęs teismas [36]. Vis dėlto neginčijama, kad jis susijęs su Sprendimo 2010/87 galiojimu. Kaip nurodyta nutartyje dėl prašymo priimti prejudicinį sprendimą ir prie jos pridėtame teismo sprendime, šis teismas mano, kad DPC išreikštos abejonės, nesvarbu, ar jos buvo negalutinės, ar galutinės, yra pagrįstos, todėl jis kreipėsi į Teisingumo Teismą su klausimu dėl šio sprendimo galiojimo. Tokiomis aplinkybėmis Teisingumo Teismo išaiškinimas šiuo klausimu yra neabejotinai svarbus minėtam teismui, kad jis galėtų išspręsti jam perduotą ginčą.

3. Dėl neaiškumų, susijusių su faktinių aplinkybių nustatymu

96. Jungtinės Karalystės vyriausybė teigia, kad prašymą priimti prejudicinį sprendimą pateikęs teismas netiksliai apibūdino faktines aplinkybes, todėl prejudiciniai klausimai yra nepriimtini. Minėtas teismas nepaaiškino, ar M. Schrems asmens duomenys tikrai buvo perduodami į JAV, o jei taip, tai ar JAV valdžios institucijos juos rinko. Be to, nebuvo tiksliai nustatytas šio galimo duomenų perdavimo teisinis pagrindas, nutartyje dėl prašymo priimti prejudicinį sprendimą tiesiog paminint, kad socialinio tinklo *Facebook* naudotojų Europoje duomenys „daugiausia“ perduodami remiantis Sprendime 2010/87 numatytomis standartinėmis sutarčių sąlygomis. Bet kuriuo atveju nebuvo nustatyta, kad šios sąlygos buvo tiksliai įtrauktos į *Facebook Ireland* ir *Facebook Inc*. sutartį, kuria buvo remiamasi kaip ginčijamo duomenų perdavimo pagrindu. Vokietijos vyriausybė taip pat ginčija prašymo priimti prejudicinį sprendimą priimtinumą, motyvuodama tuo, kad prašymą priimti prejudicinį sprendimą pateikęs teismas neišnagrinėjo, ar M. Schrems iš tiesų davė sutikimą perduoti duomenis, nes tokiu atveju perdavimas būtų buvęs teisėtai grindžiamas Direktyvos 95/46 26 straipsnio 1 dalimi (šios nuostatos turinys iš esmės pakartotas BDAR 49 straipsnio 1 dalies a punkte).

97. Šie argumentai neleidžia suabejoti prašymo priimti prejudicinį sprendimą svarba atsižvelgiant į pagrindinės bylos dalyką. Kadangi šis ginčas kilo DPC pasinaudojus Sprendimo *Schrems* 65 punkte numatyta teisių gynimo priemone, pats jo tikslas yra tas, kad nacionalinis teismas kreiptųsi prejudicinio sprendimo dėl Sprendimo 2010/87 galiojimo. Vokietijos ir Jungtinės Karalystės vyriausybės ginčija prejudicinių klausimų reikalingumą ne tam, kad būtų nustatyta, ar šis sprendimas galioja, o tam, kad DPC būtų suteikta galimybė priimti sprendimą *in concreto* dėl M. Schrems skundo.

98. Bet kuriuo atveju, net atsižvelgiant į šią pirminę procedūrą pagrindinėje byloje, prejudiciniai klausimai, susiję su Sprendimo 2010/87 galiojimu, man neatrodo nesvarbūs. Iš tiesų prašymą priimti prejudicinį sprendimą pateikęs teismas nustatė, kad po sprendimo dėl „saugaus uosto“ pripažinimo negaliojančiu *Facebook Ireland* toliau perdavinėjo savo naudotojų duomenis į JAV ir kad šios duomenų perdavimo operacijos (bent dalis jų) grindžiamos Sprendimu 2010/87. Be to, nors ir gali būti naudinga, kad visos reikšmingos faktinės aplinkybės būtų nustatytos prieš prašymą priimti prejudicinį sprendimą pateikusiam teismui pasinaudojant jam pagal SESV 267 straipsnį suteikta kompetencija, tik šis teismas turi įvertinti, kokiu proceso etapu jam yra reikalingas Teisingumo Teismo prejudicinis sprendimas [37].

99. Atsižvelgdamas į visa tai, kas išdėstyta, manau, kad prašymas priimti prejudicinį sprendimą yra priimtinas.

36 Žr. šios išvados 87 punktą.

37 Šiuo klausimu žr. 1982 m. balandžio 1 d. Sprendimą *Holdijk ir kt.* (141/81–143/81, EU:C:1982:122, 5 punktas) ir 2003 m. gruodžio 9 d. Sprendimą *Gasser* (C-116/02, EU:C:2003:657, 27 punktas).

C. Dėl Sąjungos teisės taikytinumo asmens duomenų perdavimui komerciniais tikslais į trečiąją valstybę, kuri gali juos tvarkyti nacionalinio saugumo tikslais (pirmasis klausimas)

100. Pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, ar Sąjungos teisė taikoma tais atvejais, kai valstybėje narėje esanti bendrovė komerciniais tikslais perduoda asmens duomenis trečiojoje šalyje įsteigtai bendrovei, jeigu pradėjus perduoti duomenis šios trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis, be kita ko, nacionalinio saugumo tikslais.

101. Šis klausimas yra svarbus sprendimui pagrindinėje byloje priimti, nes jeigu tokiam duomenų perdavimui Sąjungos teisė netaikoma, visi šioje byloje iškelti prieštaravimai dėl Sprendimo 2010/87 galiojimo netektų pagrindo.

102. Kaip pažymėjo prašymą priimti prejudicinį sprendimą pateikęs teismas, asmens duomenų tvarkymas nacionalinio saugumo tikslais nebuvo įtrauktas į Direktyvos 95/46 taikymo sritį pagal jos 3 straipsnio 2 dalį. Dabar BDAR 2 straipsnio 2 dalyje patikslinta, kad šis reglamentas netaikomas, be kita ko, duomenų tvarkymui, kai duomenys tvarkomi vykdant veiklą, kuriai Sąjungos teisė netaikoma, arba kai kompetentingos valdžios institucijos juos tvarko, siekdamos apsaugoti visuomenės saugumą. Šios nuostatos atspindi ESS 4 straipsnio 2 dalyje valstybėms narėms pripažįstamą išlygą dėl kompetencijos nacionalinio saugumo užtikrinimo srityje.

103. DPC, M. Schrems, Airija, Vokietijos, Austrijos, Belgijos, Čekijos, Nyderlandų, Lenkijos ir Portugalijos vyriausybės, taip pat Parlamentas ir Komisija teigia, kad tokiam duomenų perdavimui, kuris nurodytas M. Schrems skunde, šios nuostatos netaikomos, todėl jis patenka į Sąjungos teisės taikymo sritį. *Facebook Ireland* teigia priešingai. Palaikau pirmąjį iš šių požiūrių.

104. Šiuo klausimu reikėtų pažymėti, kad asmens duomenų perdavimas iš valstybės narės į trečiąją šalį savaime yra „duomenų tvarkymas“, kaip tai suprantama pagal BDAR 4 straipsnio 2 punktą, atliekamas valstybės narės teritorijoje [38]. Pirmuoju prejudiciniu klausimu konkrečiai siekiama nustatyti, ar Sąjungos teisė taikoma *duomenų tvarkymui, kurį sudaro pats duomenų perdavimas*. Šis klausimas nėra susijęs su Sąjungos teisės taikytinumu galimam paskesniam į JAV perduotų duomenų tvarkymui, kurį JAV valdžios institucijos atliktų nacionalinio saugumo tikslais, nepatenkančiam į BDAR teritorinę taikymo sritį [39].

105. Šiuo požiūriu siekiant nustatyti, ar Sąjungos teisė taikoma 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 [40].

106. Vis dėlto iš nutarties dėl prašymo priimti prejudicinį sprendimą matyti, kad M. Schrems skunde nurodytas duomenų tvarkymas susijęs su komercine veikla. Be to, nagrinėjami duomenys buvo perduodami nesiekiant tikslo leisti JAV valdžios institucijoms vėliau juos tvarkyti nacionalinio saugumo tikslais.

38 Šiuo klausimu žr. 2006 m. gegužės 30 d. Sprendimą *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346, toliau – Sprendimas *PNR*, 56 punktas) ir Sprendimą *Schrems* (45 punktas). BDAR 4 straipsnio 2 punkte iš esmės pakartojama sąvokos „duomenų tvarkymas“ apibrėžtis, kuri buvo pateikta Direktyvos 95/46 2 straipsnio b punkte.

39 Pagal BDAR 3 straipsnio 1 dalį šis reglamentas 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. Klausimą dėl Sąjungos teisės taikytinumo trečiosios šalies žvalgybos tarnybų už Sąjungos ribų atliekamam duomenų tvarkymui reikia skirti nuo šio duomenų tvarkymo taisyklių ir praktikos svarbos nagrinėjamoje trečiojoje šalyje, siekiant nustatyti, ar joje yra užtikrinama tinkamo lygio apsauga. Su šia tema susijęs antrasis prejudicinis klausimas, kuris nagrinėjamas šios išvados 201–229 punktuose.

40 Savo išvadoje byloje *Ministerio Fiscal* (C-207/16, EU:C:2018:300, 47 punktas) pabrėžiau skirtumą tarp, pirma, vykdant valstybės veiksmus atliekamo tiesioginio duomenų tvarkymo ir, antra, atliekamo komercinio duomenų, kuriuos paskui naudoja viešosios valdžios institucijos, tvarkymo.

107. Dar reikėtų pridurti, kad, laikantis *Facebook Ireland* siūlomo požiūrio, BDAR nuostatos, susijusios su duomenų perdavimu į trečiąsias šalis, taptų neveiksmingos, nes niekada negalima atmesti, kad vykdant komercinę veiklą perduoti duomenys po jų perdavimo bus tvarkomi nacionalinio saugumo tikslais.

108. Mano siūlomą aiškinimą patvirtina BDAR 45 straipsnio 2 dalies a punkto formuluotė. Šioje nuostatoje nurodyta, kad jeigu Komisija priima sprendimą dėl tinkamumo, ji atsižvelgia, be kita ko, į konkrečios trečiosios šalies teisės aktus *nacionalinio saugumo srityje*. Iš to galima spręsti, kad galimybė, kad trečiosios paskirties šalies valdžios institucijos tvarkys duomenis, siekdamos užtikrinti nacionalinį saugumą, nereiškia, kad Sąjungos teisė netaikytina duomenų tvarkymui, kurį sudaro duomenų perdavimas į šią trečiąją šalį.

109. Teisingumo Teismo motyvai ir išvados Sprendime *Schrems* taip pat grindžiami šia prielaida. Visų pirma Teisingumo Teismas jame nagrinėjo sprendimo dėl „saugaus uosto“ galiojimą, kiek jis buvo susijęs su asmens duomenų perdavimu į JAV, kur jie galėjo būti renkami ir tvarkomi nacionalinio saugumo užtikrinimo tikslais, atsižvelgiant į Direktyvos 95/46 25 straipsnio 6 dalį, aiškinamą atsižvelgiant į Chartiją [41].

110. Atsižvelgdamas į šiuos argumentus, laikausi nuomonės, kad Sąjungos teisė taikoma asmens duomenų perdavimui iš valstybės narės į trečiąją šalį, jeigu šie duomenys perduodami vykdant komercinę veiklą, ir tai, ar šie duomenys vėliau gali būti tvarkomi šios trečiosios šalies viešosios valdžios institucijų siekiant užtikrinti nacionalinį saugumą, neturi reikšmės.

D. Dėl apsaugos lygio, reikalaujamo perduodant duomenis remiantis standartinėmis sutarčių sąlygomis (šeštojo prejudicinio klausimo pirma dalis)

111. Šeštojo prejudicinio klausimo pirmoje dalyje prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, koks yra duomenų subjektų pagrindinių teisių apsaugos lygis, kuris turi būti užtikrinamas, kad asmens duomenys galėtų būti perduodami į trečiąją šalį pagal Sprendime 2010/87 numatytas standartines sutarčių sąlygas.

112. Minėtas teismas pažymi, jog Sprendime *Schrems* Teisingumo Teismas Direktyvos 95/46 25 straipsnio 6 dalį (jos turinys iš esmės pakartotas BDAR 45 straipsnio 3 dalyje) tiek, kiek joje buvo numatyta, kad Komisija gali priimti sprendimą dėl tinkamumo tik įsitikinusi, kad nurodyta trečioji šalis užtikrina *tinkamą* apsaugos lygį, aiškino taip, kad ši šalis užtikrina *iš esmės tokį patį* pagrindinių laisvių ir teisių apsaugos lygį, koks garantuojamas Sąjungoje pagal šią direktyvą, aiškinamą atsižvelgiant į Chartiją [42].

113. Šiomis aplinkybėmis pagal pirmą šeštojo prejudicinio klausimo dalį Teisingumo Teismo prašoma nustatyti, ar „sutarčių standartinių sąlygų“, kurias Komisija priėmė pagal Direktyvos 95/46 26 straipsnio 4 dalį ir kurios atitinka dabar BDAR 46 straipsnio 2 dalies c punkte minimas „standartines duomenų apsaugos sąlygas“, taikymas turi leisti pasiekti tokį apsaugos lygį, kuris atitiktų tą patį „esminio tapatumo“ standartą.

41 2017 m. liepos 26 d. Nuomonėje 1/15 (*ES ir Kanados susitarimas dėl PNR*) (EU:C:2017:592, toliau – Nuomonė 1/15) Teisingumo Teismas nagrinėjo, ar Kanados ir Sąjungos tarptautinio susitarimo dėl duomenų, kurie, perduoti į Kanadą, turėjo būti tvarkomi viešosios valdžios institucijų nacionalinio saugumo tikslais, projektas atitinka Chartijos 7, 8 ir 47 straipsnius.

42 Sprendimas *Schrems* (73 punktas). Teisingumo Teismas patvirtino šią išvadą Nuomonėje 1/15 (134 punktas).

114. Šiuo klausimu BDAR 46 straipsnio 1 dalyje numatyta, kad duomenų valdytojas gali perduoti asmens duomenis į trečiąją šalį nesant sprendimo dėl tinkamumo 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“ (išskirta mano)[43]. Pagal BDAR 46 straipsnio 2 dalies c punktą šios apsaugos priemonės, be kita ko, gali būti nustatomos Komisijos parengtomis standartinėmis duomenų apsaugos sąlygomis.

115. Pritardamas DPC, M. Schrems ir Airijai, laikausi nuomonės, kad BDAR 46 straipsnio 1 dalyje nurodytos duomenų valdytojo nustatomos „tinkamos apsaugos priemonės“ turi užtikrinti, kad asmenų, kurių duomenys perduodami, teisėms, kaip ir perduodant duomenis remiantis sprendimu dėl tinkamumo, suteikiamas apsaugos lygis būtų iš esmės toks pat kaip numatytasis BDAR, aiškinamame atsižvelgiant į Chartiją.

116. Šią išvadą lemia šios nuostatos ir teisės akto, kuriame ji įtvirtinta, tikslas.

117. BDAR 45 ir 46 straipsnių tikslas – užtikrinti šiuo reglamentu garantuojamo aukšto asmens duomenų apsaugos lygio tęstinumą, kai šie duomenys perduodami už Sąjungos ribų. BDAR 44 straipsniu „Bendras duomenų perdavimo principas“ pradedamas jo V skyrius, kuriame reglamentuojamas duomenų perdavimas į trečiąsias šalis, nurodant, kad visos šio skyriaus nuostatos taikomos siekiant užtikrinti, kad, jeigu duomenys perduodami į trečiąją valstybę, nebūtų pakenkta šiuo reglamentu garantuojamam apsaugos lygiui[44]. Šia taisykle siekiama išvengti, kad perduodant asmens duomenis į trečiąją šalį jų tvarkymo tikslu būtų nepaisoma Sąjungos teisės suteikiamo apsaugos lygio[45]. Atsižvelgiant į šį tikslą, nesvarbu, ar duomenų perdavimas grindžiamas sprendimu dėl tinkamumo, ar duomenų valdytojo numatytomis apsaugos priemonėmis, be kita ko, pasitelkiant standartines sutarčių sąlygas. Chartijoje užtikrinamų pagrindinių teisių apsaugos reikalavimai taikomi nedarant skirtumo pagal tai, kokiu teisiniu pagrindu grindžiamas konkretus duomenų perdavimas[46].

118. Vis dėlto tai, kaip yra išlaikomas aukšto apsaugos lygio tęstinumas, skiriasi atsižvelgiant į duomenų perdavimo teisinį pagrindą.

119. Pirma, sprendimo dėl tinkamumo tikslas – konstatuoti, kad jame nurodyta trečioji šalis pati užtikrina iš esmės tokį patį apsaugos lygį kaip tas, kuris turi būti užtikrinamas Sąjungoje. Priimdama sprendimą dėl tinkamumo Komisija prieš tai konkrečios trečiosios šalies atveju turi įvertinti šios trečiosios šalies teisėje ir praktikoje užtikrinamą apsaugos lygį atsižvelgiant į BDAR 45 straipsnio 3 dalyje nurodytus veiksnius. Taigi asmens duomenys gali būti perduodami į šią trečiąją šalį nereikalaujant, kad duomenų valdytojas gautų kokį nors leidimą.

120. Antra, kaip išsamiau paaiškinta tolesnėje šios išvados dalyje, duomenų valdytojo numatytomis tinkamomis apsaugos priemonėmis siekiama užtikrinti aukštą apsaugos lygį, jeigu trečiojoje paskirties šalyje suteikiamos apsaugos priemonės nėra pakankamos. Taigi, nors pagal BDAR 46 straipsnio 1 dalį asmens duomenis į trečiąsias valstybes leidžiama perduoti neužtikrinant tinkamo apsaugos lygio, pagal

43 Direktyvos 95/46 26 straipsnio 2 dalyje buvo numatyta, kad valstybė narė gali leisti tokį duomenų perdavimą, „jeigu duomenų valdytojas pateikia *adekvačias apsaugos priemones* asmenų privatumui ir pagrindinėms teisėms bei laisvėms apsaugoti ir atitinkamoms teisėms įgyvendinti“ (išskirta mano). Mano nuomone, minėtoje nuostatoje ir BDAR 46 straipsnio 1 dalyje atitinkamai vartojamų adekvačių apsaugos priemonių ir tinkamų apsaugos priemonių sąvokų turinys nesiskiria.

44 Šiuo klausimu BDAR 6 konstatuojamojoje dalyje nurodyta, kad perduodant duomenis Sąjungoje ir už jos ribų turi būti užtikrinamas „aukštas“ duomenų apsaugos lygis. Taip pat žr. BDAR 101 konstatuojamąją dalį.

45 Žr. Sprendimą *Schrems* (73 punktas) ir Nuomonę 1/15 (214 punktas).

46 Tai neturi poveikio galimybei perduoti asmens duomenis net ir nesant tinkamų apsaugos priemonių remiantis BDAR 49 straipsnio 1 dalyje numatytais nukrypti leidžiančių nuostatų pagrindais.

šią nuostatą šiuos duomenis leidžiama perduoti tik jeigu tinkamos apsaugos priemonės užtikrinamos kitais būdais. Šiuo atveju Komisijos priimtos standartinės sutarčių sąlygos yra duomenų perdavimui taikomas bendras mechanizmas, neatsižvelgiant į trečiąją paskirties šalį ir joje užtikrinamą apsaugos lygį.

E. Dėl Sprendimo 2010/87 galiojimo atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius (septintasis, aštuntasis ir vienuoliktasis prejudiciniai klausimai)

121. Septintuoju prejudiciniu klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia sužinoti, ar Sprendimas 2010/87 negalioja todėl, kad jis nesaisto trečiųjų valstybių, į kurias duomenys perduodami remiantis šio sprendimo priede numatytomis standartinėmis sutarčių sąlygomis, valdžios institucijų, ir visų pirma todėl, kad juo šioms valdžios institucijoms nedraudžiama reikalauti, kad duomenų importuotojas pateiktų joms šiuos duomenis. Taigi šiuo klausimu kvestionuojama pati galimybė užtikrinti tinkamą tokių duomenų apsaugos lygį taikant vien sutartinio pobūdžio mechanizmus. Vienuoliktasis prejudicinis klausimas bendrai susijęs su Sprendimo 2010/87 galiojimu atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius.

122. Aštuntuoju prejudiciniu klausimu Teisingumo Teismo prašoma nustatyti, ar priežiūros institucija turi pasinaudoti jai pagal BDAR 58 straipsnio 2 dalies f ir j punktus suteiktais įgaliojimais, kad sustabdytų Sprendime 2010/87 numatytomis standartinėmis sutarčių sąlygomis grindžiamą duomenų perdavimą į trečiąją šalį, jeigu mano, kad duomenų importuotojui šioje trečiojoje šalyje taikomi įpareigojimai, neleidžiantys jam laikytis šių sąlygų ir dėl šių įpareigojimų nėra užtikrinamas tinkamas perduodamų duomenų apsaugos lygis. Kadangi, mano nuomone, atsakymas į šį klausimą turi poveikį Sprendimo 2010/87 galiojimui [47], nagrinėsiu jį kartu su septintuoju ir vienuoliktuoju prejudiciniais klausimais.

123. BDAR 46 straipsnio 1 dalies formuluotė, nurodant, kad *„jeigu nėra priimtas sprendimas pagal 45 straipsnio 3 dalį*, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją valstybę <…> tik tuo atveju, jeigu duomenų valdytojas arba duomenų tvarkytojas *yra nustatęs* tinkamas apsaugos priemones <…>“ (išskirta mano), parodo logiką, kuria grindžiami sutartiniai mechanizmai, kaip antai numatytieji Sprendime 2010/87. Kaip pažymėta BDAR 108 ir 114 konstatuojamosiose dalyse, šių mechanizmų tikslas – leisti perduoti duomenis į trečiąsias šalis, dėl kurių Komisija nėra priėmusi sprendimo dėl tinkamumo, todėl galimai nepakankama šios trečiosios šalies teisės sistemoje užtikrinama duomenų apsauga *kompensuojama* apsaugos priemonėmis, kurių duomenų eksportuotojas ir duomenų importuotojas įsipareigoja laikytis pagal sutartį.

124. Kadangi sutartinių garantijų esmė būtent ir yra užpildyti galimas trečiosios paskirties šalies siūlomos apsaugos spragas, nesvarbu, kokios jos būtų, sprendimo, kuriuo Komisija konstatuoja, kad tam tikros standartinės sąlygos tinkamai užpildo šias spragas, galiojimas negali priklausyti nuo kiekvienoje konkrečioje trečiojoje šalyje, į kurią gali būti perduodami duomenys, užtikrinamo apsaugos lygio. Tokio sprendimo galiojimas priklauso tik nuo šiose sąlygose numatytų apsaugos priemonių, skirtų galimam apsaugos nepakankamumui trečiojoje paskirties šalyje kompensuoti, patikimumo. Šių apsaugos priemonių veiksmingumas taip pat turi būti vertinamas atsižvelgiant į saugiklius – BDAR 58 straipsnio 2 dalyje numatytus priežiūros institucijų įgaliojimus.

47 Žr. šios išvados 128 punktą.

125. Šiuo klausimu, kaip iš esmės pažymėjo DPC, M. Schrems, BSA, Airija, Austrijos, Prancūzijos, Lenkijos ir Portugalijos vyriausybės bei Komisija, standartinėse sutarčių sąlygose nustatytos garantijos gali būti susilpnintos ar net panaikintos, jeigu trečiosios paskirties šalies teisėje duomenų importuotojui nustatyti minėtų sąlygų reikalavimams prieštaraujantys įpareigojimai. Taigi dėl trečiojoje paskirties šalyje galiojančių teisės aktų, atsižvelgiant į konkrečias duomenų perdavimo aplinkybes [48], šiose sąlygose numatytų įpareigojimų gali būti neįmanoma įgyvendinti.

126. Tokiomis aplinkybėmis, kaip pažymėjo M. Schrems ir Komisija, BDAR 46 straipsnio 2 dalies c punkte numatytas sutartinis mechanizmas grindžiamas duomenų eksportuotojo ir papildomai – priežiūros institucijų atsakomybės nustatymu. Taigi *atsižvelgdamas į kiekvieną konkretų atvejį* dėl kiekvieno konkretaus duomenų perdavimo duomenų valdytojas arba, jam nesiėmus veiksmų, priežiūros institucija nagrinės, ar trečiosios paskirties šalies teisė kliudo įgyvendinti standartines sąlygas, vadinasi, ir užtikrinti tinkamą perduodamų duomenų apsaugą, ir ar duomenų perdavimą reikia uždrausti arba sustabdyti.

127. Atsižvelgdamas į šias pastabas manau, jog vien tai, kad Sprendimas 2010/87 ir jame nustatytos standartinės sutarčių sąlygos nesaisto trečiosios paskirties šalies valdžios institucijų, savaime nedaro šio sprendimo negaliojančio. Mano nuomone, Sprendimo 2010/87 atitiktis Chartijos 7, 8 ir 47 straipsniams priklauso nuo to, ar yra pakankamai patikimi mechanizmai, leidžiantys užtikrinti, kad standartinėmis sutarčių sąlygomis grindžiamas duomenų perdavimas būtų sustabdytas ar uždraustas pažeidus šias sąlygas arba nesant galimybės jų laikytis.

128. Šiuo klausimu BDAR 46 straipsnio 1 dalyje numatyta, kad taikant tinkamas apsaugos priemones duomenys gali būti perduodami „su sąlyga, kad suteikiama galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis“. Reikės patikrinti, ar Sprendimo 2010/87 priede nustatytose sąlygose numatytos apsaugos priemonės, papildytos priežiūros institucijų įgaliojimais, leidžia užtikrinti šios sąlygos laikymąsi. Manau, taip yra tik tuo atveju, jeigu duomenų valdytojams (1 dalis), o jeigu jie nesiima veiksmų – priežiūros institucijoms (2 dalis) nustatyta *pareiga* sustabdyti arba uždrausti duomenų perdavimą, jeigu dėl įpareigojimų, kylančių iš sutarčių standartinių sąlygų, ir trečiosios paskirties šalies teisėje nustatytų įpareigojimų prieštaros šių sąlygų neįmanoma laikytis.

1. Dėl duomenų valdytojams tenkančių įpareigojimų

129. Pirma, pagal Sprendimo 2010/87 priede esančias standartines sutarčių sąlygas reikalaujama, kad jeigu jose numatyti įpareigojimai prieštarauja iš trečiosios paskirties šalies teisės kylantiems reikalavimams, šiomis sąlygomis negali būti remiamasi perduodant duomenis į šią trečiąją šalį, o jeigu duomenys jau buvo pradėti perduoti remiantis šiomis sąlygomis, duomenų eksportuotojui turi būti pranešama apie šį prieštaravimą ir jis gali duomenų perdavimą sustabdyti.

130. Taigi pagal 5 sąlygos a punktą duomenų importuotojas įsipareigoja tvarkyti perduotus asmens duomenis tik duomenų eksportuotojo vardu laikydamasis jo nurodymų bei sutarčių standartinių sąlygų. Jeigu duomenų importuotojas negali užtikrinti atitikties šioms sąlygoms, jis sutinka kuo skubiau pranešti duomenų importuotojui apie tai, ir tokiu atveju duomenų eksportuotojas turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį [49].

48 Pavyzdžiui, galima įsivaizduoti, kad trečioji šalis numato telekomunikacijų paslaugų teikėjams įpareigojimą suteikti viešosios valdžios institucijoms prieigą prie perduodamų duomenų be jokių apribojimų ar apsaugos priemonių. Nors šie paslaugų teikėjai negalėtų laikytis sutarčių standartinių sąlygų, vis dėlto įmonės, kurioms šis įpareigojimas netaikomas, galėtų nekliudomai jų laikytis.

49 Taip pat pažymiu, kad pagal 5 sąlygos d punkto i papunktį duomenų importuotojas atleidžiamas nuo pareigos informuoti duomenų eksportuotoją apie teisiškai įpareigojantį trečiosios šalies teisėsaugos institucijų prašymą atskleisti asmens duomenis, jeigu pagal šios trečiosios šalies teisę toks informavimas yra draudžiamas. Tokiu atveju duomenų eksportuotojas neturės galimybės sustabdyti duomenų perdavimo, jeigu dėl tokio atskleidimo, apie kurį jis nežinojo, pažeidžiamos standartinės sąlygos. Vis dėlto pagal 5 sąlygos a punktą duomenų importuotojui išlieka pareiga prireikus informuoti duomenų eksportuotoją apie tai, kad, jo nuomone, šios trečiosios šalies teisės aktai neleidžia jam laikytis savo įsipareigojimų pagal standartines sutarčių sąlygas.

131. 5 sąlygos 5 išnašoje patikslinama, kad standartinės sutarčių sąlygos nėra pažeidžiamos, jeigu duomenų importuotojas laikosi nacionalinės teisės aktuose, kurie jam taikomi trečiojoje šalyje, įtvirtintų privalomų reikalavimų, jeigu šie reikalavimai neviršija demokratinėje visuomenėje reikalingų apribojimų, skirtų apsaugoti vienam iš Direktyvos 95/46 13 straipsnio 1 dalyje (jos turinys iš esmės pakartotas BDAR 23 straipsnio 1 dalyje) nurodytų interesų, tarp kurių yra visuomenės saugumas ir valstybės saugumas. Ir atvirkščiai, šių sąlygų nesilaikymas siekiant įvykdyti joms prieštaraujantį įpareigojimą, kylantį iš trečiosios paskirties šalies teisės, viršijantį tai, kas yra proporcinga Sąjungos pripažįstamam teisėtam interesui apsaugoti, laikomas minėtų sąlygų pažeidimu.

132. Mano nuomone, ir kaip teigia M. Schrems ir Komisija, 5 sąlygos a punktas negali būti aiškinamas taip, kad duomenų perdavimo sustabdymas ar sutarties nutraukimas yra tik neprivalomas, jeigu duomenų importuotojas negali laikytis standartinių sąlygų. Nors šioje sąlygoje nurodoma tik teisė, šioje srityje suteikiama duomenų eksportuotojui, ši formuluotė turi būti suprantama atsižvelgiant į jos sutartinį kontekstą. Tai, kad duomenų eksportuotojui *dvišaliuose santykiuose su duomenų importuotoju* suteikiama teisė sustabdyti duomenų perdavimą arba nutraukti sutartį, jeigu duomenų importuotojas negali laikytis standartinių sąlygų, neturi poveikio duomenų eksportuotojui nustatytai pareigai sustabdyti duomenų perdavimą arba nutraukti sutartį *atsižvelgiant į duomenų subjektų teisių, kylančių iš BDAR, apsaugos reikalavimus*. Bet koks kitas aiškinimas lemtų Sprendimo 2010/87 negaliojimą, nes jame numatytos standartinės sutarčių sąlygos neleistų duomenų perdavimui taikyti „tinkamas apsaugos priemones“, kaip to reikalaujama BDAR 46 straipsnio 1 dalyje, aiškinamoje atsižvelgiant į Chartijos nuostatas [50].

133. Be to, pagal 5 sąlygos b punktą duomenų importuotojas patvirtina neturintis pagrindo manyti, kad pagal jam taikytinus teisės aktus negalės vykdyti iš duomenų eksportuotojo gautų nurodymų ir įsipareigojimų pagal sutartį. Jeigu šie teisės aktai pakeičiami ir šie pakeitimai turi didelį neigiamą poveikį pagal šias sąlygas teikiamoms garantijoms ir prisiimtiems įsipareigojimams, jis kuo greičiau praneš apie šiuos pasikeitimus duomenų eksportuotojui, kai tik apie juos sužinos, o duomenų eksportuotojas tokiu atveju turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį. Pagal 4 sąlygos g punktą duomenų eksportuotojas turi persiųsti pranešimą, gautą iš duomenų importuotojo, kompetentingai priežiūros institucijai, jeigu nusprendžia tęsti perdavimą.

134. Manau, kad dabar reikia pateikti kelis patikslinimus dėl analizės, kurią sutarties šalys turi atlikti siekdamos nustatyti, ar, atsižvelgiant į 5 sąlygos išnašą, duomenų importuotojui pagal trečiosios valstybės teisę nustatyti įpareigojimai pažeidžia standartines sąlygas ir dėl to duomenų perdavimui negali būti taikomos tinkamos apsaugos priemonės, turinio. Ši problema iš esmės keliama šeštojo prejudicinio klausimo antroje dalyje.

135. Manau, siekiant atlikti tokią analizę, reikia atsižvelgti į visas kiekvieną duomenų perdavimą apibūdinančias aplinkybes, tarp kurių gali būti duomenų pobūdis ir galimas jų jautrus pobūdis, duomenų eksportuotojo ir (arba) importuotojo įgyvendinti mechanizmai duomenų saugumui užtikrinti [51], trečiosios šalies valdžios institucijų, kurioms bus pateikiami duomenys, atliekamo duomenų tvarkymo pobūdis ir tikslas, šio duomenų tvarkymo taisyklės, taip pat šios trečiosios šalies taikomi apribojimai ir garantijos. Mano supratimu, viešosios valdžios institucijų vykdomą duomenų tvarkymo veiklą apibūdinantys aspektai ir šios trečiosios šalies teisės sistemoje taikytinos apsaugos priemonės gali sutapti su įtvirtintosiomis BDAR 45 straipsnio 2 dalyje.

50 Pagal jurisprudenciją įgyvendinimo akto nuostatos turi būti aiškinamos pagal pagrindinio teisės akto, kuriuo teisės aktų leidėjas leido priimti įgyvendinimo aktą, nuostatas (šiuo klausimu žr., be kita ko, 2017 m. liepos 26 d. Sprendimą *Čekija / Komisija* (C-696/15 P, EU:C:2017:595, 51 punktas); 2018 m. gegužės 17 d. Sprendimą *Evonik Degussa* (C-229/17, EU:C:2018:323, 29 punktas) ir 2019 m. birželio 20 d. Sprendimą *ExxonMobil Production Deutschland* (C-682/17, EU:C:2019:518, 112 punktas). Be to, Sąjungos aktas turi būti aiškinamas kiek įmanoma taip, kad nebūtų paneigtas jo galiojimas, ir laikantis visos pirminės teisės ir, be kita ko, Chartijos nuostatų (žr., be kita ko, 2019 m. gegužės 14 d. Sprendimą *M ir kt.* (*Pabėgėlio statuso panaikinimas*) (C-391/16, C-77/17 ir C-78/17, EU:C:2019:403, 77 punktas ir jame nurodyta jurisprudencija).

51 Šiuo klausimu BDAR 109 konstatuojamojoje dalyje duomenų eksportuotojai ir importuotojai raginami į standartines duomenų apsaugos sąlygas įtraukti papildomas apsaugos priemones, be kita ko, sudarant sutartis.

136. Antra, Sprendimo 2010/87 priede nustatytomis standartinėmis sutarčių sąlygomis duomenų subjektams suteikiamos teisės, kuriomis jie gali remtis, ir teisių gynimo priemonės, kuriomis jie gali pasinaudoti prieš duomenų eksportuotoją ir papildomai – prieš duomenų importuotoją.

137. 3 sąlygos „Trečiosios šalies naudos gavėjos sąlyga“ 1 dalyje numatyta duomenų subjekto teisė pareikšti ieškinį duomenų eksportuotojui, jeigu yra pažeidžiami, be kita ko, 5 sąlygos a arba b punktai. Pagal 3 sąlygos 2 dalį, jeigu duomenų eksportuotojas yra faktiškai dingęs arba teisiškai nutraukė savo veiklą, duomenų subjektas gali remtis šia sąlyga prieš duomenų importuotoją.

138. 6 sąlygos 1 dalyje kiekvienam duomenų subjektui, patyrusiam žalą dėl 3 sąlygoje numatytų įpareigojimų neįvykdymo, suteikiama teisė reikalauti, kad duomenų eksportuotojas atlygintų patirtą žalą. Pagal 7 sąlygos 1 dalį, jeigu duomenų subjektas prieš duomenų importuotoją pasinaudoja trečiosios šalies naudos gavėjos teisėmis ir (arba) pareikalauja atlyginti patirtą žalą, duomenų importuotojas įsipareigoja sutikti su duomenų subjekto sprendimu kreiptis dėl ginčo į tarpininką, kurio vaidmenį atliktų nepriklausomas asmuo, arba, kai taikytina, kreiptis dėl ginčo į valstybės narės, kurioje yra įsisteigęs duomenų eksportuotojas, teismus.

139. Be teisių gynimo priemonių, suteikiamų pagal Sprendimo 2010/87 priede numatytas standartines sutarčių sąlygas, duomenų subjektai, manydami, kad šios sąlygos buvo pažeistos, gali prašyti priežiūros institucijų nustatyti taisomąsias priemones pagal BDAR 58 straipsnio 2 dalį, į kurią daroma nuoroda Sprendimo 2010/87 4 straipsnyje [52].

2. Dėl priežiūros institucijoms tenkančių įpareigojimų

140. Dėl toliau nurodytų priežasčių, pritardamas M. Schrems, Airijai, Vokietijos, Austrijos, Belgijos, Nyderlandų ir Portugalijos vyriausybėms, taip pat EDPB, esu linkęs manyti, kad pagal BDAR 58 straipsnio 2 dalį priežiūros institucijos, kruopščiai ištyrusios ir nusprendusios, kad į trečiąją šalį perduotiems duomenims nėra taikoma tinkama apsauga, nes nėra laikomasi sutartyje numatytų sąlygų, privalo imtis tinkamų priemonių šiam pažeidimui ištaisyti, ir prireikus nurodyti sustabdyti duomenų perdavimą.

141. Pirma, norėčiau pažymėti, kad, priešingai, nei teigia DPC, Sprendime 2010/87 nėra nė vienos nuostatos, pagal kurią įgyvendinti įgaliojimus „nustatyti laikiną arba galutinį duomenų tvarkymo apribojimą, įskaitant tvarkymo draudimą“ ir „nurodyti sustabdyti duomenų srautus duomenų gavėjui trečiojoje valstybėje“, suteikiamus priežiūros institucijoms pagal BDAR 58 straipsnio 2 dalies f ir j punktus, būtų leidžiama tik išimtiniais atvejais.

142. Sprendimo 2010/87 pirminės redakcijos 4 straipsnio 1 dalyje priežiūros institucijoms pasinaudoti įgaliojimais sustabdyti arba uždrausti tarpvalstybinius duomenų srautus tikrai buvo leidžiama tik tam tikrais atvejais, kai buvo nustatoma, kad duomenų perdavimas pagal sutarties sąlygas gali sukelti reikšmingus neigiamus padarinius duomenų subjektui apsaugoti skirtoms apsaugos priemonėms. Vis dėlto dabar šio sprendimo 4 straipsnyje, kurį Komisija iš dalies pakeitė 2016 m., kad jis atitiktų Sprendimą *Schrems* [53], šie įgaliojimai tiesiog nurodomi, niekaip jų neribojant. Bet kuriuo atveju priežiūros institucijoms pagal patį BDAR suteikti įgaliojimai negali būti teisėtai ribojami Komisijos įgyvendinimo sprendimu, kaip antai Sprendimu 2010/87 [54].

52 Nors Sprendimo 2010/87 4 straipsnio 1 dalyje nurodyta Direktyvos 95/46 28 straipsnio 3 dalis, primenu, kad pagal BDAR 94 straipsnio 2 dalį nuorodos į šią direktyvą turi būti laikomos nuorodomis į atitinkamas BDAR nuostatas.

53 Žr. Sprendimo 2016/2297 6 ir 7 konstatuojamąsias dalis. Sprendimo *Schrems* 101–104 punktuose Teisingumo Teismas pripažino negaliojančia sprendimo dėl „privatumo skydo“ nuostatą, kuria priežiūros institucijoms pagal Direktyvos 95/46 28 straipsnį suteikti įgaliojimai buvo apriboti iki „išimtinių atvejų“, nes Komisija neturėjo kompetencijos riboti šių įgaliojimų.

54 Žr. Sprendimą *Schrems* (103 punktas).

143. Sprendimo 2010/87 11 konstatuojamoji dalis, kurioje nurodyta, kad priežiūros institucijos gali naudotis įgaliojimais sustabdyti ir uždrausti duomenų perdavimą tik „išimtiniais atvejais“, neleidžia suabejoti šia išvada. Ši konstatuojamoji dalis, kuri jau buvo šio sprendimo pirminėje redakcijoje, buvo susijusi su ankstesne šio sprendimo 4 straipsnio 1 dalimi, pagal kurią buvo ribojami priežiūros institucijų įgaliojimai. Iš dalies keisdama Sprendimą 2010/87 Sprendimu 2016/2297, Komisija nei išbraukė šią konstatuojamąją dalį, nei ją iš dalies pakeitė, kad pritaikytų jos turinį prie nauja redakcija išdėstyto 4 straipsnio reikalavimų. Vis dėlto Sprendimo 2016/2297 5 konstatuojamojoje dalyje buvo dar kartą patvirtinti priežiūros institucijų įgaliojimai sustabdyti arba uždrausti bet kokį duomenų perdavimą, kuris, jų nuomone, prieštarauja Sąjungos teisei, be kita ko, jeigu duomenų importuotojas nesilaiko sutarčių standartinių sąlygų. Taigi Sprendimo 2010/87 11 konstatuojamoji dalis tiek, kiek dabar ji prieštarauja jo teisiškai privalomos nuostatos formuluotei ir tikslui, turi būti laikoma pasenusia [55].

144. Antra, priešingai, nei teigia ir DPC, naudojimasis BDAR 58 straipsnio 2 dalies f ir j punktuose numatytais sustabdymo ir uždraudimo įgaliojimais taip pat nėra vien teisė, palikta priežiūros institucijų nuožiūrai. Mano nuomone, tokia išvada darytina aiškinant BDAR 58 straipsnio 2 dalį atsižvelgiant į kitas šio reglamento ir Chartijos nuostatas, taip pat į bendrą Sprendimo 2010/87 struktūrą ir tikslus.

145. Visų pirma BDAR 58 straipsnio 2 dalis turi būti aiškinama atsižvelgiant į Chartijos 8 straipsnio 3 dalį ir SESV 16 straipsnio 2 dalį. Pagal šias nuostatas tai, ar laikomasi iš pagrindinės teisės į asmens duomenų apsaugą kylančių reikalavimų, kontroliuoja nepriklausomos institucijos. Ši užduotis prižiūrėti, kad būtų laikomasi reikalavimų, susijusių su asmens duomenų apsauga, taip pat paminėta BDAR 57 straipsnio 1 dalies a punkte, reiškia, kad priežiūros institucijos privalo veikti taip, kad būtų užtikrintas tinkamas šio reglamento taikymas.

146. Taigi priežiūros institucija turi labai kruopščiai išnagrinėti asmens, kurio duomenys buvo tariamai perduoti į trečiąją valstybę pažeidžiant šiam perdavimui taikytinas standartines sutarčių sąlygas, skundą [56]. Šiuo tikslu BDAR 58 straipsnio 1 dalyje priežiūros institucijoms suteikiami reikšmingi tyrimo įgaliojimai [57].

147. Kompetentinga priežiūros institucija taip pat privalo tinkamai reaguoti į galimus duomenų subjekto teisių pažeidimus, kuriuos ji konstatuoja užbaigusi tyrimą. Šiuo klausimu kiekvienai priežiūros institucijai pagal BDAR 58 straipsnio 2 dalį suteikiamas platus priemonių spektras (įvairūs įgaliojimai imtis šioje nuostatoje išvardytų taisomųjų veiksmų) jai pavestai užduočiai įvykdyti [58].

148. Nors veiksmingiausią priemonę savo nuožiūra pasirenka kompetentinga priežiūros institucija, atsižvelgdama į visas nagrinėjamo duomenų perdavimo aplinkybes, ji privalo visapusiškai įvykdyti jai pavestą priežiūros užduotį. Prireikus ši institucija turi sustabdyti duomenų perdavimą, jeigu padaro išvadą, kad nebuvo laikytasi sutarčių standartinių sąlygų ir tinkamos perduodamų duomenų apsaugos neįmanoma užtikrinti kitomis priemonėmis ir jeigu duomenų eksportuotojas pats nenutraukė duomenų perdavimo.

55 Bet kuriuo atveju Sąjungos akto preambulė neturi privalomosios teisinės galios ir ja negalima remtis siekiant nukrypti nuo šio akto nuostatų. Žr. 1998 m. lapkričio 19 d. Sprendimą *Nilsson ir kt.* (C-162/97, EU:C:1998:554, 54 punktas); 2005 m. gegužės 12 d. Sprendimą *Meta Fackler* (C-444/03, EU:C:2005:288, 25 punktas) ir 2006 m. sausio 10 d. Sprendimą *IATA ir ELFAA* (C-344/04, EU:C:2006:10, 76 punktas).

56 Pagal analogiją žr. Sprendimą *Schrems* (63 punktas).

57 Reikėtų pridurti, kad pagal Sprendimo 2010/87 priede esančios 8 sąlygos 2 dalį sutarties šalys sutinka, kad priežiūros institucijai turi būti suteikta teisė atlikti duomenų importuotojo auditą, kuriam būtų taikomos tokios pačios sąlygos kaip ir duomenų eksportuotojo auditui pagal taikytiną teisę.

58 Šiuo klausimu žr. Sprendimą *Schrems* (43 punktas).

149. Tokį aiškinimą patvirtina BDAR 58 straipsnio 4 dalis, kurioje numatyta, kad naudojimuisi priežiūros institucijoms pagal šį straipsnį suteiktais įgaliojimais taikomos atitinkamos apsaugos priemonės, apimančios teisę į veiksmingą apskundimą teismine tvarka pagal Chartijos 47 straipsnį. Be to, BDAR 78 straipsnio 1 ir 2 dalyse kiekvienam asmeniui pripažįstama teisė imtis veiksmingų teisminių teisių gynimo priemonių dėl teisiškai privalomo priežiūros institucijos sprendimo dėl šio asmens arba jeigu ši institucija neišnagrinėja šio asmens skundo [59].

150. Kaip iš esmės teigia M. Schrems, BSA, Airija, Lenkijos ir Jungtinės Karalystės vyriausybės ir Komisija, iš šių nuostatų kyla reikalavimas, kad sprendimas, kuriuo priežiūros institucija neuždraudžia arba nesustabdo duomenų perdavimo į trečiąją šalį gavusi asmens prašymą, kuriame jis nurodo, kad kyla grėsmė, jog šioje trečiojoje šalyje jo asmens duomenys bus tvarkomi pažeidžiant jo pagrindines teises, galėtų būti apskųstas teismui. Vis dėlto teisės į teisminę gynybą pripažinimas suponuoja ribotą priežiūros institucijų kompetenciją, o ne diskreciją. Be to, M. Schrems ir Komisija teisingai nurodė, jog tam, kad būtų įgyvendinta veiksmingą teisminė kontrolė, būtina, kad ginčijamą aktą parengusi institucija tinkamai jį motyvuotų [60]. Mano nuomone, ši pareiga motyvuoti apima priežiūros institucijų sprendimą pasinaudoti vienais ar kitais įgaliojimais, suteikiamais joms pagal BDAR 58 straipsnio 2 dalį.

151. Vis dėlto dar reikia atsakyti į argumentus, kuriais DPC teigia, kad net jei priežiūros institucijos privalėtų sustabdyti ar uždrausti duomenų perdavimą, kai to reikia duomenų subjekto teisėms apsaugoti, Sprendimo 2010/87 galiojimas vis tiek nebūtų užtikrintas.

152. Pirma, DPC mano, kad toks įpareigojimas neišspręstų sisteminių problemų, susijusių su tinkamų apsaugos priemonių nebuvimu tokioje trečiojoje šalyje kaip JAV. Iš tiesų priežiūros institucijų įgaliojimai gali būti įgyvendinami tik kiekvienu konkrečiu atveju, o JAV teisei būdingos spragos yra bendro ir struktūrinio pobūdžio. Kiltų pavojus, kad skirtingos priežiūros institucijos dėl panašaus duomenų perdavimo priims skirtingus sprendimus.

153. Šiuo klausimu negaliu neatsižvelgti į praktinius sunkumus, susijusius su teisės aktų leidėjo sprendimu padaryti priežiūros institucijas atsakingas už užtikrinimą, kad, esant konkrečiam duomenų perdavimui ar konkrečiam gavėjui skirtam duomenų srautui, būtų laikomasi duomenų subjektų pagrindinių teisių. Vis dėlto man atrodo, kad šie sunkumai nenulemia Sprendimo 2010/87 negaliojimo.

154. Iš tiesų man atrodo, jog Sąjungos teisėje nereikalaujama, kad visam duomenų perdavimui į konkrečią trečiąją šalį, galinčiam kelti tas pačias pagrindinių teisių pažeidimo grėsmes, būtų surastas bendras, prevencinis sprendimas.

155. Be to, rizika, kad skirtingos priežiūros institucijos laikysis nevienodo požiūrio, yra neatsiejama nuo teisės aktų leidėjo pasirinktos decentralizuotos priežiūros sistemos [61]. Taip pat, kaip pabrėžia Vokietijos vyriausybė, BDAR VII skyriuje „Bendradarbiavimas ir nuoseklumas“ nustatyti mechanizmai, skirti išvengti šios rizikos. Šio reglamento 60 straipsnyje tarpvalstybinio duomenų tvarkymo atveju numatyta atitinkamų priežiūros institucijų ir duomenų valdytojo įsisteigimo vietos priežiūros institucijos,

59 Pagal BDAR 141 konstatuojamąją dalį kiekvienas asmuo turėtų turėti teisę į veiksmingą teisminę gynybą pagal Chartijos 47 straipsnį, jeigu priežiūros institucija „nesiima veiksmų, kai tokie veiksmai yra būtini [šio asmens] teisėms apsaugoti“. Taip pat žr. BDAR 129 ir 143 konstatuojamąsias dalis.

60 Žr., be kita ko, 2011 m. liepos 28 d. Sprendimą *Samba Diouf* (C-69/10, EU:C:2011:524, 57 punktas) ir 2011 m. lapkričio 17 d. Sprendimą *Gaydarov* (C-430/10, EU:C:2011:749, 41 punktas).

61 Šiuo klausimu žr. 2018 m. birželio 5 d. Sprendimą *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, 69–73 punktai).

vadinamos „vadovaujančia priežiūros institucija“, bendradarbiavimo procedūra [62]. Jeigu jų nuomonės išsiskiria, nesutarimą turi išspręsti EDPB [63]. Pastaroji taip pat yra kompetentinga priežiūros institucijos prašymu teikti nuomones visais klausimais, kurie yra svarbūs kelioms valstybėms narėms [64].

156. Antra, DPC nurodo, kad Sprendimas 2010/87 negalioja atsižvelgiant į Chartijos 47 straipsnį, nes priežiūros institucijos gali apsaugoti duomenų subjektų teises tik ateičiai ir nepasiūlo sprendimų tiems duomenų subjektams, kurių duomenys jau yra perduoti. Visų pirma DPC pažymi, kad BDAR 58 straipsnio 2 dalyje nenumatyta nei teisė susipažinti su trečiosios šalies viešosios valdžios institucijų surinktais duomenimis, nei teisė reikalauti, kad šie duomenys būtų ištaisyti ar ištrinti, nei duomenų subjektų patirtos žalos atlyginimo galimybė.

157. Kalbant apie nurodomą teisės susipažinti su surinktais duomenimis ir teisės reikalauti juos ištaisyti ar ištrinti nebuvimą, reikia konstatuoti, kad jeigu trečiojoje paskirties šalyje nėra jokių veiksmingų teisių gynimo priemonių, Sąjungoje duomenų valdytojo atžvilgiu numatytos teisių gynimo priemonės neleidžia iš šios trečiosios šalies viešosios valdžios institucijų gauti prieigos prie šių duomenų ar reikalauti juos ištaisyti ar ištrinti.

158. Mano supratimu, šis prieštaravimas vis dėlto nesuteikia pagrindo pripažinti Sprendimo 2010/87 nesuderinamu su Chartijos 47 straipsniu. Šio sprendimo galiojimas nepriklauso nuo kiekvienoje trečiojoje šalyje, į kurią duomenys galėtų būti perduodami pagal minėtame sprendime nustatytas standartines sutarčių sąlygas, esamo apsaugos lygio. Jeigu pagal trečiosios paskirties valstybės teisę duomenų importuotojas negali laikytis šių sąlygų, reikalaujant, kad jis suteiktų viešosios valdžios institucijoms galimybę susipažinti su duomenimis, nesuteikiant atitinkamų galimybių imtis teisių gynimo priemonių, jeigu duomenų eksportuotojas nesustabdo duomenų perdavimo pagal Sprendimo 2010/87 priede esančios 5 sąlygos a arba b punktus, priežiūros institucijos turi imtis taisomųjų priemonių.

159. Be to, kaip pažymėjo M. Schrems, asmenys, kurių teisės buvo pažeistos, dabar pagal BDAR 82 straipsnį turi teisę į turtinės ar neturtinės žalos, patirtos dėl šio reglamento pažeidimo, atlyginimą ir ją turi atlyginti duomenų valdytojas arba duomenų tvarkytojas [65].

160. Taigi, kaip matyti iš viso to, kas išdėstyta, mano analizė neatskleidė jokios informacijos, kuri turėtų poveikį Sprendimo 2010/87 galiojimui atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius.

F. Dėl būtinybės atsakyti į kitus prejudicinius klausimus ir nagrinėti sprendimo dėl „privatumo skydo“ galiojimą nebuvimo

161. Šioje išvados dalyje nurodysiu priežastis, daugiausia susijusias su pagrindinės bylos dalyko apribojimu Sprendimo 2010/87 galiojimu, dėl kurių manau, kad į antrąjį–penktąjį, taip pat į devintąjį ir dešimtąjį prejudicinius klausimus atsakyti nereikia, kaip ir nuspręsti dėl sprendimo dėl „privatumo skydo“ galiojimo.

62 Žr. BDAR 56 straipsnio 1 dalį. Pagal šio reglamento 61 straipsnį priežiūros institucijos privalo viena kitai teikti pagalbą. Šio reglamento 62 straipsnyje joms leidžiama vykdyti bendras operacijas.

63 Žr. BDAR 65 straipsnį.

64 Žr. BDAR 64 straipsnio 2 dalį.

65 BDAR 83 straipsnio 5 dalies c punkte taip pat numatytos baudos, kurias turi mokėti duomenų valdytojas, jeigu yra pažeidžiami šio reglamento 44–49 straipsniai.

162. Antrasis prejudicinis klausimas susijęs su apsaugos standartų, kurių trečioji šalis turi laikytis tam, kad duomenys galėtų būti teisėtai perduoti į šią šalį remiantis standartinėmis sutarčių sąlygomis, nustatymu, jeigu šiuos duomenis po jų perdavimo nacionalinio saugumo tikslais gali tvarkyti šios trečiosios šalies valdžios institucijos. Teisingumo Teismui pateiktas trečiasis prejudicinis klausimas susijęs su trečiojoje paskirties valstybėje taikomą apsaugos sistemą apibūdinančių elementų, į kuriuos turi būti atsižvelgiama siekiant patikrinti, ar ji atitinka šiuos standartus, nustatymu.

163. Ketvirtuoju, penktuoju ir dešimtuoju prejudiciniais klausimais prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar, atsižvelgiant į jo nustatytas faktines aplinkybes, susijusias su JAV teise, joje yra numatytos atitinkamos apsaugos priemonės nuo JAV žvalgybos institucijų taikomų pagrindinės teisės į privataus gyvenimo gerbimą, asmens duomenų apsaugą ir veiksmingą teisminę gynybą įgyvendinimo ribojimų.

164. Devintasis prejudicinis klausimas susijęs su poveikiu, kurį, priežiūros institucijai tikrinant, ar remiantis Sprendime 2010/87 numatytomis standartinėmis sutarčių sąlygomis atliekamam duomenų perdavimui į JAV yra taikomos tinkamos apsaugos priemonės, turi aplinkybė, kad Komisija sprendime dėl „privatumo skydo“ konstatavo, kad JAV užtikrina tinkamą duomenų subjektų pagrindinių teisių apsaugos nuo tokių ribojimų lygį.

165. Prašymą priimti prejudicinį sprendimą pateikęs teismas aiškiai nekėlė paties sprendimo dėl „privatumo skydo“ galiojimo klausimo, nors, kaip paaiškinta toliau šioje išvadoje [66], ketvirtuoju, penktuoju ir dešimtuoju prejudiciniais klausimais netiesiogiai abejojama minėtame sprendime Komisijos konstatuoto tinkamumo pagrįstumu.

166. Mano nuomone, atsižvelgiant į tai, kas paaiškėjo man atlikus pirma šioje išvadoje išdėstytą analizę, atsakymas, kurį Teisingumo Teismas pateiktų į šiuos klausimus, negalėtų paveikti jo išvados dėl Sprendimo 2010/87 galiojimo *in abstracto*, taigi, ir turėti įtakos pagrindinės bylos baigčiai (1 dalis). Be to, nors Teisingumo Teismo atsakymai į minėtus klausimus vėliau galėtų būti naudingi DPC siekiant per pirminę procedūrą, davusią pradžią šiam ginčui, nustatyti, ar nagrinėjamas duomenų perdavimas *in concreto* turi būti sustabdytas todėl, kad galimai nėra užtikrinamos tinkamos apsaugos priemonės, manau, kad šioje byloje būtų per anksti juos nagrinėti (2 dalis).

1. Dėl to, kad Teisingumo Teismo atsakymai nėra reikalingi, atsižvelgiant į pagrindinės bylos dalyką

167. Primenu, kad pagrindinėje byloje nagrinėjamas ginčas kilo DPC pasinaudojus teisių gynimo priemone, aprašyta Sprendimo *Schrems* 65 punkte, pagal kurį kiekviena valstybė narė turi leisti priežiūros institucijai, manančiai, kad tai yra būtina jos gautam skundui išnagrinėti, prašyti nacionalinio teismo šiuo tikslu pateikti Teisingumo Teismui prejudicinį klausimą dėl sprendimo dėl tinkamumo galiojimo arba pagal analogiją – sprendimo, kuriuo nustatomos standartinės sutarčių sąlygos, galiojimo.

168. Šiuo klausimu *High Court* (Aukštasis Teismas) pažymėjo, kad po to, kai DPC kreipėsi į jį, jis turėjo tik dvi galimybes – pateikti prašymą priimti prejudicinį sprendimą dėl Sprendimo 2010/87 galiojimo, kaip prašė DPC, jeigu pritartų pastarojo abejonėms dėl šio sprendimo galiojimo, arba priešingu atveju atsisakyti patenkinti šį prašymą. Minėtas teismas laikosi nuomonės, kad, pasirinkęs antrąjį variantą, būtų turėjęs atmesti DPC ieškinį kaip netekusį dalyko [67].

66 Žr. šios išvados 175 punktą.

67 2017 m. spalio 3 d. *High Court* (Aukštasis teismas) sprendimas (337 punktas).

169. *Supreme Court* (Aukščiausiasis Teismas), gavęs *Facebook Ireland* kasacinį skundą dėl nutarties dėl prašymo priimti prejudicinį sprendimą, pagrindinę bylą apibūdino kaip procedūrą dėl pripažinimo, per kurią DPC prašymą priimti prejudicinį sprendimą pateikusio teismo prašė pateikti Teisingumo Teismui prejudicinį klausimą dėl Sprendimo 2010/87 galiojimo. Taigi, kaip nurodė Airijos Aukščiausiasis Teismas, vienintelis esminis prašymą priimti prejudicinį sprendimą pateikusiame teisme ir Teisingumo Teisme iškeltas klausimas susijęs su šio sprendimo galiojimu [68].

170. Atsižvelgdamas į taip apibrėžtą pagrindinėje byloje kilusio ginčo dalyką, prašymą priimti prejudicinį sprendimą pateikęs teismas pateikė Teisingumo Teismui dešimt pirmųjų prejudicinių klausimų, manydamas, kad juos išnagrinėjus bus galima atlikti bendrą vertinimą, kurį Teisingumo Teismas turi atlikti tam, kad, atsakydamas į vienuoliktąjį prejudicinį klausimą, nuspręstų dėl Sprendimo 2010/87 galiojimo atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius. Kaip nurodyta nutartyje dėl prašymo priimti prejudicinį sprendimą, šis klausimas logiškai išplaukia iš prieš jį einančių prejudicinių klausimų.

171. Atsižvelgiant į tai, man atrodo, kad antrasis–penktasis, taip pat devintasis ir dešimtasis prejudiciniai klausimai grindžiami prielaida, kad Sprendimo 2010/87 galiojimas priklausys nuo kiekvienoje trečiojoje valstybėje, į kurią pagal šiame sprendime numatytas standartines sutarčių sąlygas gali būti perduodami asmens duomenys, numatyto pagrindinių teisių apsaugos lygio. Vis dėlto, kaip matyti iš mano atliktos septintojo prejudicinio klausimo analizės [69], manau, kad ši prielaida yra klaidinga. Trečiosios paskirties šalies teisė turi būti nagrinėjama tik tuo atveju, jeigu Komisija priima sprendimą dėl tinkamumo arba jeigu duomenų valdytojas ar, jam nesiėmus veiksmų, kompetentinga priežiūros institucija patikrina, ar, kai duomenys perduodami taikant tinkamas apsaugos priemones, kaip tai suprantama pagal BDAR 46 straipsnio 1 dalį, įpareigojimai, kurie pagal šios trečiosios šalies teisę nustatomi duomenų importuotojui, nesusilpnina šiomis apsaugos priemonėmis užtikrinamos apsaugos veiksmingumo.

172. Taigi Teisingumo Teismo atsakymai į minėtus klausimus negali paveikti jo išvados dėl vienuoliktojo prejudicinio klausimo [70]. Atsižvelgiant į pagrindinėje byloje kilusio ginčo dalyką, į minėtą klausimą taip pat nereikia atsakyti.

173. Siūlau Teisingumo Teismui nagrinėti šią bylą atsižvelgiant tik į šio ginčo dalyką. Manau, Teisingumo Teismas neturėtų nagrinėti daugiau, nei reikalinga minėtam ginčui išspręsti, analizuodamas prejudicinius klausimus DPC pradėtos pirminės procedūros atžvilgiu. Kaip nurodyta toliau šioje išvadoje, šis siūlymas apsiriboti grindžiamas, pirma, siekiu neriboti įprastos procedūros eigos DPC po to, kai Teisingumo Teismas priims sprendimą dėl Sprendimo 2010/87 galiojimo. Antra, atsižvelgdamas į šios bylos faktines aplinkybes, manau, kad net atsižvelgiant į šios procedūros tikslą Teisingumo Teismui būtų pernelyg skubota nagrinėti antruoju–penktuoju, devintuoju ir dešimtuoju prejudiciniais klausimais keliamas problemas.

68 Kaip nurodyta 2019 m. gegužės 31 d. *Supreme Court* (Aukščiausiasis Teismas) sprendime (2.7 punktas), „[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]“). Šio sprendimo 2.9 punkte toliau nurodoma: „Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*“ (išskirta mano).

69 Žr. šios išvados 124 punktą.

70 Dėl tos pačios priežasties *Supreme Court* (Aukščiausiasis Teismas) 2019 m. gegužės 31 d. sprendime (8.1–8.5 punktai), pripažindamas, kad neturi jurisdikcijos kvestionuoti prašymą priimti prejudicinį sprendimą pateikusio teismo nutarties pateikti Teisingumo Teismui prejudicinius klausimus ir keisti jos teksto, suabejojo kai kurių iš šių klausimų reikalingumu. Šio sprendimo 8.5 punkte nurodyta: „The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures <…>“.

2. Dėl priežasčių, kodėl Teisingumo Teismas, nagrinėdamas šią bylą, neturėtų atsižvelgti į DPC vykdomos procedūros dalyką

174. DPC pateiktame skunde M. Schrems prašo šios priežiūros institucijos įgyvendinti jai pagal BDAR 58 straipsnio 2 dalies f punktą suteiktus įgaliojimus ir įpareigoti *Facebook Ireland* sustabdyti jo asmens duomenų perdavimą į JAV, atliekamą remiantis standartinėmis sutarčių sąlygomis. Grįsdamas šį reikalavimą M. Schrems iš esmės remiasi šių sutartyje numatytų apsaugos priemonių netinkamumu atsižvelgiant į jo pagrindinių teisių įgyvendinimo ribojimus, kylančius dėl JAV žvalgybos tarnybų vykdomos veiklos.

175. M. Schrems savo argumentais kvestionuoja sprendime dėl „saugaus uosto“ Komisijos padarytą išvadą, kad JAV užtikrina tinkamą pagal šį sprendimą perduodamų duomenų apsaugos lygį, atsižvelgdama į apribojimus, taikomus JAV žvalgybos institucijų galimybei susipažinti su šiais duomenimis ir jų naudojimui, taip pat į duomenų subjektams suteikiamą teisinę apsaugą [71]. DPC išreikštos negalutinės abejonės [72] ir prašymą priimti prejudicinį sprendimą pateikusio teismo ketvirtajame, penktajame ir dešimtajame prejudiciniuose klausimuose nurodytos abejonės taip pat netiesiogiai parodo abejones dėl tokios išvados pagrįstumo.

176. Žinoma, sprendime dėl „privatumo skydo“ konstatuojamas tik asmens duomenų, perduotų remiantis jame įtvirtintais principais JAV įsteigtai įmonei, kuri autosertifikavimu įsipareigojo laikytis šių principų, apsaugos lygio tinkamumas [73]. Vis dėlto jame nurodyti argumentai susiję ne vien su duomenų perdavimo, kuriam taikomas šis sprendimas, kontekstu, bet ir su šioje trečiojoje šalyje galiojančia teise ir praktika, taikoma tvarkant perduodamus duomenis nacionalinio saugumo užtikrinimo tikslais. Kaip iš esmės pažymėjo *Facebook Ireland*, M. Schrems, JAV vyriausybė ir Komisija, JAV žvalgybos institucijų vykdomas stebėjimas, taip pat priemonės, skirtos apsaugoti nuo su tuo susijusių piktnaudžiavimo pavojų, ir mechanizmai, kuriais siekiama kontroliuoti, kad šių apsaugos priemonių būtų paisoma, Sąjungos teisės požiūriu taikomi neatsižvelgiant į tai, kokiu teisiniu pagrindu remiamasi perduodant duomenis.

177. Šiuo požiūriu klausimas, ar sprendime dėl „privatumo skydo“ šiuo aspektu padarytos išvados yra privalomos priežiūros institucijoms, kai jos nagrinėja standartinėmis sutarčių sąlygomis grindžiamo duomenų perdavimo teisėtumą, gali būti reikšmingas DPC nagrinėjant M. Schrems skundą. Jeigu į šį klausimą būtų atsakyta teigiamai, kiltų klausimas, ar šis sprendimas tikrai galioja.

178. Vis dėlto nepatariu Teisingumo Teismui priimti sprendimo šiais klausimais vieninteliu tikslu padėti DPC išnagrinėti šį skundą, jeigu į juos nereikia atsakyti tam, kad prašymą priimti prejudicinį sprendimą pateikęs teismas galėtų išspręsti pagrindinėje byloje kilusį ginčą. Per SESV 267 straipsnyje numatytą procedūrą, kuria įtvirtinamas teismų dialogas, Teisingumo Teismas neturi pateikti išaiškinimo vien tam, kad padėtų administracinei institucijai per pirminę procedūrą, davusią pradžią šiam ginčui.

71 Žr. sprendimo dėl „privatumo skydo“ 64–141 konstatuojamąsias dalis. Primenu, jog iš šio sprendimo 1 straipsnio 2 dalies matyti, kad privatumo skydą sudaro ne vien principai, kurių turi laikytis įmonės, norinčios perduoti duomenis, remdamosi šiuo sprendimu, bet ir JAV vyriausybės oficialūs pareiškimai ir įsipareigojimai, išdėstyti prie šio sprendimo pridėtuose dokumentuose.

72 DPC sprendimo projektas buvo parengtas prieš priimant sprendimą dėl „privatumo skydo“. Kaip DPC patikslino šiame projekte, nors jis padarė pirminę išvadą, kad JAV teisėje numatytos apsaugos priemonės neleido užtikrinti bent duomenų perdavimo į šią trečiąją šalį atitikties Chartijos 47 straipsniui, *šiuo etapu jis nenagrinėjo naujų susitarimo dėl „privatumo skydo“ projekte numatytų taisyklių ir neatsižvelgė į jas, nes šis projektas dar nebuvo patvirtintas*. Tokiomis aplinkybėmis 2017 m. spalio 3 d. sprendimo 307 punkte *High Court* (Aukštasis teismas) nurodė: „It is fair to conclude <…> that the decision of the Commission in regard to the adequacy of the protections afforded to ES citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of ES citizens whose data are transferred from the [ES] to the [U.S.], conflicts with the case made by the DPC to this court“.

73 Žr. sprendimo dėl „privatumo skydo“ 1 straipsnio 1 ir 3 dalis ir 14–16 konstatuojamąsias dalis.

179. Manau, ši išlyga būtina dar ir todėl, kad jam nebuvo aiškiai pateiktas klausimas, kuriuo būtų siekiama išsiaiškinti, ar sprendimas dėl „privatumo skydo“ galioja, juo labiau kad Europos Sąjungos Bendrajame Teisme jau yra nagrinėjamas ieškinys dėl šio sprendimo panaikinimo [74].

180. Be to, manau, kad priimdamas sprendimą pirma nurodytais klausimais Teisingumo Teismas sutrikdytų įprastą procedūros, kuri turėtų vykti po to, kai jis priims sprendimą šioje byloje, eigą. Per šią procedūrą DCP turės išnagrinėti M. Schrems skundą, atsižvelgdamas į Teisingumo Teismo atsakymą į vienuoliktąjį prejudicinį klausimą. Jeigu Teisingumo Teismas nuspręs taip, kaip siūlau, ir priešingai, nei jame teigia DPC, t. y. kad, atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius, Sprendimas 2010/87 galioja, manau, kad DCP turėtų būti suteikta galimybė išnagrinėti jame vykdomos procedūros medžiagą iš naujo. Jeigu DPC manytų, kad negali priimti sprendimo dėl M. Schrems skundo, Teisingumo Teismui prieš tai nenustačius, ar sprendimas dėl „privatumo skydo“ neleidžia jam įgyvendinti įgaliojimų sustabdyti nagrinėjamą duomenų perdavimą, ir patvirtintų, kad abejoja šio sprendimo galiojimu, jis galėtų iš naujo kreiptis į nacionalinius teismus ir prašyti, kad jie šiuo klausimu kreiptųsi į Teisingumo Teismą [75].

181. Taip būtų pradėta procedūra, kuri leistų visoms šalims ir visiems suinteresuotiesiems asmenims, nurodytiems Teisingumo Teismo statuto 23 straipsnio antroje pastraipoje, pateikti Teisingumo Teismui pastabas būtent dėl sprendimo dėl „privatumo skydo“ galiojimo, atitinkamu atveju nurodant konkrečius vertinimus, kurie yra ginčijami, ir priežastis, dėl kurių manoma, kad Komisija viršijo jai suteiktą ribotą diskreciją [76]. Per tokią procedūrą Komisija turėtų galimybę tiksliai ir išsamiai atsakyti į visą galimą kritiką dėl minėto sprendimo. Nors šioje byloje šalys ir pastabas Teisingumo Teisme pateikę suinteresuotieji asmenys turėjo galimybę pareikšti poziciją dėl kai kurių aspektų, kurie yra reikšmingi vertinant sprendimo dėl „privatumo skydo“ atitiktį Chartijos 7, 8 ir 47 straipsniams, atsižvelgiant į šio klausimo svarbą, jį derėtų išanalizuoti išsamiai ir nuodugniai.

182. Mano nuomone, apdairumo sumetimais reikia palaukti, kol bus užbaigti šie procedūriniai etapai, kad Teisingumo Teismas galėtų nagrinėti sprendimo dėl „privatumo skydo“ poveikį priežiūros institucijos atliekamam prašymo sustabdyti duomenų perdavimą į JAV pagal BDAR 46 straipsnio 1 dalį nagrinėjimui ir priimti sprendimą dėl šio sprendimo galiojimo.

183. Tai reikėtų padaryti dar ir todėl, kad Teisingumo Teismui pateikta bylos medžiaga neleidžia daryti išvados, kad M. Schrems skundo nagrinėjimas DPC būtinai priklausys nuo atsakymo į klausimą, ar sprendimas dėl „privatumo skydo“ neleidžia priežiūros institucijoms pasinaudoti jų įgaliojimais sustabdyti standartinėmis sutarčių sąlygomis grindžiamą duomenų perdavimą.

184. Šiuo klausimu, pirma, negalima atmesti, kad DPC teks sustabdyti nagrinėjamą duomenų perdavimą dėl kitų priežasčių nei susijusios su JAV užtikrinama galimai netinkamo lygio apsauga nuo duomenų subjektų pagrindinių teisių pažeidimų dėl JAV žvalgybos tarnybų veiklos. Prašymą priimti prejudicinį sprendimą pateikęs teismas patikslino, jog M. Schrems DPC pateiktame skunde teigia, kad sutarčių sąlygos, kuriomis *Facebook Ireland* grindžia šį duomenų perdavimą, tiksliai neatitinka Sprendimo 2010/87 priede išdėstytų sąlygų. M. Schrems taip pat teigia, kad minėtas duomenų perdavimas patenka ne į šio sprendimo, bet į kitų sprendimų dėl SSS taikymo sritį [77].

74 Nagrinėjama byla *La Quadrature du Net ir kt. / Komisija* (T-738/16, OL C 6, 2017, p. 39).

75 Taip pat reikėtų pažymėti, kad savo rašytinėse pastabose DPC nepareiškė pozicijos dėl sprendimo dėl „privatumo skydo“ poveikio jam pateikto skundo nagrinėjimui.

76 Šiuo klausimu žr. Sprendimą *Schrems* (78 punktas).

77 Siekdamas pagrįsti šį teiginį, M. Schrems nurodo, kad *Facebook Inc.* reikia laikyti ne tik duomenų tvarkytoju, bet ir „duomenų valdytoju“, kaip tai suprantama pagal BDAR 4 straipsnio 7 punktą, kiek tai susiję su socialinio tinklo *Facebook* naudotojų asmens duomenų tvarkymu. Šiuo klausimu žr. 2018 m. birželio 5 d. Sprendimą *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, 30 punktas).

185. Antra, DPC ir prašymą priimti prejudicinį sprendimą pateikęs teismas pažymėjo, kad *Facebook Ireland*, siekdama pagrįsti M. Schrems skunde nurodomą duomenų perdavimą, nesirėmė sprendimu dėl „privatumo skydo“[78], ir ši bendrovė patvirtino tai per teismo posėdį. Nors *Facebook Inc.* nuo 2016 m. rugsėjo 30 d. autosertifikavo, kad laikosi privatumo skydo principų[79], *Facebook Ireland* tvirtina, kad laikosi šių principų tik tiek, kiek tai susiję su kai kurių kategorijų duomenų perdavimu, t. y. duomenų, susijusių su *Facebook Inc.* prekybos partneriais. Man atrodo, Teisingumo Teismui netikslinga spėlioti, kokių klausimų galėtų kilti šioje srityje, nagrinėjant, ar darant prielaidą, kad *Facebook Ireland* negali grįsti nagrinėjamo duomenų perdavimo Sprendimu 2010/87, šiam duomenų perdavimui vis tiek būtų taikomas sprendimas dėl „privatumo skydo“, nors ši bendrovė nepateikė šio argumento nei prašymą priimti prejudicinį sprendimą pateikusiame teisme, nei DPC.

186. Iš to darau išvadą, kad į antrąjį–penktąjį, devintąjį ir dešimtąjį prejudicinius klausimus atsakyti nereikia, kaip ir nagrinėti sprendimo dėl „privatumo skydo“ galiojimo.

G. Papildomos pastabos, susijusios su sprendimo dėl „privatumo skydo“ padariniais ir galiojimu

187. Nors, remdamasis pirma pateikta analize, siūlau Teisingumo Teismui pirmiausia nespręsti dėl sprendimo dėl „privatumo skydo“ poveikio skundo, kurį M. Schrems pateikė DPC, nagrinėjimui ir šio sprendimo galiojimui, man atrodo naudinga papildomai ir su išlygomis šiuo klausimu pateikti kelias glaustas pastabas.

1. Dėl sprendimo dėl „privatumo skydo“ poveikio, priežiūros institucijai nagrinėjant skundą dėl sutartinėmis garantijomis grindžiamo duomenų perdavimo teisėtumo

188. Devintuoju prejudiciniu klausimu siekiama išsiaiškinti, ar sprendime dėl „privatumo skydo“ padaryta išvada dėl JAV užtikrinamo apsaugos lygio tinkamumo, atsižvelgiant į galimybės JAV institucijoms susipažinti su perduodamais duomenimis ir juos naudoti nacionalinio saugumo tikslais bei į duomenų subjektų teisinės apsaugos apribojimus, neleidžia priežiūros institucijai sustabdyti duomenų perdavimo į šią trečiąją šalį, vykdomo pagal standartines sutarčių sąlygas.

189. Man atrodo, kad šį klausimą reikia suprasti atsižvelgiant į Sprendimo *Schrems* 51 ir 52 punktus, iš kurių matyti, kad sprendimas dėl tinkamumo yra privalomas priežiūros institucijoms, kol nėra pripažintas negaliojančiu. Vadinasi, priežiūros institucija, gavusi asmens, kurio duomenys perduodami į sprendime dėl tinkamumo nurodytą trečiąją šalį, skundą, negali sustabdyti duomenų perdavimo, motyvuodama tuo, kad šioje šalyje užtikrinamas apsaugos lygis nėra tinkamas, jei prieš tai Teisingumo Teismas nepripažino šio sprendimo negaliojančiu[80].

190. Prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia sužinoti, ar, kalbant apie tokį sprendimą dėl tinkamumo, koks yra sprendimas dėl „privatumo skydo“, ar prieš priimant jį – sprendimą dėl „saugaus uosto“, grindžiamą įmonių savanorišku jame įtvirtintų principų laikymusi, ši išvada tinka tik tuo atveju, jeigu toks sprendimas taikomas nagrinėjamam duomenų perdavimui į trečiąją šalį, ar ir tuo atveju, jeigu šis duomenų perdavimas turi kitokį teisinį pagrindą.

191. Kaip teigia M. Schrems, Vokietijos, Nyderlandų, Lenkijos ir Portugalijos vyriausybės, taip pat Komisija, tai, kad sprendime dėl „privatumo skydo“ konstatuojamas tinkamumas, nereiškia, kad priežiūros institucijos netenka įgaliojimų sustabdyti arba uždrausti duomenų perdavimą į JAV, vykdomą remiantis standartinėmis sutarčių sąlygomis. Jeigu duomenų perdavimas į JAV nėra grindžiamas sprendimu dėl „privatumo skydo“, formaliai šis sprendimas nėra privalomas priežiūros

78 Žr. 2017 m. spalio 3 d. *High Court* (Aukštasis teismas) sprendimą (66 punktas).

79 Žr. „privatumo skydo“ interneto svetainę (https://www.privacyshield.gov/participant_search).

80 Šiuo klausimu žr. Sprendimą *Schrems* (59 punktas).

institucijoms joms įgyvendinant pagal BDAR 58 straipsnio 2 dalį suteiktus įgaliojimus. Kitaip tariant, šios institucijos galėtų atsiriboti nuo to, ką Komisija konstatavo dėl apsaugos nuo JAV viešosios valdžios institucijų ribojimų, taikomų įgyvendinant duomenų subjektų pagrindines teises, lygio tinkamumo. Nyderlandų vyriausybė ir Komisija patikslina, kad priežiūros institucijos, naudodamosi šiais įgaliojimais, vis dėlto turi į tai atsižvelgti. Vokietijos vyriausybės nuomone, šios valdžios institucijos galėtų pateikti priešingus vertinimus tik išnagrinėjusios Komisijos padarytas išvadas iš esmės, atlikdamos reikalingus tyrimus.

192. Vis dėlto *Facebook Ireland* ir JAV vyriausybė iš esmės teigia, kad, atsižvelgiant į teisinio saugumo ir vienodo Sąjungos teisės taikymo reikalavimus, privalomoji sprendimo dėl tinkamumo galia reiškia, kad priežiūros institucijos neturi teisės kvestionuoti tokiame sprendime padarytų išvadų net ir nagrinėdamos skundą, kuriuo siekiama, kad būtų sustabdytas nagrinėjamas duomenų perdavimas į trečiąją šalį, vykdomas kitu pagrindu nei šis sprendimas.

193. Palaikau pirmąjį iš šių dviejų požiūrių. Kadangi sprendimas dėl „privatumo skydo“ taikomas tik duomenų perdavimui pagal šį sprendimą autosertifikuotai įmonei, toks sprendimas negali būti formaliai privalomas priežiūros institucijoms, kiek tai susiję su duomenų perdavimu, nepatenkančiu į šio sprendimo taikymo sritį. Sprendimu dėl „privatumo skydo“ koreliatyviai siekiama užtikrinti teisinį saugumą tik duomenų eksportuotojams, perduodantiems duomenis šiame sprendime nustatytu pagrindu. Mano nuomone, priežiūros institucijoms pagal BDAR 52 straipsnį pripažįstamas nepriklausomumas taip pat neleidžia įpareigoti jų laikytis išvadų, kurias Komisija padarė sprendime dėl tinkamumo net ne pagal jo taikymo sritį.

194. Akivaizdu, kad sprendime dėl „privatumo skydo“ padarytos išvados dėl JAV užtikrinamo apsaugos nuo ribojimų, susijusių su jų žvalgybos tarnybų veikla, lygio tinkamumo yra atspirties taškas atliekant analizę, kuria priežiūros institucija kiekvienu konkrečiu atveju vertina, ar standartinėmis sutarčių sąlygomis grindžiamas duomenų perdavimas turi būti sustabdytas dėl tokių ribojimų. Vis dėlto manau, kad jeigu kompetentinga priežiūros institucija, atlikusi išsamų tyrimą, nusprendžia, kad negali pritarti šioms išvadoms, kiek tai susiję su duomenų perdavimu, kurį jai buvo pavesta ištirti, ji išlaiko teisę pasinaudoti jai pagal BDAR 58 straipsnio 2 dalies f ir j punktus suteiktais įgaliojimais.

195. Tokiomis aplinkybėmis, jeigu Teisingumo Teismas pateiktų priešingą, nei mano siūlomas, atsakymą į ką tik išnagrinėtą klausimą, reikėtų išsiaiškinti, ar vis dėlto šių įgaliojimų nereikėtų išlaikyti, jeigu sprendimas dėl „privatumo skydo“ būtų pripažintas negaliojančiu.

2. Dėl sprendimo dėl „privatumo skydo“ galiojimo

196. Toliau nurodytomis pastabomis keliami tam tikri klausimai dėl sprendime dėl „privatumo skydo“ pateikto vertinimo pagrįstumo, kiek tai susiję su JAV užtikrinamo apsaugos lygio tinkamumu, kaip tai suprantama pagal BDAR 45 straipsnio 1 dalį, atsižvelgiant į JAV žvalgybos institucijų vykdomą elektroninių pranešimų stebėjimo veiklą. Šiomis pastabomis nesiekiama išreikšti galutinės ar išsamios pozicijos dėl šio sprendimo galiojimo. Tai tik tam tikri pamąstymai, kurie galėtų būti naudingi Teisingumo Teismui, jeigu jis, priešingai, nei siūlau, nuspręstų priimti sprendimą šiuo klausimu.

197. Šiuo klausimu iš sprendimo dėl „privatumo skydo“ 64 konstatuojamosios dalies ir II priedo I dalies 5 punkto matyti, kad įmonių pareiga laikytis šiame sprendime nurodytų privatumo principų gali būti ribojama, be kita ko, dėl reikalavimų, susijusių su nacionaliniu saugumu, viešuoju interesu ir teisės aktų laikymusi arba prieštaraujančių pareigų, susijusių su JAV teise.

198. Taigi Komisija įvertino JAV teisėje numatytas apsaugos priemones, kiek tai susiję su galimybe susipažinti su perduodamais duomenimis ir su JAV viešosios valdžios institucijų atliekamu šių duomenų naudojimu visų pirma nacionalinio saugumo tikslais [81]. Ji gavo tam tikrus JAV vyriausybės įsipareigojimus dėl, pirma, JAV valdžios institucijų galimybės susipažinti su perduodamais duomenimis ir jų naudojimo apribojimų ir, antra, duomenų subjektams suteikiamos teisinės apsaugos [82].

199. Teisingumo Teisme M. Schrems teigė, kad sprendimas dėl „privatumo skydo“ negalioja, nes pirma nurodytų apsaugos priemonių nepakanka siekiant užtikrinti asmenų, kurių duomenys perduodami į JAV, tinkamą pagrindinių teisių apsaugos lygį. DPC, EPIC, Austrijos, Lenkijos ir Portugalijos vyriausybės, tiesiogiai nekvestionuodamos šio sprendimo galiojimo, ginčija jame pateiktus Komisijos vertinimus, susijusius su apsaugos nuo ribojimų, kylančių dėl JAV žvalgybos tarnybų veiklos, lygio tinkamumu. Šios abejonės atspindi Parlamento [83], EDPB [84] ir EDAPP [85] išreikštus susirūpinimą keliančius klausimus.

200. Prieš nagrinėjant sprendime dėl „privatumo skydo“ padarytos išvados dėl tinkamumo pagrįstumą reikia patikslinti šio nagrinėjimo metodus.

a) Patikslinimai, susiję su sprendimo dėl tinkamumo galiojimo analizės turiniu

1) Dėl lyginimo sąlygų, leidžiančių įvertinti, ar apsaugos lygis yra „iš esmės toks pats“

201. Pagal BDAR 45 straipsnio 3 dalį ir Teisingumo Teismo jurisprudenciją [86] Komisija gali konstatuoti, kad trečioji šalis užtikrina tinkamo lygio apsaugą tik jeigu ji, deramai motyvavusi, nusprendžia, kad duomenų subjektų pagrindinių teisių apsaugos lygis šioje trečiojoje šalyje yra „iš esmės toks pat“ kaip ir tas, kurio reikalaujama Sąjungoje pagal šį reglamentą, aiškinamą atsižvelgiant į Chartiją.

202. Taigi siekiant patikrinti trečiojoje šalyje užtikrinamo apsaugos lygio tinkamumą, šioje trečiojoje šalyje vyraujančias taisykles ir praktiką būtinai reikia palyginti su Sąjungoje galiojančiais apsaugos standartais. Antruoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas prašo Teisingumo Teismo patikslinti šio palyginimo sąlygas [87].

81 Žr. sprendimo dėl „privatumo skydo“ 65 konstatuojamąją dalį.

82 Žr. sprendimo dėl „privatumo skydo“ III–VII priedus.

83 2017 m. balandžio 6 d. Europos Parlamento rezoliucija dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo, P8_TA(2017)0131 ir 2018 m. liepos 5 d. Europos Parlamento rezoliucija dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo, P8_TA-PROV(2018)0315.

84 Žr. 29 straipsnio duomenų apsaugos darbo grupės (toliau – 29 straipsnio darbo grupė) 2016 m. balandžio 13 d. nuomonę „Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision“, WP 238; 2017 m. lapkričio 28 d. 29 straipsnio darbo grupės nuomonę „EU-US Privacy Shield – First Annual Joint Review“, WP 255 ir 2019 m. sausio 22 d. EDPB dokumentą „EU-US Privacy Shield – Second Annual Joint Review“. 29 straipsnio darbo grupė buvo sudaryta pagal Direktyvos 95/46 29 straipsnio 1 dalį, kurioje buvo numatytas jos patariamasis vaidmuo ir nepriklausomas pobūdis. Pagal minėto straipsnio 2 dalį šią grupę sudarė kiekvienos nacionalinės priežiūros institucijos atstovas, Bendrijos institucijoms ir organams įsteigtos valdžios institucijos ar institucijų atstovas ir Komisijos atstovas. Įsigaliojus BDAR 29 straipsnio darbo grupė buvo pakeista EDPB (žr. šio reglamento 94 straipsnio 2 dalį).

85 Žr. 2016 m. gegužės 30 d. EDAPP nuomonę 4/2016 dėl JAV ir ES privatumo skydo (Privacy Shield) – sprendimo dėl tinkamumo projektas. EDAPP buvo įsteigtas 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001, p. 1; 2004 m. specialusis leidimas lietuvių k., 13 sk., 26 t., p. 102) 1 straipsnio 2 dalimi. Jis prižiūri šio reglamento nuostatų taikymą.

86 Žr. šios išvados 112 punktą.

87 Primenu, kad trečiosios valstybės užtikrinamo apsaugos lygio ir Sąjungoje reikalaujamo apsaugos lygio esminį tapatumą taip pat reikia įvertinti, jeigu esant konkrečiam duomenų perdavimui, grindžiamam Sprendime 2010/87 numatytomis standartinėmis sutarčių sąlygomis, duomenų valdytojas arba jam nesiėmus veiksmų – kompetentinga priežiūros institucija tikrina, ar trečiosios paskirties šalies valdžios institucijos taiko duomenų importuotojui reikalavimus, viršijančius tai, kas yra būtina demokratinėje visuomenėje (žr. Sprendimo 2010/87 priede esančią 5 sąlygą ir jos išnašą). Žr. šios išvados 115, 134 ir 135 punktus.

203. Kalbant konkrečiau, prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, ar ESS 4 straipsnio 2 dalyje ir BDAR 2 straipsnio 2 dalyje valstybėms narėms pripažįstama išlyga dėl kompetencijos nacionalinio saugumo užtikrinimo srityje reiškia, kad Sąjungos teisės sistemoje nėra apsaugos standartų, su kuriais, siekiant įvertinti tinkamumą, turėtų būti lyginamos apsaugos priemonės, taikomos trečiojoje šalyje viešosios valdžios institucijoms nacionalinio saugumo užtikrinimo tikslais tvarkant į šią šalį perduodamus duomenis. Jeigu atsakymas į šį klausimą yra teigiamas, minėtas teismas siekia sužinoti, kaip turi būti nustatomas pagrindas, kuriuo reikia remtis.

204. Šiuo klausimu nereikia pamiršti, kad Sąjungos teisėje tarptautiniam asmens duomenų perdavimui nustatytų apribojimų loginis pagrindas, reikalaujant, kad būtų užtikrinamas duomenų subjektų teisių apsaugos lygio tęstinumas, susijęs su siekiu išvengti Sąjungoje taikomų standartų apėjimo rizikos [88]. Kaip iš esmės teigia *Facebook Ireland*, atsižvelgiant į šį tikslą, nebūtų jokio pagrindo tikėtis, kad trečioji šalis laikysis reikalavimų, kurie neatitinka valstybėms narėms tenkančių įpareigojimų.

205. Vis dėlto pagal Chartijos 51 straipsnio 1 dalį Chartija taikoma valstybėms narėms tik tais atvejais, kai jos įgyvendina Sąjungos teisę. Taigi sprendimo dėl tinkamumo galiojimas atsižvelgiant į duomenų subjektų pagrindinių teisių įgyvendinimo apribojimus, kylančius dėl trečiosios paskirties šalies teisės aktų, priklauso nuo šių apribojimų ir apribojimų, kurie valstybėse narėse būtų leidžiami pagal Chartijos nuostatas, palyginimo *tik tiek, kiek panašūs valstybės narės teisės aktai patektų į Sąjungos teisės taikymo sritį*.

206. Vis dėlto trečiojoje paskirties šalyje užtikrinamo apsaugos lygio tinkamumas negali būti vertinamas neatsižvelgiant į galimus duomenų subjektų pagrindinių teisių įgyvendinimo ribojimus, kylančius dėl, be kita ko, nacionalinio saugumo srityje valstybės nustatytų priemonių, kurios, jeigu jas nustatytų valstybė narė, nepatektų į Sąjungos teisės taikymo sritį. Atliekant šį vertinimą, pagal BDAR 45 straipsnio 2 dalies a punktą reikalaujama be jokių apribojimų atsižvelgti į šioje trečiojoje valstybėje galiojančius teisės aktus nacionalinio saugumo srityje.

207. Mano nuomone, vertinant apsaugos lygio tinkamumą, atsižvelgiant į tokias valstybės priemones, jose numatytas garantijas reikia palyginti su Sąjungoje pagal valstybių narių teisę reikalaujamu apsaugos lygiu, įskaitant jų įsipareigojimus pagal EŽTK. Kadangi prisijungdamos prie EŽTK valstybės narės privalo suderinti savo vidaus teisę su šios konvencijos nuostatomis ir, kaip iš esmės nurodo *Facebook Ireland*, Vokietijos, Čekijos vyriausybės ir Komisija, ji valstybėms narėms yra kaip bendras vardiklis, laikyčiau šias nuostatas reikšmingu lyginamuoju veiksniu atliekant šį vertinimą.

208. Šioje byloje nagrinėjamu atveju, kaip jau minėjau šioje išvadoje [89], reikalavimai, susiję su JAV nacionaliniu saugumu, yra viršesni už autosertifikuotų įmonių įsipareigojimus pagal sprendimą dėl „privatumo skydo“. Taigi, ar šio sprendimo galiojimas priklauso nuo atsakymo į klausimą, ar šiems reikalavimams numatytos apsaugos priemonės, suteikiančios tokio lygio apsaugą, kuri yra iš esmės tokia pati kaip ir ta, kuri turi būti užtikrinama Sąjungoje?

209. Norint atsakyti į šį klausimą, iš pradžių reikia nustatyti reikalavimus, būtent grindžiamus Chartija arba EŽTK, kuriuos Sąjungoje turi atitikti elektroninių pranešimų stebėjimo srityje taikomi teisės aktai, panašūs į tuos, kuriuos Komisija nagrinėjo sprendime dėl „privatumo skydo“. Taikytinų reikalavimų nustatymas priklauso nuo to, ar tokiems teisės aktams, kaip FISA 702 straipsnis ir EO 12333, jeigu tai būtų valstybės narės teisės aktai, būtų taikomas BDAR taikymo srities apribojimas pagal šio reglamento 2 straipsnio 2 dalį, aiškinamą atsižvelgiant į ESS 4 straipsnio 2 dalį.

88 Žr. šios išvados 117 punktą.

89 Žr. šios išvados 197 punktą.

210. Šiuo klausimu iš ESS 4 straipsnio 2 dalies formuluotės ir suformuotos jurisprudencijos matyti, kad Sąjungos teisė ir, be kita ko, antrinės teisės aktai, susiję su asmens duomenų apsauga, netaikomi veiklai nacionalinio saugumo užtikrinimo srityje tiek, kiek tai yra pačios valstybės ar jos valdžios institucijų veikla, kuri nėra privačių asmenų veikla [90].

211. Šis principas reiškia, *pirma*, kad teisės aktai nacionalinio saugumo užtikrinimo srityje nepatenka į Sąjungos teisės taikymo sritį, jeigu jais reglamentuojama tik valstybės veikla, nereglamentuojant jokios privačių asmenų vykdomos veiklos. Taigi, mano nuomone, ši teisė netaikoma nacionalinėms priemonėms, susijusioms su asmens duomenų rinkimu ir naudojimu, kurias tiesiogiai įgyvendina valstybė, siekdama užtikrinti nacionalinį saugumą, nenustatant konkrečių įpareigojimų privatiems subjektams. Visų pirma, kaip Komisija teigė per teismo posėdį, valstybės narės nustatyta priemonė, pagal kurią, panašiai kaip pagal EO 12333, jos saugumo tarnyboms būtų leidžiama tiesioginė prieiga prie perduodamų duomenų, nepatektų į Sąjungos teisės taikymo sritį [91].

212. Dar sudėtingesnis yra klausimas, ar, *antra*, nacionalinės nuostatos, pagal kurias, kaip ir pagal FISA 702 straipsnį, elektroninių ryšių paslaugų teikėjai privalo teikti pagalbą nacionalinio saugumo srityje kompetentingoms valdžios institucijoms, kad jos galėtų gauti prieigą prie kai kurių asmens duomenų, taip pat nepatenka į Sąjungos teisės taikymo sritį.

213. Nors Sprendimas *PNR* leidžia manyti, kad atsakymas į šį klausimą yra teigiamas, sprendimuose *Tele2 Sverige* ir *Ministerio Fiscal* nurodyti motyvai galėtų suteikti pagrindą neigiamai atsakyti į šį klausimą.

214. Sprendime *PNR* Teisingumo Teismas panaikino sprendimą, kuriame Komisija konstatavo, kad keleivio duomenų įraše (*Passenger Name Records*, PNR) esančių asmens duomenų, perduodamų muitinių ir sienų apsaugos srityje kompetentingai JAV valdžios institucijai, apsaugos lygis yra tinkamas [92]. Teisingumo Teismas nusprendė, kad duomenų tvarkymui, dėl kurio buvo priimtas minėtas sprendimas, t. y. oro vežėjų atliekamam PNR duomenų perdavimui nagrinėjamai valdžios institucijai, *atsižvelgiant į jo tikslą*, taikoma Direktyvos 95/46 taikymo išimtis, kuri buvo numatyta jos 3 straipsnio 2 dalyje. Kaip nurodė Teisingumo Teismas, šių duomenų tvarkymas buvo būtinas ne tam, kad būtų teikiamos paslaugos, o siekiant užtikrinti visuomenės saugumą ir teisėsaugos tikslais. Kadangi nagrinėjamas duomenų perdavimas buvo priskiriamas viešosios valdžios institucijų nustatytam pagrindui, susijusiam su visuomenės saugumu, jis nepateko į šios direktyvos taikymo sritį, nepaisant to, kad PNR duomenis iš pradžių rinko privatūs ūkio subjektai, vykdydami komercinę veiklą, patenkančią į šios direktyvos taikymo sritį, ir kad jie organizavo šį duomenų perdavimą [93].

90 Žr., be kita ko, 2003 m. lapkričio 6 d. Sprendimą *Lindqvist* (C-101/01, EU:C:2003:596, 43 ir 44 punktai); Sprendimą *PNR* (58 punktas); 2008 m. gruodžio 16 d. Sprendimą *Satakunnan Markkinapörssi ir Satamedia* (C-73/07, EU:C:2008:727, 41 punktas); 2016 m. gruodžio 21 d. Sprendimą *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970, toliau – Sprendimas *Tele2 Sverige*, 69 punktas) ir 2018 m. spalio 2 d. Sprendimą *Ministerio Fiscal* (C-207/16, EU:C:2018:788, toliau – Sprendimas *Ministerio Fiscal*, 32 punktas).

91 Siekdamas išvengti bet kokios painiavos šiuo klausimu, pažymiu, kad sprendime dėl „privatumo skydo“ Komisija negalėjo nustatyti, ar JAV iš tikrųjų perima transatlantiniais kabeliais perduodamus pranešimus, nes JAV valdžios institucijos nei patvirtino, nei paneigė šį teiginį (žr. šio sprendimo 75 konstatuojamąją dalį ir jo VI priedo I punkto a papunktyje pateiktą 2016 m. vasario 22 d. Robert Litt raštą). Vis dėlto, kadangi JAV vyriausybė neneigė rinkusi perduodamus duomenis remdamasi EO 12333, manau, kad Komisija, prieš konstatuodama tinkamumą, turėjo gauti šios vyriausybės patikinimus, kad tokiam duomenų rinkimui, jeigu jis iš tikrųjų vyktų, būtų taikomos pakankamos apsaugos nuo piktnaudžiavimo pavojų priemonės. Būtent šiuo požiūriu Komisija minėto sprendimo 68–77 konstatuojamosiose dalyse nagrinėjo apribojimus ir apsaugos priemones, kurios turėtų būti taikomos tokiu atveju pagal PPD 28.

92 Kalbama apie 2004 m. gegužės 14 d. Komisijos sprendimą 2004/535/EB dėl Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnybai perduodamų oro keleivių asmens duomenų, nurodytų Keleivio duomenų įraše (*Passenger Name Record*), tinkamos apsaugos (OL L 235, 2004, p. 11).

93 Sprendimas *PNR* (56–58 punktai). Be to, 2009 m. vasario 10 d. Sprendime *Airija / Parlamentas ir Taryba* (C-301/06, EU:C:2009:68, 90 ir 91 punktai) Teisingumo Teismas konstatavo, kad Sprendime *PNR* nurodyti motyvai negali būti taikomi duomenų tvarkymui, numatytam 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvoje 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančioje Direktyvą 2002/58/EB (OL L 105, 2006, p. 54). Teisingumo Teismas šią išvadą grindė tuo, kad, skirtingai nei Sprendime *PNR* nagrinėtas sprendimas, Direktyva 2006/24 reglamentuojama tik paslaugų teikėjų veikla vidaus rinkoje ir nereglamentuojama viešosios valdžios veikla, vykdoma teisėsaugos tikslais. Atrodo, kad tokiais motyvais Teisingumo Teismas patvirtino, kad, *a contrario*, Sprendime *PNR* padaryta išvada galėjo būti taikoma nuostatoms, susijusioms su šių valdžios institucijų galimybe susipažinti su saugomais duomenimis ar juos naudoti.

215. Vėliau priimtame Sprendime *Tele2 Sverige*[94] Teisingumo Teismas konstatavo, kad Direktyvos 2002/58/EB[95] 15 straipsnio 1 dalimi grindžiamos nuostatos, reglamentuojančios telekomunikacijų paslaugų teikėjų atliekamą srauto duomenų ir vietos nustatymo duomenų saugojimą, taip pat viešosios valdžios institucijų galimybę susipažinti su duomenimis, saugomais šioje nuostatoje nurodytais tikslais, tarp kurių yra baudžiamasis persekiojimas ir nacionalinio saugumo užtikrinimas, patenka į šios direktyvos, taigi ir į Chartijos taikymo sritį. Kaip nusprendė Teisingumo Teismas, šios direktyvos 1 straipsnio 3 dalyje, kurioje nurodoma, be kita ko, valstybės veikla teisėsaugos ir nacionalinio saugumo užtikrinimo srityje, numatyta jos taikymo išimtis netaikoma nei nuostatoms, susijusioms su duomenų saugojimu, nei nuostatoms, susijusioms su galimybe susipažinti su saugomais duomenimis[96]. Teisingumo Teismas patvirtino šią jurisprudenciją Sprendime *Ministerio Fiscal*[97].

216. Vis dėlto FISA 702 straipsnis skiriasi nuo tokių teisės aktų, nes šioje nuostatoje elektroninių ryšių paslaugų teikėjams nenustatoma jokios pareigos saugoti duomenis ar kaip nors kitaip tvarkyti duomenis, nesant žvalgybos institucijų prašymo leisti susipažinti su duomenimis.

217. Taigi kyla klausimas, ar į BDAR, vadinasi, ir į Chartijos taikymo sritį, patenka nacionalinės priemonės, kuriomis šiems paslaugų teikėjams nustatoma pareiga pateikti duomenis viešosios valdžios institucijoms nacionalinio saugumo tikslais, *neatsižvelgiant į jokį saugojimo įpareigojimą*[98].

218. Laikantis *pirmojo požiūrio* galima būtų kuo labiau tarpusavyje suderinti dvi minėtas jurisprudencijos kryptis, aiškinant Teisingumo Teismo sprendimuose *Tele2 Sverige* ir *Ministerio Fiscal* padarytą išvadą dėl Sąjungos teisės taikytinumo priemonėms, kuriomis reglamentuojama nacionalinės valdžios institucijų galimybė susipažinti su duomenimis, be kita ko, nacionalinio saugumo tikslais[99], kaip taikomą tik tais atvejais, kai duomenys saugomi *vykdant teisinę prievolę*, nustatytą Direktyvos 2002/58 15 straipsnio 1 dalyje. Vis dėlto ši išvada nebūtų taikoma kitokiomis faktinėmis aplinkybėmis nei tos, kurios buvo nurodytos Sprendime *PNR*, susijusiame su oro vežėjų komerciniais tikslais jų pačių iniciatyva saugomų duomenų perdavimu vidaus saugumo srityje kompetentingai JAV institucijai.

219. Laikantis *antrojo požiūrio*, kurį palaiko Komisija ir kuris man atrodo įtikinamesnis, sprendimuose *Tele2 Sverige* ir *Ministerio Fiscal* nurodyti motyvai pateisintų Sąjungos teisės taikytinumą nacionalinėms taisyklėms, pagal kurias elektroninių ryšių paslaugų teikėjai įpareigojami teikti pagalbą valdžios institucijoms, atsakingoms už nacionalinį saugumą, kad jos galėtų gauti prieigą prie tam tikrų duomenų, *neatsižvelgiant į tai, ar šiose taisyklėse nustatyta pareiga prieš tai saugoti šiuos duomenis*.

94 Sprendimas *Tele2 Sverige* (67–81 punktai).

95 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002, p. 37; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 514).

96 Kadangi Direktyvoje 2002/58 sukonkretinami reikalavimai, numatyti Direktyvoje 95/46, dabar panaikintoje BDAR, kuriame pakartojamas beveik visas jos turinys, man atrodo, kad jurisprudencija, susijusi su Direktyvos 2002/58 1 straipsnio 3 dalies aiškinimu, pagal analogiją taikytina BDAR 2 straipsnio 2 dalies aiškinimui. Šiuo klausimu žr. Sprendimą *Tele2 Sverige* (69 punktas) ir Sprendimą *Ministerio Fiscal* (32 punktas).

97 Sprendimas *Ministerio Fiscal* (34, 35 ir 37 punktai).

98 Tas pats klausimas keliamas kituose trijuose Teisingumo Teisme dar nagrinėjamuose prašymuose priimti prejudicinį sprendimą. Žr. bylą *Privacy International* (C-623/17) (OL C 22, 2018, p. 29) ir sujungtas bylas *La Quadrature du Net ir kt.* ir *French Data Network ir kt.* (C-511/18 ir C-512/18) (OL C 392, 2018, p. 7).

99 Nors Sprendime *Tele2 Sverige* Teisingumo Teismas daugiausia dėmesio skyrė apribojimų, kylančių dėl nagrinėjamų duomenų saugojimo ir galimybės susipažinti su duomenimis priemonių atsižvelgiant į tikslą kovoti su nusikaltimais, pateisinimo nagrinėjimui, jo padaryta išvada *mutatis mutandis* taip pat taikoma, jeigu šiomis priemonėmis siekiama nacionalinio saugumo užtikrinimo tikslo. Iš tiesų Direktyvos 2002/58 15 straipsnio 1 dalyje tarp tikslų, kuriais galima pateisinti tokias priemones, minima ir kova su baudžiamosiomis veikomis, ir nacionalinio saugumo apsauga. Be to, kaip numatyta Direktyvos 2002/58 1 straipsnio 3 dalyje ir BDAR 2 straipsnio 2 dalyje, į šių teisės aktų taikymo sritį nepatenka valstybės veikla nacionalinio saugumo srityje ir baudžiamojoje srityje. Byloje, kurioje priimtas Sprendimas *Tele2 Sverige*, nagrinėtomis priemonėmis taip pat buvo siekiama tikslo, susijusio su nacionaliniu saugumu. Šio sprendimo 119 punkte Teisingumo Teismas aiškiai nagrinėjo priemonių, susijusių su srauto ir vietos nustatymo duomenų saugojimu ir galimybe susipažinti su jais, pateisinimą atsižvelgiant į nacionalinio saugumo užtikrinimo tikslą, kiek jis apima kovą su terorizmu.

220. Iš tiesų tokie motyvai grindžiami ne nagrinėjamų nuostatų tikslu, kaip Sprendime *PNR*, o tuo, kad šiomis nuostatomis reglamentuojama paslaugų teikėjų veikla, įpareigojant juos tvarkyti duomenis. Ši veikla nėra valstybės veikla srityse, nurodytose Direktyvos 2002/58 1 straipsnio 3 dalyje ir Direktyvos 95/46 3 straipsnio 2 dalyje, kurios turinys iš esmės pakartotas BDAR 2 straipsnio 2 dalyje.

221. Sprendime *Tele2 Sverige* Teisingumo Teismas pažymėjo, kad „prieig[a] prie tokių teikėjų saugomų duomenų apima asmens duomenų tvarkymą, kurį atlieka *tokie teikėjai*, t. y. tvarkymą, kuris patenka į šios direktyvos taikymo sritį“ [100]. Sprendime *Ministerio Fiscal* jis taip pat konstatavo, kad teisėkūros priemonės, kuriomis elektroninių ryšių paslaugų teikėjams nustatoma pareiga suteikti kompetentingoms nacionalinėms institucijoms prieigą prie saugomų duomenų, „neišvengiamai apima *šių teikėjų atliekamą* minėtų duomenų tvarkymą“ [101].

222. Vis dėlto duomenų valdytojo vykdomas duomenų pateikimas viešosios valdžios institucijai atitinka BDAR 4 straipsnio 2 punkte pateiktą sąvokos „duomenų tvarkymas“ apibrėžtį [102]. Tas pats pasakytina apie išankstinį duomenų filtravimą pagal paieškos kriterijus siekiant atskirti duomenis, prie kurių viešosios valdžios institucijos prašė suteikti prieigą [103].

223. Iš to darau išvadą, kad, vadovaujantis motyvais, kuriuos Teisingumo Teismas pateikė sprendimuose *Tele2 Sverige* ir *Ministerio Fiscal*, BDAR, taigi ir Chartija, taikomi nacionalinės teisės aktams, kuriais elektroninių ryšių paslaugų teikėjas įpareigojamas teikti pagalbą valdžios institucijoms, atsakingoms už nacionalinį saugumą, pateikdamas jiems duomenis, prireikus prieš tai juos išfiltravęs, net neatsižvelgiant į jokią teisės aktuose nustatytą prievolę saugoti šiuos duomenis.

224. Be to, atrodo, kad toks aiškinimas bent netiesiogiai išplaukia iš Sprendimo *Schrems*. Kaip pažymėjo DPC, Austrijos, Lenkijos vyriausybės ir Komisija, Teisingumo Teismas, nagrinėdamas sprendimo dėl „privatumo skydo“ galiojimą, jame nusprendė, kad sprendime dėl tinkamumo nurodytoje trečiosios šalies teisėje turi būti numatytos apsaugos priemonės nuo jos viešosios valdžios institucijų taikomų duomenų subjektų pagrindinių teisių ribojimų, kurios yra iš esmės tokios pat kaip ir apsaugos priemonės, kylančios, be kita ko, iš Chartijos 7, 8 ir 47 straipsnių [104].

225. Vadinasi, kalbant konkrečiau, nacionalinė priemonė, kuria elektroninių ryšių paslaugų teikėjai įpareigojami vykdyti nacionalinio saugumo srityje kompetentingų valdžios institucijų prašymą leisti susipažinti su tam tikrais šių paslaugų teikėjų vykdant komercinę veiklą saugomais duomenimis, neatsižvelgiant į jokią teisės aktuose nustatytą prievolę, prašomus pateikti duomenis iš anksto nustatant pagal selektorius (kaip pagal programą PRISM), nepatenka į BDAR 2 straipsnio 2 dalies taikymo sritį. Tas pats pasakytina apie nacionalinę priemonę, pagal kurią reikalaujama, kad įmonės, naudojančios telekomunikacijų „dorsale“, suteiktų už nacionalinį saugumą atsakingoms valdžios institucijoms prieigą prie duomenų, perduodamų per jų naudojamą infrastruktūrą (kaip pagal programą *Upstream*).

226. Vis dėlto, kai valstybės valdžios institucijos gauna nagrinėjamus duomenis, mano supratimu, jų paskesniam saugojimui ir naudojimui nacionalinio saugumo tikslais dėl tų pačių priežasčių, kurios nurodytos šios išvados 211 punkte, taikoma BDAR 2 straipsnio 2 dalyje numatyta leidžianti nukrypti nuostata, todėl jie nepatenka į šio reglamento, taigi, ir į Chartijos taikymo sritį.

100 Sprendimas *Tele2 Sverige* (78 punktas, išskirta mano). Kaip rodo žodžiai „be to“, Teisingumo Teismas šio sprendimo 79 punkte pabrėžė byloje, kurioje buvo priimtas šis sprendimas, nagrinėjamos duomenų saugojimo pareigos ir nuostatų, susijusių su nacionalinės valdžios institucijų galimybe susipažinti su saugojamais duomenimis, neatsiejamą ryšį tik siekdamas patvirtinti savo išvadą dėl Direktyvos 2002/58 taikytinumo.

101 Sprendimas *Ministerio Fiscal* (37 punktas, išskirta mano).

102 Šiuo klausimu žr. Sprendimą *Ministerio Fiscal* (38 punktas).

103 Šiuo klausimu žr. 2014 m. gegužės 13 d. Sprendimą *Google Spain ir Google* (C-131/12, EU:C:2014:317, 28 punktas).

104 Sprendimas *Schrems* (91–96 punktai). Sprendimo dėl „privatumo skydo“ 90, 124 ir 141 konstatuojamosiose dalyse Komisija taip pat nurodė Chartijos nuostatas, taip pripažindama principą, pagal kurį pagrindinių teisių ribojimai, kuriais siekiama nacionalinio saugumo užtikrinimo tikslo, turi atitikti Chartiją.

227. Atsižvelgdamas į visa tai, kas išdėstyta, laikausi nuomonės, kad sprendimo dėl „privatumo skydo“ galiojimui patikrinti, atsižvelgiant į jame įtvirtintų principų apribojimus, kurie gali būti taikomi dėl JAV žvalgybos institucijų veiklos, reikalingas dvejopas vertinimas.

228. *Pirma*, reikia patikrinti, ar JAV užtikrina iš esmės tokio pat lygio kaip numatytoji BDAR ir Chartijos nuostatose apsaugą nuo ribojimų, kylančių taikant FISA 702 straipsnį, pagal kurį NSA leidžiama įpareigoti paslaugų teikėjus pateikti jai asmens duomenis.

229. *Antra*, EŽTK nuostatos yra svarbus referencinis pagrindas vertinant, ar ribojimai, kurie gali būti taikomi įgyvendinant EO 12333, tiek, kiek pagal jį žvalgybos institucijoms leidžiama pačioms, be privačių subjektų pagalbos, rinkti asmens duomenis, leidžia abejoti JAV užtikrinamo apsaugos lygio tinkamumu. Šios nuostatos taip pat pateiktų lyginamuosius kriterijus, kurie leistų įvertinti šio apsaugos lygio tinkamumą atsižvelgiant į šių institucijų gautų duomenų saugojimą ir naudojimą nacionalinio saugumo tikslais.

230. Vis dėlto dar reikia nustatyti, ar tinkamumą patvirtinanti išvada reiškia, kad renkant duomenis pagal EO 12333 yra užtikrinama tokio lygio apsauga, kuri yra iš esmės tokia pat kaip ir apsauga, kuri turi būti užtikrinama Sąjungoje, *net jeigu duomenys būtų renkami ne JAV teritorijoje* tuo etapu, kai jie perduodami iš Sąjungos į šią trečiąją šalį.

2) Dėl būtinybės užtikrinti tinkamą duomenų apsaugos lygį duomenų perdavimo etapu

231. Teisingumo Teisme buvo palaikomos trys skirtingos pozicijos dėl to, ar Komisijai vertinant trečiojoje šalyje užtikrinamo apsaugos lygio tinkamumą būtina atsižvelgti į nacionalines priemones, susijusias su šios trečiosios šalies valdžios institucijų galimybe susipažinti su šiais duomenimis už jos teritorijos ribų tuo etapu, kai duomenys yra perduodami iš Sąjungos į šią teritoriją.

232. Pirma, *Facebook Ireland*, taip pat JAV ir Jungtinės Karalystės vyriausybės iš esmės teigia, kad tokių priemonių buvimas neturi poveikio nustatant tinkamumą. Tokį savo požiūrį jos grindžia tuo, kad trečioji valstybė negali kontroliuoti visų už jos teritorijos ribų esančių ryšio priemonių, kuriomis iš Sąjungos perduodami duomenys, taigi iš esmės niekada neįmanoma užtikrinti, kad kita trečioji valstybė slapta nerinktų duomenų, kol jie perduodami.

233. Antra, DPC, M. Schrems, EPIC, Austrijos ir Nyderlandų vyriausybės, Parlamentas ir EDPB teigia, kad pagal BDAR 44 straipsnyje įtvirtintą apsaugos lygio tęstinumo reikalavimą būtina, kad šis lygis būtų tinkamas visą laiką, kol perduodami duomenys, taip pat ir tada, kai duomenys perduodami povandeniniais kabeliais, dar prieš jiems pasiekiant trečiosios paskirties šalies teritoriją.

234. Pripažindama šį principą Komisija teigia, trečia, kad tinkamumo konstatavimo tikslas siejasi su trečiosios šalies užtikrinama apsauga *jos teritorijos viduje*, taigi aplinkybė, kad tinkamas apsaugos lygis nėra užtikrinamas *duomenų perdavimo* į šią trečiąją šalį metu, neleidžia abejoti sprendimo dėl tinkamumo galiojimu. Vis dėlto duomenų valdytojas pagal BDAR 32 straipsnį turi užtikrinti duomenų perdavimo saugumą, kuo labiau apsaugodamas asmens duomenis tuo metu, kai jie perduodami į minėtą trečiąją šalį.

235. Šiuo klausimu pažymiu, kad BDAR 44 straipsnyje reikalaujama, kad duomenų perdavimas į trečiąją šalį atitiktų šio reglamento V skyriaus nuostatas, jeigu duomenys gali būti tvarkomi „juos perdavus“. Šią frazę galima suprasti taip, kad, kaip JAV vyriausybė nurodė raštu atsakydama į Teisingumo Teismo klausimus, šių sąlygų turi būti laikomasi *nuo tada, kai duomenys pasiekia paskirties vietą*, t. y. kad jos tampa privalomos *po to, kai duomenys pradėti perduoti* (įskaitant jų perdavimo etapą).

236. Kadangi BDAR 44 straipsnio formuluotė nėra vienareikšmė, remdamasis teleologiniu aiškinimu, rinkčiausi antrąjį iš pirma pateiktų aiškinimo variantų, taigi pritarčiau antrajam iš minėtų požiūrių. Tiesą sakant, jeigu būtų manoma, kad šioje nuostatoje numatytas apsaugos lygio tęstinumo reikalavimas taikomas tik stebėjimo priemonėms, įgyvendinamoms trečiosios paskirties šalies teritorijoje, jį būtų galima apeiti, jeigu ši trečioji šalis taikytų tokias priemones už savo teritorijos ribų tuo metu, kai duomenys yra perduodami. Siekiant išvengti tokio pavojaus, trečiosios šalies užtikrinamo apsaugos lygio tinkamumo vertinimas turi apimti visas šios trečiosios šalies teisės sistemos nuostatas, be kita ko, susijusias su nacionaliniu saugumu [105], tarp jų ir tas nuostatas, kurios susijusios su jos teritorijoje įgyvendinamu stebėjimu, ir nuostatas, pagal kurias leidžiama stebėti į šią teritoriją perduodamus duomenis [106].

237. Atsižvelgiant į tai, niekas neginčija, kad, kaip pažymi EDPB, apsaugos lygio tinkamumo vertinimas, kaip matyti iš BDAR 45 straipsnio 1 dalies, apima tik trečiosios *duomenų paskirties šalies* teisės sistemos nuostatas. *Facebook Ireland*, JAV ir Jungtinės Karalystės vyriausybių nurodomas galimybės užtikrinti, kad kita trečioji valstybė slapta nerinktų šių duomenų jų perdavimo metu, nebuvimas neturi poveikio šiam vertinimui. Be to, tokio pavojaus negalima atmesti net ir po to, kai duomenys pasiekia trečiosios paskirties valstybės teritoriją.

238. Be to, tiesa yra ir tai, kad Komisija, vertindama trečiosios šalies užtikrinamos apsaugos lygio tinkamumą, galėtų tam tikrais atvejais susidurti su tuo, kad ši trečioji šalis neinformuos jos apie tam tikrų slaptų stebėjimo programų buvimą. Vis dėlto tai nereiškia, kad, *jeigu Komisijai pranešama apie tokias programas*, ji gali neatsižvelgti į jas tikrindama tinkamumą. Be to, jeigu po sprendimo dėl tinkamumo priėmimo Komisijai atskleidžiama informacija apie tai, kad egzistuoja tam tikros slaptos stebėjimo programos, kurias savo teritorijoje arba perduodant duomenis į ją įgyvendina atitinkama trečioji šalis, Komisija turi peržiūrėti savo išvadą dėl šios trečiosios šalies užtikrinamo apsaugos lygio tinkamumo, jeigu atskleidus tokią informaciją dėl šios išvados kyla abejonių [107].

3) Dėl atsižvelgimo į Komisijos ir prašymą priimti prejudicinį sprendimą pateikusio teismo konstatuotas faktines aplinkybes, susijusias su JAV teise

239. Nors neginčijama, kad Teisingumo Teismas neturi jurisdikcijos aiškinti trečiosios šalies teisės sistemoje taikomos teisės, sprendimo dėl „privatumo skydo“ galiojimas priklauso nuo to, ar pagrįsti yra Komisijos atlikti vertinimai, susiję su JAV teisėje ir praktikoje užtikrinamu asmenų, kurių duomenys perduodami į šią trečiąją šalį, pagrindinių teisių apsaugos lygiu. Iš tiesų Komisija turėjo motyvuoti savo išvadą dėl tinkamumo, atsižvelgdama į aspektus, susijusius, be kita ko, su minėtos trečiosios šalies teisės turiniu, nurodytus BDAR 45 straipsnio 2 dalyje [108].

240. 2017 m. spalio 3 d. sprendime *High Court* (Aukštasis Teismas) išsamiai apibūdino reikšmingus JAV teisės aspektus, prieš tai įvertinęs ginčo šalių pateiktus įrodymus [109]. Šis apibūdinimas iš esmės sutampa su tuo, ką Komisija sprendime dėl „privatumo skydo“ konstatavo dėl taisyklių, taikomų JAV žvalgybos institucijoms renkant duomenis ir gaunant prieigą prie jų, turinio, teisių gynimo būdų ir priežiūros mechanizmų, susijusių su šia veikla.

105 Šiuo klausimu žr. Sprendimą *Schrems* (74 ir 75 punktai).

106 Šiuo klausimu žr. 2019 m. sausio 22 d. EDPB antrąją bendrą metinę apžvalgą „JAV ir ES privatumo skydas“ (p. 17, 86 punktas).

107 Žr. BDAR 45 straipsnio 5 dalį. Taip pat žr. Sprendimą *Schrems* (76 punktas).

108 Sprendimas dėl „saugaus uosto“ buvo pripažintas negaliojančiu todėl, kad Komisija jame nekonstatavo, kad JAV savo įstatymais arba tarptautiniais įsipareigojimais iš tikrųjų užtikrina tinkamo lygio apsaugą (Sprendimo *Schrems* 97 punktas). Visų pirma Komisija nekonstatavo, kad JAV yra valstybinio pobūdžio taisyklių, skirtų nustatyti duomenų subjektų pagrindinių teisių galimų apribojimų riboms (Sprendimo *Schrems* 88 punktas), ar veiksminga teisinė apsauga nuo tokio pobūdžio apribojimų (Sprendimo *Schrems* 89 punktas).

109 Tai, ką jis konstatavo, apibendrinta šios išvados 54–73 punktuose.

241. Prašymą priimti prejudicinį sprendimą pateikęs teismas ir dauguma pastabas Teisingumo Teisme pateikusių šalių bei suinteresuotųjų asmenų abejoja teisinėmis pasekmėmis, kurias Komisija nustatė remdamasi savo konstatuotomis aplinkybėmis, t. y. išvada, kad JAV užtikrina tinkamą asmenų, kurių duomenys perduodami pagal šį sprendimą, pagrindinių teisių apsaugos lygį, ir jos pateiktu JAV teisės turinio apibūdinimu.

242. Tokiomis aplinkybėmis sprendimo dėl „privatumo skydo“ galiojimą vertinsiu daugiausia atsižvelgdamas į tai, ką pati Komisija konstatavo dėl JAV teisės turinio, nagrinėdamas, ar tai, ką ji konstatavo šiuo klausimu, pagrindė šio sprendimo dėl tinkamumo priėmimą.

243. Šiuo klausimu nepritariu DPC ir M. Schrems palaikomam požiūriui, kad *High Court* (Aukštasis Teismas) konstatuotos aplinkybės, susijusios su JAV teise, yra privalomos Teisingumo Teismui, jam nagrinėjant sprendimo dėl „privatumo skydo“ galiojimą. Minėtų šalių teigimu, kadangi pagal Airijos proceso teisę užsienio teisė yra fakto klausimas, tik prašymą priimti prejudicinį sprendimą pateikęs teismas turi jurisdikciją nustatyti jos turinį.

244. Žinoma, pagal suformuotą jurisprudenciją nacionaliniam teismui pripažįstama išimtinė jurisdikcija nustatyti bylai reikšmingas faktines aplinkybes bei aiškinti valstybės narės teisę ir taikyti ją savo nagrinėjamam ginčui [110]. Šioje jurisprudencijoje išreiškiamas funkcijų pasidalijimas tarp Teisingumo Teismo ir prašymą priimti prejudicinį sprendimą pateikusio teismo vykstant SESV 267 straipsnyje nustatytai procedūrai. Nors tik Teisingumo Teismas yra kompetentingas aiškinti Sąjungos teisę ir priimti sprendimą dėl antrinės teisės galiojimo, nacionalinis teismas, kuris turi išspręsti jame nagrinėjamą konkretų ginčą, turi nustatyti jo faktinį ir teisinį pagrindą, kad Teisingumo Teismas galėtų pateikti jam naudingą atsakymą.

245. Man atrodo, kad logika, kuria grindžiama ši prašymą priimti prejudicinį sprendimą pateikusio teismo išimtinė kompetencija, negali būti taikoma trečiosios šalies teisės nustatymui kaip aspektui, kuris gali paveikti Teisingumo Teismo išvadą dėl antrinės teisės akto galiojimo [111]. Kadangi tokio akto pripažinimas negaliojančiu Sąjungos teisės sistemoje yra privalomas *erga omnes* [112], Teisingumo Teismo išvada negali priklausyti nuo prašymo priimti prejudicinį sprendimą turinio. Vis dėlto, kaip pažymėjo *Facebook Ireland* ir JAV vyriausybė, minėta išvada priklausytų nuo to, jeigu Teisingumo Teismui būtų privalomos prašymą priimti prejudicinį sprendimą pateikusio teismo konstatuotos aplinkybės, susijusios su trečiosios valstybės teise, kurios gali skirtis, atsižvelgiant į jas konstatavusį nacionalinį teismą.

246. Atsižvelgdamas į tai, kas išdėstyta, manau, kad jeigu, siekiant atsakyti į prejudicinį klausimą dėl Sąjungos akto galiojimo, reikia įvertinti trečiosios valstybės teisės turinį, prašymą priimti prejudicinį sprendimą pateikusio teismo konstatuotos aplinkybės, susijusios su šios trečiosios valstybės teise, nėra privalomos Teisingumo Teismui, nors jis gali atsižvelgti į jas. Atitinkamu atveju Teisingumo Teismas gali jas atmesti arba papildyti, pagal rungimosi principą atsižvelgdamas į kitus šaltinius, siekdamas nustatyti aplinkybes, kurios yra būtinos nagrinėjamo akto galiojimui įvertinti [113].

110 Žr., be kita ko, 1999 m. gegužės 4 d. Sprendimą *Sürül* (C-262/96, EU:C:1999:228, 95 punktas); 2008 m. rugsėjo 11 d. Sprendimą *Eckelkamp ir kt.* (C-11/07, EU:C:2008:489, 32 punktas) ir 2016 m. spalio 26 d. Sprendimą *Senior Home* (C-195/15, EU:C:2016:804, 20 punktas).

111 Šiuo klausimu žr. 2019 m. gegužės 31 d. *Supreme Court* (Aukščiausiasis Teismas) sprendimą (6.18 punktas).

112 Žr. 1981 m. gegužės 13 d. Sprendimą *International Chemical Corporation* (66/80, EU:C:1981:102, 12 ir 13 punktai).

113 Šiuo klausimu žr. 2012 m. kovo 22 d. Sprendimą *GLS* (C-338/10, EU:C:2012:158, 15, 33 ir 34 punktai), kuriame Teisingumo Teismas, siekdamas įvertinti reglamento, kuriuo nustatomas antidempingo muitas, galiojimą, atsižvelgė į Eurostato statistinius duomenis, kuriuos Teisingumo Teismo prašymu pateikė Komisija. Taip pat žr. 1991 m. spalio 22 d. Sprendimą *Nölle* (C-16/90, EU:C:1991:402, 17, 23 ir 24 punktai). Be to, Sprendime *Schrems* (90 punktas) Teisingumo Teismas, nagrinėdamas sprendimo dėl „saugaus uosto“ galiojimą, atsižvelgė į kai kuriuos Komisijos komunikatus.

4) Dėl „esminio tapatumo“ reikalavimo taikymo srities

247. Primenu, kad sprendimo dėl „privatumo skydo“ galiojimas priklauso nuo to, ar JAV teisės sistemoje asmenims, kurių duomenys perduodami iš Sąjungos į šią trečiąją šalį, yra užtikrinamas „iš esmės toks pat“ apsaugos lygis kaip ir valstybėse narėse pagal BDAR ir Chartiją ir srityse, kurioms Sąjungos teisė netaikoma, jų įsipareigojimus pagal EŽTK.

248. Kaip Teisingumo Teismas pažymėjo Sprendime *Schrems*[114], šis reikalavimas nereiškia, kad apsaugos lygis turi būti „identiškas“ apsaugos lygiui, kurio reikalaujama Sąjungoje. Priemonės, kurių trečioji šalis ėmėsi duomenų subjektų teisėms apsaugoti, gali skirtis nuo reikalaujamųjų BDAR, aiškinamame atsižvelgiant į Chartiją, tačiau „praktiškai šios priemonės turi būti veiksmingos, kad būtų užtikrinta iš esmės tokia pati apsauga, kokia garantuojama Sąjungoje“.

249. Manau, tai taip pat rodo, kad trečiosios paskirties valstybės teisė gali turėti savo vertybių skalę ir atsižvelgiant į ją įvairių iškylančių interesų svarba gali būti vertinama skirtingai nei Sąjungos teisės sistemoje. Be to, Sąjungoje taikoma asmens duomenų apsauga yra labai aukšto lygio, palyginti su likusiame pasaulyje galiojančiu apsaugos lygiu. Taigi, mano supratimu, „iš esmės tokio pat“ apsaugos lygio kriterijus turėtų būti taikomas išlaikant tam tikrą lankstumą, kad būtų atsižvelgta į skirtingas teisines ir kultūrines tradicijas. Vis dėlto šis kriterijus reikalauja, kad trečiosios šalies teisės sistemoje egzistuotų tam tikrų minimalių garantijų ir bendrųjų iš Chartijos ir EŽTK kylančių pagrindinių teisių apsaugos reikalavimų atitikmuo, antraip būtų paneigta šio kriterijaus esmė[115].

250. Šiuo klausimu pagal Chartijos 52 straipsnio 1 dalį bet koks šios Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės ir, remiantis proporcingumo principu, būti būtinas ir tikrai atitikti Sąjungos pripažintus bendrus interesus arba reikalingas kitų teisėms ir laisvėms apsaugoti. Šie reikalavimai iš esmės atitinka nustatytuosius EŽTK 8 straipsnio 2 dalyje[116].

251. Pagal Chartijos 52 straipsnio 3 dalį tiek, kiek šios Chartijos 7, 8 ir 47 straipsniuose įtvirtintos teisės atitinka EŽTK 8 ir 13 straipsniuose garantuojamas teises, jų esmė ir taikymo sritis yra tokia, kaip nustatyta toje Konvencijoje, turint omenyje tai, kad vis dėlto Sąjungos teisėje joms gali būti numatyta didesnė apsauga. Atsižvelgiant į tai, kaip bus matyti iš šioje išvadoje pateiktos mano analizės, iš Chartijos 7, 8 ir 47 straipsnių kylantys reikalavimai, kaip juos yra išaiškinęs Teisingumo Teismas, tam tikrais aspektais yra griežtesni už kylančiuosius iš EŽTK 8 straipsnio, kaip jį yra išaiškinęs Europos Žmogaus Teisių Teismas (toliau – EŽTT).

252. Be to, reikėtų pažymėti, kad, kiekvienam iš minėtų teismų nagrinėjant juose iškeltas bylas tenka persvarstyti kai kuriuos savo atitinkamos jurisprudencijos aspektus. Taigi, pirma, neseniai priimtus du EŽTT sprendimus dėl elektroninių pranešimų stebėjimo, t. y. Sprendimą *Centrüm för Rättvisa prieš Švediją*[117] ir Sprendimą *Big Brother Watch prieš Jungtinę Karalystę*[118], buvo prašoma peržiūrėti didžiojoje kolegijoje. Antra, trys nacionaliniai teismai pateikė Teisingumo Teismui prašymus priimti prejudicinį sprendimą, sukėlusius diskusijas, ar nereikėtų keisti Teisingumo Teismo jurisprudencijos, suformuotos Sprendime *Tele2 Sverige*[119].

114 Sprendimas *Schrems* (73 ir 74 punktai).

115 Šiuo klausimu žr. 2017 m. lapkričio 28 d. 29 straipsnio darbo grupės parengtą dokumentą „Adequacy Referential (updated)“, WP 254 (p. 3, 4 ir 9).

116 Vis dėlto EŽTK 8 straipsnio 2 dalyje nevartojama teisės į privataus gyvenimo gerbimą „esmės“ sąvoka. Šiuo klausimu žr. šios išvados 161 išnašą.

117 2018 m. birželio 19 d. EŽTT sprendimas (CE:ECHR:2018:0619JUD003525208, toliau – Sprendimas *Centrüm för Rättvisa*).

118 2018 m. rugsėjo 13 d. EŽTT sprendimas (CE:ECHR:2018:0913JUD005817013, toliau – Sprendimas *Big Brother Watch*).

119 Žr. šios išvados 98 išnašoje nurodytas bylas ir bylą *Ordre des barreaux francophones et germanophones ir kt.* (C-520/18) (OL C 408, 2018, p. 39).

253. Turėdamas omenyje pirma pateiktus patikslinimus, dabar nagrinėsiu sprendimo dėl „privatumo skydo“ galiojimą, atsižvelgdamas į BDAR 45 straipsnio 1 dalį, aiškinamą atsižvelgiant į Chartiją ir EŽTK, kiek jomis užtikrinamos teisės, pirma, į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą (b dalis) ir, antra, teisė į veiksmingą teisminę gynybą (c dalis).

b) Dėl sprendimo dėl „privatumo skydo“ galiojimo atsižvelgiant į teisę į privataus gyvenimo gerbimą ir teisę į asmens duomenų apsaugą

254. Ketvirtuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės abejoja, ar JAV užtikrinamas apsaugos lygis yra iš esmės toks, koks Sąjungoje užtikrinamas duomenų subjektų pagrindinėms teisėms į privataus gyvenimo gerbimą ir asmens duomenų apsaugą.

1) Dėl ribojimų buvimo

255. Sprendimo dėl „privatumo skydo“ 67–124 konstatuojamosiose dalyse Komisija nurodo galimybę, kad JAV viešosios valdžios institucijos gaus iš Sąjungos perduodamus duomenis ir naudos juos nacionalinio saugumo tikslais įgyvendinant programas, grindžiamas visų pirma FISA 702 straipsniu arba EO 12333.

256. Įgyvendinant šias programas JAV žvalgybos tarnybos imasi ribojamųjų veiksmų, o jeigu tai būtų valstybės narės valdžios institucijų veiksmai, jie būtų laikomi Chartijos 7 straipsnyje ir EŽTK 8 straipsnyje užtikrinamos teisės į privataus gyvenimo gerbimą ribojimais. Įgyvendinant šias programas taip pat kyla pavojus, kad duomenų subjektų asmens duomenys bus tvarkomi nesilaikant Chartijos 8 straipsnyje nustatytų reikalavimų [120].

257. Iš karto patikslinu, kad teisė į privataus gyvenimo gerbimą ir teisė į asmens duomenų apsaugą apima ne tik pranešimų turinio, bet ir srauto duomenų [121] bei vietos nustatymo duomenų (toliau kartu – metaduomenys) apsaugą. Ir Teisingumo Teismas, ir EŽTT yra pripažinę, kad metaduomenys, kaip ir turinio duomenys, gali atskleisti labai tikslią informaciją apie asmens privatų gyvenimą [122].

258. Pagal Teisingumo Teismo jurisprudenciją siekiant nustatyti Chartijos 7 straipsnyje užtikrinamos teisės ribojimo buvimą nesvarbu, kad atitinkami duomenys yra arba nėra ypatingo pobūdžio ar kad dėl nagrinėjamos stebėjimo priemonės suinteresuotieji asmenys galbūt patyrė nepatogumų [123].

259. Tai priminus, FISA 702 straipsniu grindžiamos stebėjimo programos, pirma, sukelia asmenų, kurių pranešimai atitinka NSA pasirinktus selektorius, todėl elektroninių ryšių paslaugų teikėjai perduoda jai šiuos pranešimus, pagrindinių teisių ribojimus [124]. Kalbant konkrečiau, paslaugų teikėjams nustatyta pareiga *pateikti* duomenis NSA, tiek, kiek ja nukrypstama nuo ryšių konfidencialumo

120 Nors tvarkant duomenis gali būti kartu pažeisti Chartijos 7 ir 8 straipsniai, analizė, kurią reikia atlikti taikant 8 straipsnį, pagal savo struktūrą skiriasi nuo analizės, kurią reikia atlikti taikant 7 straipsnį. Kaip nurodyta Chartijos 8 straipsnio 2 dalyje, teisė į asmens duomenų apsaugą reikalauja, kad „tokie duomenys turi būti tinkamai tvarkomi ir naudojami tik konkretiems tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais“ ir kad „kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei į tai, kad jie būtų ištaisomi“. Jeigu ši teisė pažeidžiama, tai reiškia, kad asmens duomenys tvarkomi nesilaikant šių reikalavimų. Taip yra, be kita ko, tuo atveju, kai duomenys tvarkomi negavus duomenų subjekto sutikimo ir nesiremiant *jokiu kitu įstatymo numatytu teisėtu pagrindu*. Tokiu atveju, nors, kiek tai susiję su 7 straipsniu, klausimas dėl ribojimo buvimo konceptualiai skiriasi nuo klausimo dėl šio ribojimo pateisinimo, šie klausimai nesiskiria, kiek tai susiję su Chartijos 8 straipsniu.

121 Direktyvos 2002/58 2 straipsnio antros pastraipos b punkte sąvoka „srauto duomenys“ apibrėžiama kaip „duomenys, tvarkomi pranešimui perduoti elektroninių ryšių tinklu, taip pat sąskaitoms už tokį perdavimą pateikti“.

122 Žr. 2014 m. balandžio 8 d. Sprendimą *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, toliau – Sprendimas *Digital Rights Ireland*, 27 punktas) ir Sprendimą *Tele2 Sverige* (99 punktas). Taip pat žr. 1984 m. rugpjūčio 2 d. EŽTT sprendimą *Malone prieš Jungtinę Karalystę* (CE:ECHR:1984:0802JUD000869179, 84 punktas) ir 2018 m. vasario 8 d. Sprendimą *Ben Faiza prieš Prancūziją* (CE:ECHR:2018:0208JUD003144612, 66 punktas).

123 Žr. Sprendimą *Digital Rights Ireland* (33 punktas); Nuomonę 1/15 (124 punktas) ir Sprendimą *Ministerio Fiscal* (51 punktas).

124 Žr. sprendimo dėl „privatumo skydo“ 78–81 konstatuojamąsias dalis, taip pat VI priedo II punktą.

principo [125], savaime yra apribojimas, nors žvalgybos institucijos vėliau ir nesusipažįsta su šiais duomenimis ir jų nenaudoja [126]. Tai, kad šios valdžios institucijos faktiškai *saugo* joms pateiktus metaduomenis ir pranešimų turinį ir *turi galimybę susipažinti* su jais, taip pat *naudoja* šiuos duomenis, yra papildomi apribojimai [127].

260. Be to, kaip konstatavo prašymą priimti prejudicinį sprendimą pateikęs teismas [128] ir kaip nurodoma kituose šaltiniuose, pavyzdžiui, PCLOB parengtoje pagal FISA 702 straipsnį įgyvendintų programų ataskaitoje, apie kurią Teisingumo Teismą informavo JAV vyriausybė [129], įgyvendinant programą *Upstream* NSA *filtravimo tikslais jau turėjo prieigą* prie didelio kiekio („duomenų rinkiniai“) duomenų, kuriuos apėmė per telekomunikacijų „dorsale“ siunčiamų pranešimų srautas ir į kuriuos įėjo pranešimai, kuriuose nebuvo NSA nustatytų selektorių. NSA galėtų nagrinėti šiuos duomenis tik tam, kad automatizuotomis priemonėmis greitai nustatytų, ar juose yra šie selektoriai. Taigi NSA duomenų bazėse buvo saugomi tik tokiu būdu filtruojami pranešimai. Manau, tokia prieiga prie duomenų jų filtravimo tikslais taip pat yra duomenų subjektų teisės į privataus gyvenimo gerbimą įgyvendinimo ribojimas, nesvarbu, kaip saugomi duomenys naudojami vėliau [130].

261. Be to, sąvoka „duomenų tvarkymas“, kaip ji suprantama pagal BDAR 4 straipsnio 2 punktą ir Chartijos 8 straipsnio 2 dalį, apima nagrinėjamų duomenų pateikimą ir filtravimą [131], žvalgybos tarnybų prieigą prie jų, taip pat šių duomenų galimą saugojimą, analizę ir naudojimą. Vadinasi, toks duomenų tvarkymas turi atitikti šioje Chartijos nuostatoje numatytus reikalavimus [132].

262. Stebėjimas pagal EO 12333 galėtų reikšti tiesioginę žvalgybos institucijų prieigą prie perduodamų duomenų, taigi EŽTK 8 straipsnyje užtikrinamos teisės įgyvendinimo ribojimą. Prie šio ribojimo dar prisidėtų ribojimas, pasireiškiantis galimu paskesniu šių duomenų naudojimu.

2) Dėl to, ar ribojimai yra „numatyti įstatymo“

263. Pagal Teisingumo Teismo jurisprudenciją [133] ir EŽTT jurisprudenciją [134] reikalavimas, pagal kurį kiekvienas pagrindinių teisių įgyvendinimo apribojimas turi būti „numatytas įstatymo“, kaip tai suprantama pagal Chartijos 52 straipsnio 1 dalį ir EŽTK 8 straipsnio 2 dalį, reiškia ne tik tai, kad ribojimą numatanti priemonė turi turėti teisinį pagrindą vidaus teisėje, bet ir tai, kad šiam teisiniam pagrindui turi būti būdingas tam tikras prieinamumas ir nuspėjamumas, kad būtų išvengta savavališkumo pavojaus.

264. Šiuo klausimu pastabas Teisingumo Teisme pateikusios šalys ir suinteresuotieji asmenys iš esmės nesutaria dėl to, ar FISA 702 straipsnis ir EO 12333 atitinka sąlygą, susijusią su įstatymo nuspėjamumu.

125 Šiuo klausimu žr. Sprendimą *Digital Rights Ireland* (32 punktas).

126 Šiuo klausimu žr. Nuomonę 1/15 (124 ir 125 punktai), iš kurios matyti, kad duomenų perdavimas trečiajam asmeniui yra duomenų subjektų pagrindinių teisių įgyvendinimo apribojimas, nesvarbu, kaip perduota informacija bus naudojama vėliau.

127 Šiuo klausimu žr. Sprendimą *Digital Rights Ireland* (35 punktas); Sprendimą *Schrems* (87 punktas) ir Nuomonę 1/15 (123–126 punktai).

128 Žr. šios išvados 60 punktą.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2014 m. liepos 2 d. (toliau – PCLOB ataskaita, p. 84 ir 111). Taip pat žr. 2017 m. lapkričio 28 d. 29 straipsnio darbo grupės parengtą dokumentą „EU-U.S. Privacy Shield – First Annual Joint Review“, WP 255 (B.1.1, p. 15).

130 Žr. šios išvados 126 išnašą.

131 Šiuo klausimu žr. šios išvados 222 punktą.

132 Žr. Nuomonę 1/15 (123 punktas ir jame nurodyta jurisprudencija).

133 Žr., be kita ko, Nuomonę 1/15 (146 punktas).

134 Žr., be kita ko, 1984 m. rugpjūčio 2 d. EŽTT sprendimą *Malone prieš Jungtinę Karalystę* (CE:ECHR:1984:0802JUD000869179, 66 punktas); 2006 m. birželio 29 d. Sprendimą *Weber ir Saravia prieš Vokietiją* (CE:ECHR:2006:0629DEC005493400, 84 punktas ir jame nurodyta jurisprudencija, toliau – Sprendimas *Weber ir Saravia*) ir 2015 m. gruodžio 4 d. Sprendimą *Zakharov prieš Rusiją* (CE:ECHR:2015:1204JUD004714306, toliau – Sprendimas *Zakharov*, 228 punktas).

265. Pagal šią sąlygą, kaip ją yra išaiškinę Teisingumo Teismas [135] ir EŽTT [136], reikalaujama, kad teisės į privataus gyvenimo gerbimą apribojimą nustatančiame teisės akte turi būti nustatytos aiškios ir tikslios taisyklės, kuriomis būtų reglamentuojama atitinkamos priemonės apimtis ir taikymas ir nustatomi minimalūs reikalavimai, kad duomenų subjektams būtų suteikta pakankamai garantijų, leidžiančių veiksmingai apsaugoti jų asmens duomenis nuo piktnaudžiavimo pavojų ir nuo bet kokios neteisėtos prieigos prie šių duomenų ar jų neteisėto panaudojimo. Tokiose taisyklėse konkrečiai turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis viešosios valdžios institucijos gali saugoti asmens duomenis, susipažinti su jais ir juos naudoti [137]. Be to, pačiame teisiniame pagrinde, kuriame yra leidžiamas ribojimas, turi būti apibrėžta atitinkamos teisės įgyvendinimo apribojimo apimtis [138].

266. Kaip ir M. Schrems bei EPIC, abejoju, kad EO 12333 ir PPD 28, kurioje įtvirtinamos apsaugos priemonės, taikomos visai žvalgybos veiklai, susijusiai su duomenų perdavimu elektromagnetinėmis priemonėmis [139], yra pakankamai nuspėjami, kad atitiktų reikalavimą „numatytas įstatymo“.

267. Minėtuose teisės aktuose aiškiai nurodyta, kad jais duomenų subjektams nesuteikiamos teisės, kurias galima teisiškai įgyvendinti [140]. Taigi duomenų subjektai negali PPD 28 numatytomis apsaugos priemonėmis remtis teismuose [141]. Be to, Komisija sprendime dėl „privatumo skydo“ nurodė, kad nors šioje prezidento direktyvoje įtvirtintos apsaugos priemonės yra privalomos žvalgybos tarnyboms [142], jos „nėra suformuluot[os] vartojant teisinius terminus“ [143]. Be to, EO 12333 ir PPD 28 yra panašūs į vidaus administracinius nurodymus, kuriuos gali panaikinti arba iš dalies pakeisti JAV prezidentas. Vis dėlto EŽTT jau yra nusprendęs, kad vidaus administraciniai nurodymai nėra „įstatymas“ [144].

268. Kalbant apie FISA 702 straipsnį, pažymėtina, kad M. Schrems kvestionuoja šios nuostatos nuspėjamą pobūdį, motyvuodamas tuo, kad jame atrankos kriterijai, pagal kuriuos filtruojami duomenys, nėra apriboti pakankamomis apsaugos nuo piktnaudžiavimo pavojų priemonėmis. Kadangi ši problema taip pat susijusi su griežtai būtinu FISA 702 straipsnyje numatytų ribojimų pobūdžiu, nagrinėsiu ją tolesnėje šios išvados dalyje [145].

135 Žr., be kita ko, Sprendimą *Digital Rights Ireland* (54 ir 65 punktai); Sprendimą *Schrems* (91 punktas); Sprendimą *Tele2 Sverige* (109 punktas) ir Nuomonę 1/15 (141 punktas).

136 Žr., be kita ko, Sprendimą *Weber ir Saravia* (94 ir 95 punktai); Sprendimą *Zakharov* (236 punktas) ir 2016 m. sausio 12 d. Sprendimą *Szabó ir Vissy prieš Vengriją* (CE:ECHR:2016:0112JUD003713814, toliau – Sprendimas *Szabó ir Vissy*, 59 punktas).

137 Žr. Sprendimą *Tele2 Sverige* (117 punktas) ir Nuomonę 1/15 (190 punktas). Taip pat žr., be kita ko, 1984 m. rugpjūčio 2 d. EŽTT sprendimą *Malone prieš Jungtinę Karalystę* (CE:ECHR:1984:0802JUD000869179, 67 punktas); Sprendimą *Zakharov* (229 punktas) ir Sprendimą *Szabó ir Vissy* (62 punktas). EŽTT jame patikslino, kad nuspėjamumo reikalavimo taikymo sritis pranešimų perėmimo srityje nėra tokia pati kaip kitose srityse. Kalbant apie slapto stebėjimo priemones, „nuspėjamumo reikalavimas negali reikšti, kad asmeniui turėtų būti suteikiama galimybė numatyti, ar, o jei taip, tai kada valdžios institucijos gali perimti jo pranešimus, kad jis galėtų atitinkamai pritaikyti savo elgesį“.

138 Nuomonė 1/15 (139 punktas). Šiuo klausimu taip pat žr. 1983 m. kovo 25 d. EŽTT sprendimą *Silver ir kt. prieš Jungtinę Karalystę* (CE:ECHR:1983:0325JUD000594772, 88 ir 89 punktai).

139 PPD 28 išdėstyta sprendimo dėl „privatumo skydo“ 69–77 konstatuojamosiose dalyse ir jo VI priedo I punkte. Joje patikslinta, kad ši prezidento direktyva taikoma ir žvalgybos veiklai, grindžiamai FISA 702 straipsniu, ir žvalgybos veiklai, vykdomai už JAV teritorijos ribų.

140 EO 12333 3.7 punkto c papunktyje nurodyta: „[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person“. PPD 28 6 straipsnio d punkte taip pat numatyta: „This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person“.

141 Šiuo klausimu žr. 2019 m. sausio 22 d. EDPB dokumentą „EU-U.S. Privacy Shield – Second Annual Joint Review“ (99 punktas).

142 Žr. sprendimo dėl „privatumo skydo“ 69 ir 77 konstatuojamąsias dalis.

143 Sprendimo dėl „privatumo skydo“ 76 konstatuojamoji dalis.

144 Žr. 1983 m. kovo 25 d. EŽTT sprendimą *Silver ir kt. prieš Jungtinę Karalystę* (CE:ECHR:1983:0325JUD000594772, 26 ir 86 punktai).

145 Žr. šios išvados 295–301 punktus. Sprendime *Tele2 Sverige* (116 ir 117 punktai) ir Nuomonėje 1/15 (140 ir 141 punktai) įstatymo nuspėjamumo sąlyga buvo pateikiama kaip neatsiejama nuo ribojimo būtinumo ir proporcingumo sąlygos. Be to, pagal EŽTT jurisprudenciją veiksmingų apsaugos nuo piktnaudžiavimo pavojų priemonių buvimas siejamas su ribojimo „numatomumo“ sąlyga ir „būtinumo demokratinėje visuomenėje“ sąlyga ir šių abiejų sąlygų laikymasis nagrinėjamas kartu. Žr., be kita ko, 2010 m. gegužės 18 d. EŽTT sprendimą *Kennedy prieš Jungtinę Karalystę* (CE:ECHR:2010:0518JUD002683905, 155 punktas); Sprendimą *Zakharov* (236 punktas); Sprendimą *Centrüm för Rättvisa* (107 punktas) ir Sprendimą *Big Brother Watch* (322 punktas).

269. Trečiasis prejudicinis klausimas susijęs su reikalavimo „numatytas įstatymo“ laikymusi. Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar trečiojoje šalyje užtikrinamo apsaugos lygio tinkamumas turi būti nagrinėjamas atsižvelgiant tik į šioje šalyje galiojančias teisiškai privalomas taisykles ir praktiką, kuria siekiama užtikrinti jų laikymąsi, ar taip pat į šioje šalyje taikomas įvairias neprivalomas priemones ir neteisminius kontrolės mechanizmus.

270. Šiuo klausimu BDAR 45 straipsnio 2 dalies a punkte pateikiamas neišsamus sąrašas aplinkybių, į kurias Komisija turi atsižvelgti, vertindama trečiosios šalies užtikrinamos apsaugos lygio tinkamumą. Tarp šių aplinkybių yra taikytini teisės aktai ir kaip jie įgyvendinami. Šioje nuostatoje taip pat minimas kitų normų, pavyzdžiui, profesinių taisyklių ir saugumo priemonių, poveikis. Pagal šią nuostatą taip pat reikalaujama atsižvelgti į „veiksmingas ir vykdytinas duomenų subjektų teises“ ir į „veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones“ [146].

271. Manau, kad, aiškinant šią nuostatą visą ir atsižvelgiant į tai, kad joje pateiktas sąrašas nėra išsamus, ši nuostata reiškia, kad, visapusiškai vertinant nagrinėjamos trečiosios šalies užtikrinamą apsaugos lygį, gali būti atsižvelgiama į praktiką ar priemones, kurios nėra grindžiamos prieinamu ir nuspėjamu teisiniu pagrindu, siekiant patvirtinti apsaugos priemones, kurios pačios yra grindžiamos šiomis savybėmis pasižyminčiu teisiniu pagrindu. Vis dėlto, kaip iš esmės teigė DPC, M. Schrems, Austrijos vyriausybė ir EDPB, tokios priemonės ar praktika negali pakeisti minėtų apsaugos priemonių nei savaime užtikrinti reikalaujamo apsaugos lygio.

3) Dėl poveikio pagrindinių teisių esmei nebuvimo

272. Chartijos 52 straipsnio 1 dalyje įtvirtintas reikalavimas, kad bet koks šios Chartijos pripažįstamų teisių ir laisvių apribojimas neturi pakeisti jų esmės, reiškia, kad, jeigu ribojimas pažeidžia teisės ar laisvės esmę, jo negalima pateisinti jokiu teisėtu tikslu. Taigi toks ribojimas laikomas pažeidžiančiu Chartiją, nereikalaujant nagrinėti, ar jis yra tinkamas ir būtinas numatytam tikslui pasiekti.

273. Šiuo klausimu Teisingumo Teismas yra nusprendęs, kad reglamentavimas, leidžiantis valstybės institucijoms apskritai susipažinti su elektroninės komunikacijos *turiniu*, turi būti laikomas keliančiu pavojų Chartijos 7 straipsnyje garantuotos pagrindinės teisės į privatų gyvenimą esmei [147]. Vis dėlto pabrėždamas pavojus, susijusius su *galimybe susipažinti su srauto ir vietos nustatymo duomenimis* ir jų analize [148], Teisingumo Teismas nusprendė, kad šios teisės esmė nėra pakeičiama, jeigu pagal nacionalinės teisės aktus valstybės institucijoms yra leidžiama bendra prieiga prie šių duomenų [149].

274. Manau, kad šioje byloje nagrinėjamu atveju FISA 702 straipsnis negali būti laikomas suteikiančiu JAV žvalgybos institucijoms bendrą prieigą prie elektroninių pranešimų turinio.

146 Taip pat žr. BDAR 104 konstatuojamąją dalį.

147 Žr. Sprendimą *Schrems* (94 punktas). Taip pat žr. Sprendimą *Digital Rights Ireland* (39 punktas) ir Sprendimą *Tele2 Sverige* (101 punktas). Man atrodo, kad, atsižvelgiant į glaudų ryšį tarp teisės į privataus gyvenimo gerbimą ir teisės į asmens duomenų apsaugą, nacionaline priemone, kuria viešosios valdžios institucijoms suteikiama bendra prieiga prie pranešimų turinio, taip pat būtų pakeičiama Chartijos 8 straipsnyje įtvirtintos teisės esmė.

148 Žr. šios išvados 257 punktą. Sprendime *Tele2 Sverige* (99 punktas) Teisingumo Teismas pažymėjo, kad metaduomenys suteikia priemonių, be kita ko, atitinkamų asmenų profiliui nustatyti. 2014 m. balandžio 10 d. Nuomonėje Nr. 4/2014 dėl elektroninių ryšių stebėjimo žvalgybos ir nacionalinio saugumo tikslais WP 215 (p. 5) 29 straipsnio darbo grupė pažymėjo, kad dėl jų struktūrinio pobūdžio metaduomenis apibendrinti ir analizuoti lengviau nei turinio duomenis.

149 Žr. Sprendimą *Tele2 Sverige* (99 punktas). Kai kurie autoriai kėlė klausimą, ar toks bendros prieigos prie pranešimų turinio ir bendros prieigos prie metaduomenų atskyrimas yra pagrįstas, atsižvelgiant į technologijų ir ryšio priemonių raidą. Žr. Falot, N. ir Hijmans, H., „Tele2: de afweging tussen privacy en veiligheid nader omlijnd“, *Nederlands Tijdschrift voor Europees Recht*, nº 3, 2017 (p. 48) ir Ojanen, T., „Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter“ (Sprendimo *Schrems* komentaras), *European Constitutional Law Review*, 2016 (p. 5).

275. Iš tiesų, pirma, pagal FISA 702 straipsnį žvalgybos institucijų galimybė susipažinti su duomenimis galimos *jų analizės ir naudojimo tikslais* apima tik tuos duomenis, kurie atitinka atrankos kriterijus, susietus su tiksliniais asmenimis.

276. Antra, vykdant programą *Upstream* tikrai gali reikėti bendros prieigos prie elektroninių pranešimų turinio *siekiant juos filtruoti automatizuotomis priemonėmis*, jeigu selektoriai būtų naudojami ne tik „išeinantiems“ ir „įeinantiems“ pranešimams, bet visam pranešimų srauto turiniui (paieška, „susijusi su“ selektoriumi)[150]. Vis dėlto, kaip teigia Komisija, ir, priešingai, nei teigia M. Schrems ir EPIC, laikina žvalgybos tarnybų prieiga prie viso elektroninių pranešimų turinio vieninteliu tikslu – filtruoti juos pagal atrankos kriterijus – negali būti prilyginama bendrai prieigai prie šio turinio[151]. Manau, kad ribojimas, atsirandantis dėl šios laiko atžvilgiu ribotos prieigos siekiant automatizuotomis priemonėmis filtruoti pranešimus, nėra toks didelis kaip ribojimas, atsirandantis dėl viešosios valdžios institucijoms suteikiamos bendros prieigos prie šio turinio siekiant jį analizuoti ir galbūt naudoti[152]. Laikina prieiga filtravimo tikslais neleidžia šioms institucijoms saugoti atrankos kriterijų neatitinkančių metaduomenų ar pranešimų turinio ar, be kita ko, kaip pažymi JAV vyriausybė, nustatyti asmenų, kuriems šie kriterijai tikslingai netaikomi, profilius.

277. Atsižvelgiant į tai, klausimas, ar numatomų stebėti asmenų tikslingas pasirinkimas naudojant selektorius pagal FISA 702 straipsniu grindžiamas programas iš tikrųjų riboja žvalgybos institucijų įgaliojimus, priklauso nuo selektorių pasirinkimo ribų apibrėžimo[153]. M. Schrems šiuo klausimu teigia, kad, šiuo tikslu nesant pakankamos kontrolės, JAV teisėje apsaugos priemonė nuo bendros prieigos prie pranešimų turinio nenumatyta dar filtravimo etapu, taigi pakeičiama pati teisės į duomenų subjektų privataus gyvenimo gerbimą esmė.

278. Kaip išsamiau paaiškinsiu toliau[154], esu linkęs pritarti minėtoms abejonėms dėl to, ar selektorių pasirinkimo ribos yra pakankamai apibrėžtos, kad jis atitiktų ribojimų nuspėjamumo ir proporcingumo kriterijus. Vis dėlto tai, kad šios ribos yra apibrėžtos, nors ir netobulai, neleidžia daryti išvados, kad pagal FISA 702 straipsnį viešosios valdžios institucijoms yra leidžiama bendra prieiga prie elektroninių pranešimų turinio, ir tai reiškia, kad pakeičiama Chartijos 7 straipsnyje įtvirtintos teisės esmė.

279. Taip pat pažymiu, jog Nuomonėje 1/15 Teisingumo Teismas nurodė, kad Chartijos 8 straipsnyje įtvirtintos teisės į asmens duomenų apsaugą esmė nekeičiama, jeigu yra nurodyti duomenų tvarkymo tikslai ir jeigu duomenų tvarkymui taikomos taisyklės, visų pirma skirtos tokių duomenų saugumui, konfidencialumui ir vientisumui užtikrinti, taip pat jų apsaugai nuo neteisėtos prieigos ir tvarkymo[155].

150 Žr. sprendimo dėl „privatumo skydo“ 87 išnašą. Vis dėlto, kaip EPIC nurodo savo pastabose ir kaip matyti iš JAV vyriausybės raštu pateikto atsakymo į Teisingumo Teismo klausimus, 2017 m. FISC dėl pažeidimų, susijusių su šio pobūdžio paieška, pareikalavo sustabdyti paiešką, „susijusią su“ selektoriumi. Vis dėlto 2018 m. Kongresas, priimdamas įstatymą dėl FISA atnaujinimo, numatė galimybę ir vėl atlikti šio pobūdžio paieškas gavus FISC ir Kongreso pritarimą. Taip pat žr. 2019 m. sausio 22 d. EDPB dokumentą „EU-U.S. Privacy Shield – Second Annual Joint Review“ (p. 27, 55 punktas).

151 Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas savo 2017 m. spalio 3 d. sprendimo 188 ir 189 punktuose atskiria „masinę“ duomenų paiešką nuo „masinio“ duomenų gavimo, rinkimo ir saugojimo. Šis teismas iš esmės mano, kad, jeigu vykdant programą *Upstream* reikia atlikti „masinę“ duomenų paiešką iš viso per telekomunikacijų „dorsale“ perduodamų duomenų srauto, duomenų gavimas, rinkimas ir saugojimas yra tikslinis tuo požiūriu, kad gaunami, renkami ir saugojami tik tie duomenys, į kuriuos įeina nagrinėjami selektoriai.

152 Šiuo klausimu žr. 2019 m. gegužės 31 d. *Supreme Court* (Aukščiausiasis Teismas) sprendimą (11.2 ir 11.3 punktai). Juose minėtas teismas nurodo: „[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term "processing" covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis“.

153 Žr. Nuomonę 1/15 (122 punktas). Taip pat žr. 2015 m. gruodžio 15 d. Europos „demokratijos per teisę“ komisijos (Venecijos komisijos) ataskaitą dėl elektromagnetinės kilmės informacijos rinkimo tarnybų demokratinės kontrolės, tyrimas Nr. 719/2013 [CDL-AD(2015)011] (toliau – Venecijos komisijos ataskaita, p. 11): „Praktiškai atsakant į klausimą, ar šis procesas tinkamai riboja perteklinį kišimąsi į niekuo dėtus asmeninius pranešimus, reikia nustatyti, ar selektorius yra pakankamai reikšmingas ir konkretus ir ar kompiuterio algoritmas, naudojamas duomenims, kurie yra reikšmingi pagal pasirinktus parametrus, nustatyti, yra tinkamos kokybės <…>“.

154 Žr. šios išvados 297–301 punktus.

155 Nuomonė 1/15 (150 punktas).

280. Sprendime dėl „privatumo skydo“ Komisija konstatavo, kad FISA 702 straipsnyje ir PPD 28 apibrėžiami tikslai, kurių siekiant duomenys gali būti renkami vykdant programas, įgyvendinamas pagal FISA 702 straipsnį [156]. Komisija jame taip pat pažymėjo, jog PPD 28 numatytos taisyklės, kuriomis apibrėžiama prieiga prie duomenų, jų saugojimas ir sklaida siekiant užtikrinti jų saugumą ir apsaugoti nuo neteisėtos prieigos [157]. Kaip bus aišku toliau iš mano išvados [158], visų pirma abejoju, ar nagrinėjamo duomenų tvarkymo tikslai yra apibrėžti pakankamai aiškiai ir tiksliai, kad būtų užtikrinamas iš esmės toks pat apsaugos lygis kaip ir užtikrinamas Sąjungos teisės sistemoje. Vis dėlto, mano nuomone, šių galimų trūkumų nepakanka, kad būtų galima konstatuoti, kad tokiomis programomis, jeigu jos būtų diegiamos Sąjungoje, būtų pakeičiama teisės į asmens duomenų apsaugą esmė.

281. Be to, primenu, kad apsaugos, užtikrinamos vykdant stebėjimo veiklą pagal EO 12333, lygio tinkamumas turi būti vertinamas atsižvelgiant į EŽTK nuostatas. Šiuo klausimu iš sprendimo dėl „privatumo skydo“ matyti, kad apribojimai, taikomi įgyvendinant EO 12333 grindžiamas priemones, skirtas rinkti duomenims apie ne JAV asmenis, yra tik tie, kurie numatyti PPD 28 [159]. Šioje prezidento direktyvoje nurodyta, kad užsienio žvalgybos duomenys turi būti renkami „kuo tikslingiau“. Vis dėlto joje aiškiai paminėta galimybė „masiškai“ rinkti duomenis už JAV teritorijos ribų siekiant tam tikrų konkrečių nacionalinio saugumo tikslų [160]. M. Schrems nuomone, PPD 28 nuostatomis, kuriomis privatiems asmenims dar ir nesuteikiama teisių, duomenų subjektai nėra apsaugoti nuo galimos bendros prieigos prie jų elektroninių pranešimų turinio.

282. Šiuo klausimu pažymėsiu tik tiek, kad EŽTT savo jurisprudencijoje, susijusioje su EŽTK 8 straipsniu, nevartojo teisės į privataus gyvenimo gerbimą esminio turinio arba pačios esmės pakeitimo sąvokos [161]. Iki šiol jis nėra nusprendęs, kad tokios sistemos, pagal kurias leidžiama net ir masiškai perimti elektroninius pranešimus, *viršija valstybių narių diskrecijos ribas*. EŽTK laikosi pozicijos, kad tokios sistemos yra suderinamos su EŽTK 8 straipsnio 2 dalimi, jeigu joms taikomos tam tikros minimalios garantijos [162]. Tokiomis aplinkybėmis nemanau, jog galima konstatuoti, kad tokia stebėjimo sistema, kuri numatyta EO 12333, viršija valstybių narių diskrecijos ribas, nesiimant nagrinėti galimų kartu su ja taikomų apsaugos priemonių.

156 Žr. sprendimo dėl „privatumo skydo“ 70, 103 ir 109 konstatuojamąsias dalis.

157 Žr. sprendimo dėl „privatumo skydo“ 83–87 konstatuojamąsias dalis ir VI priedo I dalies c papunktį. Pažymiu, kad, kaip nurodyta PCLOB ataskaitoje (p. 51–66), NSA „minimalios informacijos“ procedūros pagal FISA 702 straipsnį daugeliu aspektų taikomos tik JAV asmenims. PPD 28 buvo siekiama taikytinas apsaugos priemones taikyti ir ne JAV asmenims. Žr. PCLOB dokumentą „Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities“, pateikiamą adresu https://www.pclob.gov/reports/report-PPD28/ (p. 2). Atsižvelgdamas į tai, manau, kad duomenų saugojimas ir naudojimas nacionalinio saugumo tikslais po to, kai juos gauna viešosios valdžios institucijos, nepatenka į Sąjungos teisės taikymo sritį (žr. šios išvados 226 punktą). Vadinasi, vykdant šią veiklą užtikrinamo apsaugos lygio tinkamumas turi būti vertinamas atsižvelgiant tik į EŽTK 8 straipsnį.

158 Žr. šios išvados 283 – 289 punktus.

159 Visų pirma Komisija sprendimo dėl „privatumo skydo“ 127 konstatuojamojoje dalyje konstatavo, kad JAV Konstitucijos Ketvirtoji pataisa netaikoma ne JAV asmenims.

160 Žr. sprendimo dėl „privatumo skydo“ 73 ir 74 konstatuojamąsias dalis ir VI priedo I dalies b punktą. Šie tikslai apima kovą su šnipinėjimu ir kitomis grėsmėmis bei užsienio valdžios veikla, nukreipta prieš JAV ir jos interesus; kovą su terorizmo grėsmėmis; kovą su grėsmėmis, kylančiomis dėl masinio naikinimo ginklo kūrimo, turėjimo, platinimo ar naudojimo; kovą su grėsmėmis, susijusiomis su kibernetiniu saugumu; kovą su grėsmėmis, kylančiomis JAV ginkluotosioms pajėgoms ar jų sąjungininkams, ir kovą su tarptautinio nusikalstamumo keliamomis grėsmėmis. Kaip nurodyta PPD 28 5 išnašoje, tikslų, kuriais grindžiamas „masiškai“ renkamų duomenų naudojimas, ribojimas netaikomas, jeigu duomenys renkami tik laikinai ir jų rinkimas yra skirtas tiksliniam duomenų rinkimui palengvinti.

161 Nors EŽTK nuostatose pagrindinių teisių „(turinio) esmė“ neminima, sąvoka, lygiavertė pagrindinės teisės „esmės“ sąvokai, vartojama EŽTT jurisprudencijoje, susijusioje su kai kuriomis EŽTK nuostatomis. Dėl EŽTK 6 straipsnyje užtikrinamos teisės į teisingą bylos nagrinėjimą esmės žr., be kita ko, 1985 m. gegužės 25 d. EŽTT sprendimą *Ashingdane prieš Jungtinę Karalystę* (CE:ECHR:1985:0528JUD000822578, 57 ir 59 punktai); 2000 m. gruodžio 21 d. Sprendimą *Heaney ir McGuinness prieš Airiją* (CE:ECHR:2000:1221JUD003472097, 55 ir 58 punktai) ir 2016 m. birželio 23 d. Sprendimą *Baka prieš Vengriją* (CE:ECHR:2016:0623JUD002026112, 121 punktas). Dėl EŽTK 12 straipsnyje įtvirtintos teisės į santuoką esmės žr. 2002 m. liepos 11 d. Sprendimą *Christine Goodwin prieš Jungtinę Karalystę* (CE:ECHR:2002:0711JUD002895795, 99 ir 101 punktai). Dėl EŽTK protokolo Nr. 1 2 straipsnyje užtikrinamos teisės į mokslą esmės žr. 1968 m. liepos 23 d. EŽTT bylą dėl kalbų vartojimo tvarkos aspektų Belgijos švietimo sistemoje (CE:ECHR:1968:0723JUD000147462, 5 punktas).

162 Visų pirma žr. Sprendimą *Centrüm för Rättvisa* (112–114 punktai ir juose nurodyta jurisprudencija) ir Sprendimą *Big Brother Watch* (337 punktas).

4) Dėl teisėto tikslo siekimo

283. Pagal Chartijos 52 straipsnio 1 dalį bet koks šios Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas turi iš tiesų atitikti Sąjungos pripažintus bendrus interesus. Chartijos 8 straipsnio 2 dalyje taip pat nurodyta, kad jeigu asmens duomenys tvarkomi negavus atitinkamo asmens sutikimo, tai turi būti daroma „įstatymo nustatytais teisėtais pagrindais“. EŽTK 8 straipsnio 2 dalyje išvardyti tikslai, kuriais galima pateisinti teisės į privataus gyvenimo gerbimą įgyvendinimo ribojimą.

284. Pagal sprendimą dėl „privatumo skydo“ jame įtvirtintų principų laikymasis gali būti ribojamas siekiant vykdyti įpareigojimus, susijusius su nacionaliniu saugumu, viešuoju interesu ir teisės aktų laikymusi [163]. Šio sprendimo 67–124 konstatuojamosiose dalyse konkrečiau nagrinėjami apribojimai, kylantys dėl JAV viešosios valdžios institucijų prieigos prie duomenų ir jų naudojimo nacionalinio saugumo tikslais.

285. Neginčijama, kad nacionalinio saugumo užtikrinimas yra teisėtas tikslas, kuriuo galima pateisinti nukrypimus nuo reikalavimų, kylančių iš BDAR [164], taip pat nuo Chartijos 7 ir 8 straipsniuose [165] ir EŽTK 8 straipsnio 2 dalyje įtvirtintų pagrindinių teisių. Vis dėlto M. Schrems, Austrijos vyriausybė ir EPIC pažymėjo, kad tikslai, kurių siekiama vykdant FISA 702 straipsniu ir EO 12333 grindžiamas stebėjimo programas, apima ne vien nacionalinį saugumą. Iš tiesų šiomis priemonėmis siekiama gauti „užsienio žvalgybos informaciją“, o ši sąvoka apima įvairių rūšių informaciją, įskaitant informaciją, susijusią su nacionaliniu saugumu, bet nebūtinai vien šią informaciją [166]. Sąvoka „užsienio žvalgybos informacija“, kaip ji suprantama pagal FISA 702 straipsnį, apima duomenis, susijusius su užsienio reikalų tvarkymu [167]. Pačiame EO 12333 ši sąvoka apibrėžiama kaip apimanti informaciją, susijusią su užsienio valdžios, užsienio organizacijų ar užsieniečių galimybėmis, ketinimais ar veikla [168]. M. Schrems kvestionuoja tokio tikslo teisėtumą, kiek jis apima ne vien nacionalinį saugumą.

286. Mano nuomone, nacionalinio saugumo sritis tam tikru mastu gali apimti interesų, susijusių su užsienio reikalų tvarkymu, apsaugą [169]. Be to, visai gali būti, kad kai kurie kiti tikslai nei nacionalinio saugumo užtikrinimas, kuriuos apima sąvoka „užsienio žvalgybos informacija“, kaip ji apibrėžta FISA 702 straipsnyje ir EO 12333, atitinka svarbius bendrojo intereso tikslus, galinčius pateisinti pagrindinių teisių į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą ribojimą. Bet kuriuo atveju, derinant duomenų subjektų pagrindines teises ir ribojimais siekiamą tikslą tarpusavyje, šie tikslai būtų mažiau svarbūs nei nacionalinio saugumo užtikrinimas [170].

163 Žr. šios išvados 197 punktą.

164 Žr. BDAR 23 straipsnio 1 dalies a punktą.

165 Žr. Sprendimą *Schrems* (88 punktas). Teisingumo Teismas artimą sąvoką „visuomenės saugumas“, kaip ji suprantama pagal SESV nuostatas, kuriomis leidžiama nukrypti nuo joje užtikrinamų pagrindinių laisvių, aiškino kaip savarankišką Sąjungos teisės sąvoką, apimančią valstybių narių vidaus ir išorės saugumą (be kita ko, žr. 1999 m. spalio 26 d. Sprendimą *Sirdar* (C-273/97, EU:C:1999:523, 17 punktas) ir 2016 m. rugsėjo 13 d. Sprendimą *CS* (C-304/14, EU:C:2016:674, 39 punktas ir jame nurodyta jurisprudencija). Vidaus saugumas gali būti paveiktas, pavyzdžiui, dėl tiesioginio pavojaus atitinkamos valstybės narės gyventojų rimčiai ir fiziniam saugumui, o išorės saugumas gali būti paveiktas, pavyzdžiui, dėl didelio neigiamo poveikio šios valstybės narės išoriniams santykiams ar taikiam tautų sugyvenimui rizikos. Negalėdama vienašališkai nustatyti šių sąvokų turinio, kiekviena valstybė narė turi tam tikrą diskreciją apibrėžti jos saugumui svarbiausius interesus. Visų pirma žr. 2018 m. gegužės 2 d. Sprendimą *K. ir H. F.* (*Teisė gyventi šalyje ir kaltinimai karo nusikaltimais*) (C-331/16 ir C-366/16, EU:C:2018:296, 40–42 punktai ir juose nurodyta jurisprudencija). Manau, šiuos motyvus galima pritaikyti aiškinant sąvoką „nacionalinis saugumas“ kaip interesą, kurio apsauga gali pateisinti BDAR nuostatų ir Chartijos 7 ir 8 straipsniuose užtikrinamų teisių ribojimus.

166 Šiuo klausimu žr. sprendimo dėl „privatumo skydo“ 89 konstatuojamąją dalį ir 97 išnašą.

167 Žr. šios išvados 55 punktą.

168 Žr. šios išvados 61 punktą.

169 Sprendime *Centrüm för Rättvisa* (111 punktas) EŽTT konstatavo, kad stebėjimo veikla, kuria siekiama palaikyti Švedijos užsienio politiką, gynybos politiką ir saugumo politiką ir nustatyti išorės grėsmes Švedijai, siekiama teisėtų tikslų, susijusių su nacionaliniu saugumu.

170 Šiuo klausimu žr. Sprendimą *Tele2 Sverige* (115 punktas) ir Sprendimą *Ministerio Fiscal* (55 punktas). Teisingumo Teismas juose pažymėjo apribojimo rimtumo ir intereso, kuriuo remiamasi siekiant pateisinti ribojimą, tarpusavio ryšį.

287. Vis dėlto laikantis Chartijos 52 straipsnio 1 dalies dar reikalaujama, kad nacionalinio saugumo ar kurio kito teisėto tikslo būtų faktiškai siekiama priemonėmis, kuriomis būtų numatyti nagrinėjami ribojimai [171]. Be to, ribojimų tikslai turi būti apibrėžti taip, kad atitiktų aiškumo ir tikslumo reikalavimus [172].

288. Vis dėlto, kaip teigia M. Schrems, FISA 702 straipsnyje ir EO 12333 numatytų stebėjimo priemonių tikslas nėra nurodytas taip tiksliai, kad atitiktų nuspėjamumo ir proporcingumo garantijas. Taip visų pirma yra todėl, kad šiuose teisės aktuose sąvoka „užsienio žvalgybos informacija“ apibrėžta labai plačiai. Be to, Komisija sprendimo dėl „privatumo skydo“ 109 konstatuojamojoje dalyje nustatė, kad FISA 702 straipsnyje reikalaujama, kad informacijos rinkimas užsienio žvalgybos srityje yra „svarbus [duomenų rinkimo] tikslas“, taigi iš pirmo žvilgsnio ir, kaip pažymėjo EPIC, atrodo, kad ši formuluotė gali apimti kitų neapibrėžtų tikslų siekimą.

289. Dėl šių priežasčių, neatmetant, kad pagal FISA 702 straipsnį arba EO 12333 numatytos stebėjimo priemonės atitinka teisėtus tikslus, galima kelti klausimą, ar jos yra apibrėžtos pakankamai aiškiai ir tiksliai, kad užkirstų kelią piktnaudžiavimo pavojams ir kad būtų galima tikrinti dėl šių priemonių kylančių apribojimų proporcingumą [173].

5) Dėl ribojimų būtinumo ir proporcingumo

290. Teisingumo Teismas yra ne kartą pažymėjęs, kad Chartijos 7 ir 8 straipsniuose įtvirtintos teisės nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų visuomeninę paskirtį ir derėti su kitomis pagrindinėmis teisėmis, remiantis proporcingumo principu [174]. Kaip pažymėjo *Facebook Ireland*, tarp šių kitų teisių yra Chartijos 6 straipsnyje užtikrinama teisė į saugumą.

291. Šiuo klausimu taip pat pagal suformuotą jurisprudenciją turi būti griežtai tikrinamas kiekvieno Chartijos 7 ir 8 straipsniuose užtikrinamų pagrindinių teisių įgyvendinimo ribojimo proporcingumas [175].

292. Visų pirma pagal Sprendimą *Schrems* „nėra ribojamas tuo, kas yra griežtai būtina, toks reglamentavimas, kuris apskritai leidžia saugoti visų asmenų <…> 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“ [176].

171 29 straipsnio darbo grupė savo 2014 m. gruodžio 5 d. darbiniame dokumente dėl elektroninių pranešimų stebėjimo žvalgybos ir nacionalinio saugumo tikslais WP 228 (p. 27) pažymėjo, kad svarbu kritiškai įvertinti, ar stebėjimas tikrai vykdomas nacionalinio saugumo tikslais.

172 Žr. Nuomonę 1/15 (181 punktas), kurioje Teisingumo Teismas konstatavo, kad teisės aktų nuostatų, kuriose numatyti apribojimai, formuluotės neatitiktų aiškumo ir tikslumo reikalavimų, jeigu nebūtų ribojama tik tiek, kiek tai yra griežtai būtina. Tuo pačiu klausimu generalinis advokatas Y. Bot savo išvadoje, pateiktoje byloje *Schrems* (C-362/14, EU:C:2015:627, 181–184 punktai), laikėsi nuomonės, kad stebėjimo priemonių tikslai buvo suformuluoti pernelyg bendrai, kad būtų laikomi bendrojo intereso tikslais, išskyrus, kiek jie susiję su nacionaliniu saugumu.

173 Panašių abejonių yra išreiškęs EDAPP savo 2016 m. gegužės 30 d. Nuomonėje 4/2016 dėl sprendimo dėl ES ir JAV „privatumo skydo“ (*Privacy Shield*) tinkamumo projekto (p. 8).

174 Žr. 2010 m. lapkričio 9 d. Sprendimą *Volker und Markus Schecke ir Eifert* (C-92/09 ir C-93/09, EU:C:2010:662, 48 punktas); Nuomonę 1/15 (136 punktas) ir 2019 m. rugsėjo 24 d. Sprendimą *Google* (*Teisės reikalauti pašalinti nuorodą teritorinė taikymo sritis*) (C-507/17, EU:C:2019:772, 60 punktas).

175 Žr., be kita ko, 2008 m. gruodžio 16 d. Sprendimą *Satakunnan Markkinapörssi ir Satamedia* (C-73/07, EU:C:2008:727, 56 punktas); Sprendimą *Digital Rights Ireland* (48 ir 52 punktai); Sprendimą *Schrems* (78 ir 92 punktai) ir Nuomonę 1/15 (139 ir 140 punktai). Taip pat žr. sprendimo dėl „privatumo skydo“ 140 konstatuojamąją dalį.

176 Sprendimas *Schrems* (93 punktas). Taip pat šiuo klausimu žr. Sprendimą *Digital Rights Ireland* (60 punktas).

293. Teisingumo Teismas taip pat yra nusprendęs, kad, išskyrus tinkamai pagrįstus skubos atvejus, prieiga turi būti siejama su išankstine kontrole, kurią atliktų teismas arba nepriklausomas administracinis subjektas, kurio sprendimu prieiga prie duomenų ir jų naudojimas yra galimas tik tiek, kiek tai yra griežtai būtina numatytam tikslui pasiekti [177].

294. Dabar BDAR 23 straipsnio 2 dalyje nustatytos įvairios apsaugos priemonės, kurias valstybė narė turi numatyti, jeigu nukrypsta nuo šio reglamento nuostatų. Teisės aktuose, kuriuose leidžiama tokia išimtis, turi būti nuostatos, susijusios, be kita ko, su duomenų tvarkymo tikslais, išimties apimtimi, apsaugos priemonėmis, kurios neleistų piktnaudžiauti, duomenų saugojimo trukme ir duomenų subjektų teise būti informuotais apie išimčių taikymą, nebent būtų pakenkta išimtimi siekiamam tikslui.

295. Šioje byloje nagrinėjamu atveju M. Schrems teigia, kad taikant FISA 702 straipsnį nėra numatytos pakankamos apsaugos priemonės nuo piktnaudžiavimo pavojų ir neteisėtos prieigos prie duomenų. Visų pirma atrankos kriterijų pasirinkimas nėra pakankamai apibrėžtas, taigi šia nuostata nesuteikiamos garantijos, apsaugančios nuo bendros prieigos prie pranešimų turinio.

296. JAV vyriausybė ir Komisija teigia priešingai, t. y. kad FISA 702 straipsnyje selektorių pasirinkimas apribojamas objektyviais kriterijais, nes šioje nuostatoje leidžiama rinkti tik ne JAV asmenų, esančių už JAV teritorijos ribų, elektroninių pranešimų duomenis siekiant gauti informaciją užsienio žvalgybos srityje.

297. Mano nuomone, kyla abejonių, ar šie kriterijai yra pakankamai aiškūs ir tikslūs, ir ar yra pakankamos apsaugos priemonės, kurios leistų išvengti piktnaudžiavimo pavojų.

298. Visų pirma sprendimo dėl „privatumo skydo“ 109 konstatuojamojoje dalyje nurodyta, kad selektorių prieš pradedant juos taikyti atskirai netvirtina nei FISC, nei jokia kita nepriklausoma teisminė ar administracinė institucija. Komisija jame konstatavo, kad „FISC neleidžia taikyti individualių stebėjimo priemonių; tiesą sakant, jis suteikia leidimus įgyvendinti stebėjimo programas <…> remdamasis metiniais pažymėjimais“, ir JAV vyriausybė tai patvirtino Teisingumo Teisme. Šioje konstatuojamojoje dalyje patikslinta, kad „pažymėjimuose, kuriuos tvirtins FISC, nėra informacijos apie individualius asmenis, kurie bus sekami, vietoj to nustatomos užsienio žvalgybos informacijos kategorijos“. Komisija joje taip pat konstatuoja, kad „nors FISC, atsižvelgdamas į pagrįstą tikimybę arba kitą standartą, nevertina, ar asmenys tinkamai sekami siekiant gauti užsienio žvalgybos informacijos, vykdydamas kontrolę jis vadovaujasi sąlyga, kad „svarbus sekimo tikslas – gauti užsienio žvalgybos informacijos“.

299. Be to, kaip nurodyta minėtoje konstatuojamojoje dalyje, pagal FISA 702 straipsnį NSA leidžiama rinkti pranešimus „tik jeigu galima pagrįstai manyti, kad atitinkamos ryšio priemonės naudojamos užsienio žvalgybos informacijai perduoti“. Sprendimo dėl „privatumo skydo“ 70 konstatuojamojoje dalyje priduriama, kad selektoriai pasirenkami vadovaujantis bendra nacionaline žvalgybos prioritetų sistema (*National Intelligence Priorities Framework*, NIPF). Šiame sprendime nenurodomi konkretesni reikalavimai dėl selektorių pasirinkimo motyvų ar pateisinimo atsižvelgiant į šiuos NSA privalomus administracinius prioritetus [178].

177 Žr. Sprendimą *Tele2 Sverige* (120 punktas) ir Nuomonę 1/15 (202 punktas).

178 PCLOB ataskaitoje (p. 45) nurodyta: „With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to “identify” the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst’s rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification“.

300. Galiausiai sprendimo dėl „privatumo skydo“ 71 konstatuojamojoje dalyje nurodomas PPD 28 numatytas reikalavimas, pagal kurį užsienio žvalgybos informacijos rinkimas turi būti „kuo [tikslingesnis]“. Šia prezidento direktyva ne tik nesuteikiamos teisės asmenims, bet ir, mano nuomone, tikrai nėra akivaizdu, kad „kuo [tikslingesnės]“ veiklos kriterijus ir „griežto būtinumo“ kriterijus, kuris pagal Chartijos 52 straipsnio 1 dalį yra privalomas siekiant pateisinti jos 7 ir 8 straipsniuose užtikrinamų teisių įgyvendinimo ribojimą, yra iš esmės tokie patys [179].

301. Atsižvelgiant į šiuos argumentus, neaišku, ar, remiantis sprendime dėl „privatumo skydo“ nurodyta informacija, FISA 702 straipsniu grindžiamos stebėjimo priemonės taikomos kartu su apsaugos priemonėmis, kuriomis ribojama, kokiems asmenims gali būti taikoma stebėjimo priemonė ir kokiais tikslais duomenys gali būti renkami, ir kurios iš esmės yra tokios pačios kaip tos, kurių reikalaujama pagal BDAR, aiškinamą atsižvelgiant į Chartijos 7 ir 8 straipsnius [180].

302. Be to, kalbant apie apsaugos lygio, siejamo su stebėjimu pagal EO 12333, tinkamumo vertinimą, pažymėtina, kad EŽTT pripažįsta valstybėms narėms plačią diskreciją pasirinkti priemones, skirtas užtikrinti savo nacionaliniam saugumui, bet vis dėlto šią diskreciją riboja reikalavimas numatyti tinkamas ir pakankamas apsaugos nuo piktnaudžiavimo priemones [181]. Savo jurisprudencijoje, susijusioje su slapto stebėjimo priemonėmis, EŽTT tikrina, ar vidaus teisėje, kuria grindžiamos šios priemonės, yra numatytos pakankamos ir veiksmingos garantijos ir apsaugos priemonės, kurios yra tinkamos „nuspėjamumo“ ir „būtinumo demokratinėje visuomenėje“ reikalavimams įvykdyti [182].

303. EŽTT šiuo klausimu yra nurodęs tam tikras minimalias garantijas. Šios garantijos susijusios su pažeidimų, dėl kurių gali būti duodamas leidimas perimti duomenis, pobūdžio aiškiu nurodymu, asmenų, kurių pranešimai gali būti perimami, kategorijų apibrėžimu, priemonės vykdymo trukmės nustatymu, procedūra, kuria turi būti vadovaujamasi nagrinėjant, naudojant ir saugant surinktus duomenis, atsargumo priemonėmis, kurių turi būti imamasi pateikiant duomenis kitiems asmenims, ir aplinkybėmis, kuriomis surinkti duomenys gali arba turi būti ištrinami ar sunaikinami [183].

304. Kartu su ribojimu taikomų apsaugos priemonių tinkamumas ir veiksmingumas priklauso nuo visų atvejo aplinkybių, įskaitant priemonių pobūdį, apimtį ir trukmę, priežastis, dėl kurių jas reikia nurodyti taikyti, institucijas, kompetentingas leisti taikyti, vykdyti ir kontroliuoti šias priemones, ir vidaus teisėje suteikiamas teisių gynimo priemones [184].

179 Šiuo klausimu žr. 2016 m. balandžio 13 d. 29 straipsnio darbo grupės Nuomonę 1/2016 dėl „ES-U.S. Privacy Shield draft adequacy decision“, WP 238 (3.3.1 skirsnis, p. 38); 2017 m. balandžio 6 d. Europos Parlamento rezoliuciją dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo, P8_TA(2017)0131 (17 punktas), taip pat 2017 m. vasario 20 d. Europos Parlamento pranešimą „Didelių duomenų kiekių poveikis pagrindinėms teisėms: privatumas, duomenų apsauga, nediskriminavimas, saugumas ir teisėsauga“, A8-0044/2017 (17 punktas).

180 Šiuo klausimu žr. 2017 m. lapkričio 28 d. 29 straipsnio darbo grupės dokumentą „EU-U.S. Privacy Shield – First Annual Joint Review“, WP 255 (p. 3); 2018 m. liepos 5 d. Europos Parlamento rezoliuciją dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo, P8 _TA(2018)0315 (22 punktas) ir EDPB dokumentą „EU-U.S. Privacy Shield – Second Annual Joint Review“, 2019 m. sausio 22 d. (81–83 ir 87 punktai).

181 Žr., be kita ko, Sprendimą *Zakharov* (232 punktas) ir Sprendimą *Szabó ir Vissy* (57 punktas).

182 Žr., be kita ko, Sprendimą *Zakharov* (237 punktas); Sprendimą *Centrüm för Rättvisa* (111 punktas) ir Sprendimą *Big Brother Watch* (322 punktas).

183 Žr., be kita ko, Sprendimą *Weber ir Saravia* (95 punktas); 2007 m. birželio 28 d. EŽTT sprendimą *Europos integracijos ir žmogaus teisių asociacija ir Ekimdjiev prieš Bulgariją* (CE:ECHR:2007:0628JUD006254000, 76 punktas) ir Sprendimą *Zakharov* (231 punktas).

184 Žr., be kita ko, Sprendimą *Weber ir Saravia* (106 punktas); Sprendimą *Zakharov* (232 punktas) ir Sprendimą *Centrüm för Rättvisa* (104 punktas).

305. Pavyzdžiui, siekdamas įvertinti slapto stebėjimo priemonės pateisinimą EŽTT atsižvelgia į visas kontrolės priemones, taikomas „kai šią priemonę nurodoma taikyti“, „kol ji taikoma“, ir „po to, kai jos taikymas nutraukiamas“ [185]. Kalbant apie pirmąjį iš šių trijų etapų, EŽTT reikalauja, kad leidimą taikyti tokią priemonę suteiktų nepriklausoma institucija. Nors, EŽTT teigimu, teismų valdžia suteikia geriausias proceso nepriklausomumo, nešališkumo ir teisėtumo garantijas, nagrinėjama institucija nebūtinai turi priklausyti teismų sistemai [186]. Nuodugni teisminė kontrolė paskesniu etapu gali ištaisyti galimus leidimo suteikimo procedūros trūkumus [187].

306. Šioje byloje nagrinėjamu atveju iš sprendimo dėl „privatumo skydo“ matyti, kad vienintelės apsaugos priemonės, kuriomis ribojamas duomenų rinkimas ir naudojimas už JAV teritorijos ribų, yra numatytos PPD 28, nes FISA 702 straipsnis netaikomas už JAV teritorijos ribų. Nesu įsitikinęs, ar šių apsaugos priemonių gali pakakti siekiant įvykdyti „nuspėjamumo“ ir „būtinumo demokratinėje visuomenėje“ reikalavimus.

307. Jau minėjau, kad pagal minėtą prezidento direktyvą privatiems asmenims nesuteikiama jokių teisių. Taip pat abejoju, ar reikalavimas užtikrinti „kuo tikslingesnį“ stebėjimą yra suformuluotas pakankamai aiškiai ir tiksliai, kad duomenų subjektai būtų tinkamai apsaugoti nuo piktnaudžiavimo pavojų [188]. Galiausiai sprendime dėl „privatumo skydo“ nenurodyta, kad EO 12333 grindžiamam stebėjimui būtų taikoma išankstinė nepriklausomos institucijos kontrolė ar kad jam galėtų būti taikoma teisminė kontrolė *a posteriori* [189].

308. Tokiomis aplinkybėmis man kyla klausimas, ar pagrįsta yra išvada, kad JAV, jų žvalgybos tarnyboms vykdant veiklą pagal FISA 702 straipsnį ir EO 12333, užtikrina tinkamo lygio apsaugą, kaip tai suprantama pagal BDAR 45 straipsnio 1 dalį, aiškinamą atsižvelgiant į Chartijos 7 ir 8 straipsnius ir EŽTK 8 straipsnį.

c) Dėl sprendimo dėl „privatumo skydo“ galiojimo atsižvelgiant į teisę į veiksmingą teisinę gynybą

309. Penktuoju prejudiciniu klausimu Teisingumo Teismo prašoma nustatyti, ar asmenims, kurių duomenys perduodami į JAV, ten taikoma teisminė apsauga iš esmės prilygsta teisminei apsaugai, kuri turi būti užtikrinama Sąjungoje pagal Chartijos 47 straipsnį. Dešimtuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia sužinoti, ar į penktąjį klausimą reikia atsakyti teigiamai, atsižvelgiant į ombudsmeno institucijos nustatymą sprendimu dėl „privatumo skydo“.

310. Pirmiausia reikia konstatuoti, kad sprendimo dėl „privatumo skydo“ 115 konstatuojamojoje dalyje Komisija pripažįsta, kad JAV teisės sistemoje yra asmenų teisminės apsaugos spragų.

311. Kaip nurodyta šioje konstatuojamojoje dalyje, pirma, „bent jau kai kurie teisiniai pagrindai, kuriuos JAV žvalgybos institucijos gali naudoti (pvz., EO 12333), nėra taikomi“ galimybei pasinaudoti teisminėmis teisių gynimo priemonėmis. Tiesą sakant, EO 12333 ir PPD 28 duomenų subjektams nesuteikiamos teisės ir jie negali remtis šiais teisės aktais teismuose. Vis dėlto pagal veiksmingos teisminės gynybos reikalavimą būtina, kad privatūs asmenys turėtų bent teises, kuriomis jie galėtų remtis teismuose.

185 Žr., be kita ko, 1978 m. rugsėjo 6 d. Sprendimą *Klass ir kt. prieš Vokietiją* (CE:ECHR:1978:0906JUD000502971, 55 punktas); Sprendimą *Zakharov* (233 punktas) ir Sprendimą *Centrüm för Rättvisa* (105 punktas).

186 Žr., be kita ko, Sprendimą *Klass* (56 punktas); 2010 m. gegužės 18 d. EŽTT sprendimą *Kennedy prieš Jungtinę Karalystę* (CE:ECHR:2010:0518JUD002683905, 167 punktas) ir Sprendimą *Zakharov* (233 ir 258 punktai).

187 Žr. Sprendimą *Szabó ir Vissy* (77 punktas) ir Sprendimą *Centrüm för Rättvisa* (133 punktas).

188 Juo labiau atsižvelgiant į šios išvados 281 punkte pateiktus argumentus.

189 Žr. šios išvados 330 ir 331 punktus.

312. Antra, „net jeigu galimybėmis pasinaudoti teisminėmis teisių gynimo priemonėmis iš esmės gali pasinaudoti ir ne JAV asmenys, pvz., stebėjimas [dėl stebėjimo] pagal FISA, prieinami ieškinio pareiškimo pagrindai yra riboti <…> o asmenų (įskaitant JAV asmenis) pareikšti ieškiniai bus paskelbti nepriimtinais, jeigu negalima įrodyti jų pagrįstumo <…>, todėl galimybė kreiptis į bendrosios kompetencijos teismus yra ribota“.

313. Iš sprendimo dėl „privatumo skydo“ 116–124 konstatuojamųjų dalių darytina išvada, kad ombudsmeno institucija siekiama kompensuoti šiuos apribojimus. Komisija šio sprendimo 139 konstatuojamojoje dalyje daro išvadą, kad, „*atsižvelgiant į visas aplinkybes*, „privatumo skydo“ sistemoje užtikrinama *priežiūra* ir *nurodytos[-i] teisių gynimo institucijos* [mechanizmai] sudaro sąlygas <…> suteikti teisines teisių gynimo priemones duomenų subjektui, kad jis galėtų susipažinti su savo asmens duomenimis ir galiausiai panaikinti arba ištrinti tokius duomenis [reikalauti, kad jie būtų ištaisyti arba ištrinti]“ (išskirta mano).

314. Primindamas bendruosius principus, kylančius iš Teisingumo Teismo ir EŽTT jurisprudencijos, susijusios su teise pareikšti ieškinį dėl pranešimų stebėjimo priemonių, nagrinėsiu, ar JAV teisėje numatytos teisminės teisių gynimo priemonės, apibūdintos sprendime dėl „privatumo skydo“, leidžia užtikrinti tinkamą duomenų subjektų teisminę gynybą (1 dalis). Tada nustatysiu, ar neteisminio mechanizmo – ombudsmeno – numatymas atitinkamais atvejais leidžia užpildyti galimas šių asmenų teisminės gynybos spragas (2 dalis).

1) Dėl JAV teisėje numatytų teisminių teisių gynimo priemonių veiksmingumo

315. Pirma, Chartijos 47 straipsnio pirmoje pastraipoje įtvirtinama kiekvieno asmens, kurio teisės ir laisvės, garantuojamos Sąjungos teisės, yra pažeistos, teisė į veiksmingą jų gynybą teisme[190]. Kaip nurodyta šio straipsnio antroje pastraipoje, kiekvienas asmuo turi teisę, kad jo bylą išnagrinėtų nepriklausomas ir nešališkas teismas[191]. Teisė kreiptis į nepriklausomą teismą yra Chartijos 47 straipsnyje užtikrinamos teisės esmė[192].

316. Greta šios teisės į individualią teisminę gynybą valstybėms narėms pagal Chartijos 7 ir 8 straipsnius nustatyta pareiga pasirūpinti, kad, išskyrus deramai pateisinamus skubius atvejus, kiekvienai stebėjimo priemonei būtų taikoma išankstinė teismo ar nepriklausomos administracinės institucijos kontrolė[193].

317. Žinoma, kaip teigia Vokietijos ir Prancūzijos vyriausybės, teisė į veiksmingą teisminę gynybą nėra absoliuti[194] ir gali būti ribojama dėl nacionalinio saugumo priežasčių. Vis dėlto išimtys yra leidžiamos tik jeigu jos nekeičia šios teisės esmės ir jeigu yra griežtai būtinos teisėtam tikslui pasiekti.

190 Su Chartija susijusiuose išaiškinimuose šiuo klausimu nurodyta, kad „Sąjungos teisėje [Chartijos 47 straipsnyje numatyta] gynyba yra platesnė [nei numatytoji EŽTK 13 straipsnyje], nes yra garantuojama teisė į veiksmingą gynybą teisme“. Taip pat žr. generalinio advokato N. Wathelet išvadą byloje *Berlioz Investment Fund* (C-682/15, EU:C:2017:2, 37 punktas).

191 Siekiant įvertinti, ar pagal Chartijos 47 straipsnį institucija yra „teismas“, reikia atsižvelgti į tai, ar ji yra įsteigta pagal įstatymus, ar ji nuolatinė, ar jos jurisdikcija yra privaloma, ar procesas joje grindžiamas rungimosi principu, ar ji taiko teisės normas ir yra nepriklausoma. Žr. 2018 m. vasario 27 d. Sprendimą *Associação Sindical dos Juízes Portugueses* (C-64/16, EU:C:2018:117, 38 punktas ir jame nurodyta jurisprudencija).

192 Žr., be kita ko, 2018 m. liepos 25 d. Sprendimą *Minister for Justice and Equality* (*Teismų sistemos trūkumai*) (C-216/18 PPU, EU:C:2018:586, 59 ir 63 punktai); 2019 m. lapkričio 5 d. Sprendimą Komisija / Lenkija (*Bendrosios kompetencijos teismų nepriklausomumas*) (C-192/18, EU:C:2019:924, 106 punktas) ir 2019 m. lapkričio 19 d. Sprendimą *A. K. ir kt.* (*Aukščiausiojo Teismo Drausmės bylų kolegijos nepriklausomumas*) (C-585/18, C-624/18 ir C-625/18, EU:C:2019:982, 120 punktas).

193 Žr. šios išvados 293 punktą. BDAR 45 straipsnio 3 dalies a punkte numatyta, kad vertinant trečiosios valstybės užtikrinamo apsaugos lygio tinkamumą turi būti atsižvelgiama į „administracines *bei teismines* <…> teisių gynimo priemones“, kurių gali veiksmingai imtis duomenų subjektai (išskirta mano). Be to, kaip nurodyta BDAR 104 konstatuojamojoje dalyje, priimant sprendimą dėl tinkamumo turėtų būti atsižvelgiama į tai, ar duomenų subjektams nagrinėjamoje trečiojoje šalyje suteikiama „galimybė naudotis veiksmingomis administracinėmis ir teisminėmis teisių gynimo priemonėmis“ (išskirta mano). Taip pat žr. 2017 m. lapkričio 28 d. 29 straipsnio darbo grupės dokumentą „EU-U.S. Privacy Shield – First Annual Joint Review“, WP 255 (B.3 skirsnis); 2018 m. liepos 5 d. Europos Parlamento rezoliuciją dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo, P8_TA-PROV(2018)0315 (25 ir 30 punktai) ir 2019 m. sausio 22 d. EDPB dokumentą „EU-U.S. Privacy Shield – Second Annual Joint Review“ (94–97 punktai).

194 Šiuo klausimu žr. 2013 m. vasario 28 d. Sprendimą *Réexamen Arango Jaramillo ir kt. / EIB* (C-334/12 RX-II, EU:C:2013:134, 43 punktas).

318. Šiuo klausimu Teisingumo Teismas Sprendime *Schrems* konstatavo, 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 Chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės [195].

319. Pažymiu, kad ši teisė susipažinti su duomenimis, išskyrus išimtis, kurios yra griežtai būtinos siekiant teisėto intereso, reiškia asmens galimybę iš viešosios valdžios institucijų gauti *patvirtinimą, ar jos tvarko jo asmens duomenis, ar ne* [196]. Manau, tokia yra teisės susipažinti su duomenimis praktinė taikymo sritis, jeigu suinteresuotasis asmuo nežino, ar viešosios valdžios institucijos yra išsaugojusios jo asmens duomenis, be kita ko, pasibaigus automatizuotomis priemonėmis vykdytam elektroninių pranešimų srauto filtravimo procesui.

320. Be to, pagal jurisprudenciją valstybės narės valdžios institucijos iš esmės turi informuoti apie prieigą prie duomenų *nuo to momento, kai toks informavimas nebegali pakenkti šių institucijų atliekamiems tyrimams* [197]. Iš tiesų toks informavimas yra būtina teisės pareikšti ieškinį įgyvendinimo sąlyga pagal Chartijos 47 straipsnį [198]. Dabar ši pareiga pakartota BDAR 23 straipsnio 2 dalies h punkte.

321. Sprendimo dėl „privatumo skydo“ 111–135 konstatuojamosiose dalyse glaustai išdėstomos visos teisių gynimo priemonės, prieinamos asmenims, kurių duomenys perduodami, jeigu jie baiminasi, kad po perdavimo šiuos duomenis galėjo tvarkyti JAV žvalgybos tarnybos. Šios teisių gynimo priemonės taip pat apibūdintos prie nutarties dėl prašymo priimti prejudicinį sprendimą pridėtame 2017 m. spalio 3 d. *High Court* (Aukštasis Teismas) sprendime ir, be kita ko, JAV vyriausybės pateiktose pastabose.

322. Nebūtina išsamiai kartoti to, kas išdėstyta minėtose konstatuojamosiose dalyse. Iš tiesų prašymą priimti prejudicinį sprendimą pateikęs teismas kvestionuoja apsaugos priemonių, susijusių su duomenų subjektų teisine apsauga, tinkamumą, iš esmės motyvuodamas tuo, kad dėl ypač griežtų reikalavimų, susijusių su teise pareikšti ieškinį (*standing*) [199], ir kartu jokios pareigos informuoti asmenis, kuriems taikoma stebėjimo priemonė, nebuvimo, *net jeigu juos informavus nebebūtų pakenkta šios priemonės tikslams*, JAV teisėje numatytomis teisių gynimo priemonėmis tampa pernelyg sunku pasinaudoti praktiškai. Šioms abejonėms pritaria DPC, M. Schrems, Austrijos, Lenkijos ir Portugalijos vyriausybės, taip pat EDPB [200].

195 Sprendimas *Schrems* (95 punktas).

196 BDAR 15 straipsnio „Duomenų subjekto teisė susipažinti su duomenimis“ 1 dalyje nurodyta, kad šis asmuo „turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis“. Sprendimo dėl „privatumo skydo“ II priedo II dalies 8 punkto a papunktyje numatytas „galimybės susipažinti su duomenimis principas“ turi tokią pačią reikšmę.

197 Sprendimas *Tele2 Sverige* (121 punktas) ir Nuomonė 1/15 (220 punktas). Kaip pažymėjo *Facebook Ireland*, todėl negalima sistemingai reikalauti informavimo apie viešosios valdžios institucijų prieigą prie duomenų. Šiuo klausimu EŽTT yra nusprendęs, kad „praktiškai gali būti netikslinga reikalauti informavimo *a posteriori*“, jeigu grėsmė, dėl kurios taikomos stebėjimo priemonės, „gali tęstis daug metų ar net dešimtmečių“ po šių priemonių panaikinimo, todėl informavimas „gali pakenkti ilgalaikiam tikslui, kuriuo remiantis buvo pradėtas stebėjimas“, ir „atskleisti žvalgybos tarnybų darbo metodus, jų veiklos sritis ir <…> agentų tapatybę“ (Sprendimas *Zakharov* (287 punktas ir jame nurodyta jurisprudencija). Jeigu duomenų subjektas neinformuojamas, nors pažeidus teisinius reikalavimus tampa praktiškai neįgyvendinamos individualios teisių gynimo priemonės, teisei į privataus gyvenimo gerbimą apsaugoti gali pakakti ir kitų garantijų (taip pat žr. Sprendimo *Centrüm för Rättvisa* 164–167 ir 171–178 punktus). Žr. šios išvados 330 punktą.

198 Šiuo klausimu žr. šios išvados 210 išnašą.

199 Žr. šios išvados 67 punktą.

200 Žr. EDPB „EU-U.S. Privacy Shield – Second Annual Joint Review“, 2019 m. sausio 22 d. (p. 18, 97 punktas).

323. Šiuo klausimu tik noriu priminti, kad taisyklės, susijusios su teise pareikšti ieškinį, negali pažeisti teisės į veiksmingą teisminę gynybą [201], ir konstatuoti, kad sprendime dėl „privatumo skydo“ neminima jokio reikalavimo informuoti duomenų subjektus apie tai, kad jiems yra taikoma stebėjimo priemonė [202]. Kadangi pareigos informuoti apie tokią priemonę nebuvimas gali kliudyti pasinaudoti teisminėmis teisių gynimo priemonėmis, nenumatant šios pareigos net jeigu duomenų subjekto informavimas jau nebegalėtų pakenkti jos veiksmingumui, atrodo problemiška, atsižvelgiant į šios išvados 320 punkte nurodytą jurisprudenciją.

324. Be to, sprendimo dėl „privatumo skydo“ 169 išnašoje pripažįstama, kad ieškinius galima pareikšti „dėl nuostolių <…> arba įrodžius, kad vyriausybė ketina naudoti arba atskleisti informaciją, gautą arba perimtą elektroninėmis priemonėmis stebint atitinkamą asmenį <…>“. Kaip pažymėjo prašymą priimti prejudicinį sprendimą pateikęs teismas, DPC ir M. Schrems, šis reikalavimas neatitinka Teisingumo Teismo jurisprudencijos, pagal kurią nustatant, ar egzistuoja suinteresuotojo asmens pagrindinės teisės į privatų gyvenimą apribojimas, nelabai svarbu, ar dėl šio apribojimo suinteresuotieji asmenys patyrė nepatogumų [203].

325. Be to, *Facebook Ireland* ir JAV vyriausybės išreikštas požiūris, kad asmenų, kurių duomenys perduodami į JAV, teisminės gynybos trūkumus kompensuoja FISC atliekama kontrolė *a priori* ir *a posteriori* bei įvairūs vykdomojoje ir teisėkūros valdžioje nustatyti priežiūros mechanizmai [204], manęs neįtikina.

326. Jau pažymėjau, kad, pirma, kaip konstatuota sprendime dėl „privatumo skydo“, FISC nekontroliuoja individualių stebėjimo priemonių prieš jų įgyvendinimą [205]. Taigi, kaip rodo minėto sprendimo 109 konstatuojamoji dalis ir kaip raštu pateiktame atsakyme į Teisingumo Teismo klausimus tai patvirtino JAV vyriausybė, selektorių taikymo kontrolės *ex post* tikslas, antra, yra patikrinti, jeigu žvalgybos agentūra pranešė FISC apie incidentą, susijusį su numatomų stebėti asmenų tikslingo pasirinkimo ir minimalios informacijos procedūrų galimu pažeidimu [206], ar laikomasi metiniame sertifikate numatytų selektorių pasirinkimą reglamentuojančių sąlygų. Taigi atrodo, kad per FISC vykdomą procedūrą asmenims, kurių duomenys perduodami į JAV, nėra suteikiamos veiksmingos individualios teisių gynimo priemonės.

327. Mano nuomone, nors sprendimo dėl „privatumo skydo“ 95–110 konstatuojamosiose dalyse paminėti neteisminės priežiūros mechanizmai atitinkamais atvejais galėtų sustiprinti galimas teismines teisių gynimo priemones, jų negali pakakti tinkamam apsaugos lygiui užtikrinti atsižvelgiant į duomenų subjektų teisę pareikšti ieškinį. Visų pirma man atrodo, kad generaliniai inspektoriai, priklausantys kiekvienos agentūros vidaus struktūrai, nėra nepriklausomas kontrolės mechanizmas. PCLOB ir Kongreso žvalgybos komitetų vykdoma priežiūra neprilygsta individualios teisių gynimo priemonės mechanizmui ginantis nuo stebėjimo priemonių.

328. Dabar reikia išnagrinėti, ar ombudsmeno institucija užpildo šias spragas, suteikiant duomenų subjektams veiksmingą teisių gynimo priemonę nepriklausomoje ir nešališkoje institucijoje [207].

201 Žr., be kita ko, 1991 m. liepos 11 d. Sprendimą *Verholen ir kt.* (C-87/90–C-89/90, EU:C:1991:314, 24 punktas ir jame nurodyta jurisprudencija) ir 2013 m. vasario 28 d. Sprendimą *Réexamen Arango Jaramillo ir kt. / EIB* (C-334/12 RX-II, EU:C:2013:134, 43 punktas).

202 Vis dėlto JAV vyriausybė, panašiai kaip prašymą priimti prejudicinį sprendimą pateikęs teismas, patikslino, kad apie stebėjimo priemonę, taikomą pagal FISA 702 straipsnį, turi būti pranešama tiksliniam asmeniui, jeigu surinkti duomenys yra naudojami prieš jį teismo procese.

203 2003 m. gegužės 20 d. Sprendimas *Österreichischer Rundfunk ir kt.* (C-465/00, C-138/01 ir C-139/01, EU:C:2003:294, 75 punktas); Sprendimas *Digital Rights Ireland* (33 punktas); Sprendimas *Schrems* (87 punktas) ir Nuomonė 1/15 (124 punktas).

204 Šie mechanizmai apibūdinti sprendimo dėl „privatumo skydo“ 95–110 konstatuojamosiose dalyse. Komisija taisyklių, susijusių su „veiksminga teismine gynyba“, kategorijoje išskiria priežiūros mechanizmus (žr. 92–110 konstatuojamąsias dalis) ir individualias teisių gynimo priemones (žr. 111–124 konstatuojamąsias dalis).

205 Žr. šios išvados 298 punktą.

206 Kaip nurodoma sprendimo dėl „privatumo skydo“ 109 konstatuojamojoje dalyje, „generalinis prokuroras ir [NSA] direktorius tikrina, kaip laikomasi reikalavimų, o agentūros turi pareigą pranešti apie visus neatitikties incidentus FISC <…>, kuris šiuo pagrindu gali daryti leidimo pakeitimus“.

207 Žr. šios išvados 333–340 punktus.

329. Antra, primenu, kad, siekiant įvertinti sprendime dėl „privatumo skydo“ konstatuoto tinkamumo pagrįstumą, kiek tai susiję su teisių gynimo priemonėmis, prieinamomis asmenims, manantiems, kad yra stebimi remiantis EO 12333, reikšmingas referencinis pagrindas yra EŽTK nuostatos.

330. Kaip jau nurodžiau [208], EŽTT, siekdamas įvertinti, ar stebėjimo priemonė atitinka „nuspėjamumo“ ir „būtinumo demokratinėje visuomenėje“ reikalavimus, kaip jie suprantami pagal EŽTK 8 straipsnio 2 dalį [209], nagrinėja visus kontrolės ir priežiūros mechanizmus, įgyvendinamus „prieš vykdant šią priemonę, kai ji vykdoma ir po jos įvykdymo“. Jeigu individualia teisių gynimo priemone neįmanoma pasinaudoti todėl, kad apie stebėjimo priemonę neįmanoma informuoti, nes kiltų pavojus jos veiksmingumui [210], ši spraga gali būti kompensuota, jeigu prieš taikant nagrinėjamą priemonę atliekama nepriklausoma kontrolė [211]. Taigi, nors EŽTT laiko tokį informavimą „pageidautinu“, jeigu jis yra galimas nepakeičiant stebėjimo priemonės veiksmingumo, EŽTT nenustatė jo kaip reikalavimo [212].

331. Šiuo klausimu iš sprendimo dėl „privatumo skydo“ nėra aišku, kad duomenų subjektai būtų informuojami apie EO 12333 grindžiamas stebėjimo priemones ar kad kuriuo nors šių priemonių nustatymo ar įgyvendinimo etapu nepriklausomi teisminės arba administracinės kontrolės mechanizmai nubrėžtų šių priemonių ribas.

332. Tokiomis aplinkybėmis reikia išnagrinėti, ar kreipimasis į ombudsmeną vis dėlto leidžia užtikrinti nepriklausomą stebėjimo priemonių priežiūrą, taip pat ir tais atvejais, kai jos grindžiamos EO 12333.

2) Dėl ombudsmeno institucijos poveikio teisės į veiksmingą teisinę gynybą apsaugos lygiui

333. Kaip nurodyta sprendimo dėl „privatumo skydo“ 116 konstatuojamojoje dalyje, šio sprendimo III priedo A priede apibūdinta ombudsmeno institucija visiems asmenims, kurių duomenys perduodami iš Sąjungos į JAV, siekiama suteikti papildomas teisių gynimo priemones.

334. Kaip pažymėjo JAV vyriausybė, ombudsmenui pateikto skundo priimtinumas nepriklauso nuo taisyklių, susijusių su teise pareikšti ieškinį, panašių į tas, kuriomis reglamentuojama galimybė kreiptis į JAV teismus, laikymosi. Šiuo klausimu minėto sprendimo 119 konstatuojamojoje dalyje patikslinta, kad, padavęs skundą ombudsmenui, suinteresuotasis asmuo neprivalo įrodyti, kad JAV vyriausybė tikrino jo asmens duomenis.

335. Panašiai, kaip DPC, M. Schrems, Lenkijos ir Portugalijos vyriausybės, taip pat EPIC, abejoju, ar toks mechanizmas gali kompensuoti asmenims, kurių duomenys perduodami iš Sąjungos į JAV, siūlomos teisminės gynybos trūkumus.

208 Žr. šios išvados 305 punktą.

209 Jurisprudencijoje, susijusioje su telekomunikacijų stebėjimo priemonėmis, EŽTT nagrinėjo teisių gynimo priemonių klausimą, analizuodamas, ar EŽTK 8 straipsnyje užtikrinamos teisės ribojimas yra nustatytas „įstatymo“ ir ar jis yra būtinas (žr., pavyzdžiui, Sprendimą *Zakharov* (236 punktas) ir Sprendimą *Centrüm för Rättvisa* (107 punktas). 2008 m. liepos 1 d. Sprendime *Liberty ir kt. prieš Jungtinę Karalystę* (CE:ECHR:2008:0701JUD005824300, 73 punktas) ir Sprendime *Zakharov* (307 punktas) konstatavęs EŽTK 8 straipsnio pažeidimą, EŽTT nusprendė, kad nebūtina atskirai nagrinėti pagrindo, susijusio su šios konvencijos 13 straipsniu.

210 Kaip yra nusprendęs EŽTT, nors neinformavimas, nesvarbu, kuriuo etapu, nebūtinai reiškia, kad stebėjimo priemonė neatitinka „būtinumo demokratinėje visuomenėje“ reikalavimo, jis turi neigiamą poveikį galimybei kreiptis į teismą, taigi ir teisių gynimo priemonių veiksmingumui (žr., be kita ko, 1978 m. rugsėjo 6 d. Sprendimą *Klass ir kt. prieš Vokietiją* (CE:ECHR:1978:0906JUD000502971, 57 ir 58 punktai); Sprendimą *Weber ir Saravia* (135 punktas) ir Sprendimą *Zakharov* (302 punktas).

211 Šiuo klausimu žr. Sprendimą *Centrum för Rättvisa* (105 punktas).

212 Sprendime *Big Brother Watch* (317 punktas) EŽTT atsisakė reikalavimą informuoti duomenų subjektus apie stebėjimą pripažinti kaip minimalią garantiją, taikomą stebėjimo sistemai, kurią taikant buvo masiškai perimami elektroniniai pranešimai. Taip pat žr. Sprendimą *Centrüm för Rättvisa* (164 punktas). Šie sprendimai yra perduoti EŽTT didžiajai kolegijai, be kita ko, siekiant peržiūrėti tokią išvadą.

336. Pirmiausia, nors alternatyvaus ginčų sprendimo mechanizmas gali būti veiksminga teisinės gynybos priemonė, kaip tai suprantama pagal Chartijos 47 straipsnį, taip yra tik tuo atveju, jeigu nagrinėjama institucija yra numatyta įstatymo ir atitinka nepriklausomumo reikalavimą [213].

337. Vis dėlto iš sprendimo dėl „privatumo skydo“ matyti, kad ombudsmeno institucija, kuri buvo įsteigta PPD 28 [214], nėra numatyta įstatymo. Ombudsmeną skiria valstybės sekretorius ir jis įeina į JAV Valstybės departamento sudėtį [215]. Minėtame sprendime nėra jokios informacijos apie tai, kad ombudsmeno atšaukimui iš pareigų ar jo paskyrimo panaikinimui būtų taikomos ypatingos garantijos [216]. Nors ombudsmenas pristatomas kaip nepriklausomas nuo „žvalgybos bendruomenės“, jis atsiskaito valstybės sekretoriui, taigi nėra nepriklausomas nuo vykdomosios valdžios [217].

338. Be to, man atrodo, kad neteisminės teisių gynimo priemonės veiksmingumas taip pat priklauso nuo nagrinėjamos institucijos galimybės priimti privalomus ir motyvuotus sprendimus. Šiuo klausimu sprendime dėl „privatumo skydo“ nėra jokios informacijos apie tai, kad ombudsmenas priima tokius sprendimus. Jame nenurodyta, kad ombudsmeno institucija leistų skundo pateikėjams susipažinti su duomenimis, kurie yra susiję su jais, ar reikalauti juos ištaisyti arba ištrinti arba kad ombudsmenas galėtų įpareigoti atlyginti žalą nuo stebėjimo priemonės nukentėjusiems asmenims. Visų pirma, kaip matyti iš šio sprendimo III priedo A priedo 4 dalies e punkto, „ombudsmenas nei patvirtins, nei paneigs, ar asmuo buvo stebimas, „privatumo skydo“ ombudsmenas taip pat nepatvirtins, ar buvo taikoma konkreti teisių gynimo priemonė“ [218]. Nors JAV vyriausybė įsipareigojo dėl to, kad atitinkamas žvalgybos tarnybų padalinys turės ištaisyti kiekvieną ombudsmeno nustatytą taikytinų normų pažeidimą [219], minėtame sprendime nekalbama apie jokias teisines garantijas, siejamas su šiuo įsipareigojimu, kuriomis galėtų remtis atitinkami asmenys.

339. Taigi, mano nuomone, ombudsmeno institucija nesuteikia teisių gynimo priemonės nepriklausomoje institucijoje, kurioje asmenims, kurių duomenys perduodami, būtų suteikta galimybė remtis jų teise susipažinti su duomenimis arba ginčyti žvalgybos tarnybų galimai padarytus taikytinų taisyklių pažeidimus.

213 Nepriklausomumo sąvoka apima du aspektus. Pagal pirmąjį, išorinį, aspektą reikalaujama, kad atitinkama institucija būtų apsaugota nuo išorinio kišimosi ar spaudimo, galinčio kelti grėsmę jos narių nepriklausomam sprendimų dėl jiems pateiktų nagrinėti ginčų priėmimui. Antrasis, vidinis, šios sąvokos aspektas susijęs su nešališkumu ir reikalauja vienodai atsiriboti nuo bylos šalių ir jų atitinkamų interesų, susijusių su nagrinėjamos bylos dalyku. Žr., be kita ko, 2006 m. rugsėjo 19 d. Sprendimą *Wilson* (C-506/04, EU:C:2006:587, 50–52 punktai); 2018 m. liepos 25 d. Sprendimą *Minister for Justice and Equality* (*Teismų sistemos trūkumai*) (C-216/18 PPU, EU:C:2018:586, 63 ir 65 punktai) ir 2019 m. lapkričio 19 d. Sprendimą *A. K. ir kt.* (*Aukščiausiojo Teismo Drausmės bylų kolegijos nepriklausomumas*) (C-585/18, C-624/18 ir C-625/18, EU:C:2019:982, 121 ir 122 punktai). Pagal valdžių atskyrimo principą turi būti užtikrinamas teismų nepriklausomumas nuo, be kita ko, vykdomosios valdžios. Žr. 2019 m. lapkričio 19 d. Sprendimą *A. K. ir kt.* (*Aukščiausiojo Teismo Drausmės bylų kolegijos nepriklausomumas*) (C-585/18, C-624/18 ir C-625/18, EU:C:2019:982, 127 punktas ir jame nurodyta jurisprudencija)

214 Sprendimo dėl „privatumo skydo“ III priedo A priede šiuo klausimu daroma nuoroda į PPD 28 4 skirsnio d punktą.

215 Žr. sprendimo dėl „privatumo skydo“ 116 konstatuojamąją dalį.

216 2005 m. gegužės 31 d. Sprendime *Syfait ir kt.* (C-53/03, EU:C:2005:333, 31 punktas) Teisingumo Teismas pabrėžė šių garantijų svarbą, kad būtų įvykdytas nepriklausomumo reikalavimas. Šiuo klausimu taip pat žr. 2019 m. birželio 24 d. Sprendimą *Komisija / Lenkija* (*Aukščiausiojo Teismo nepriklausomumas*) (C-619/18, EU:C:2019:531, 76 punktas) ir 2019 m. lapkričio 5 d. Sprendimą *Komisija / Lenkija* (*Bendrosios kompetencijos teismų nepriklausomumas)* (C-192/18, EU:C:2019:924, 113 punktas).

217 Žr. sprendimo dėl „privatumo skydo“ 65 ir 121 konstatuojamąsias dalis ir III priedo A priedo 1 dalį.

218 Be to, sprendimo dėl „privatumo skydo“ 121 konstatuojamojoje dalyje nurodyta, kad „ombudsmenas turės patvirtinti, kad: i) skundas buvo tinkamai ištirtas; ir ii) atitinkamo JAV įstatymo, visų pirma įskaitant VI priede nustatytus apribojimus ir apsaugos priemones, buvo laikomasi arba, jeigu teisės nebuvo laikomasi, kad toks pažeidimas buvo ištaisytas“.

219 Komisija, atlikusi trečiąją metinę „privatumo skydo“ peržiūrą, konstatavo, kad, kaip pareiškė JAV vyriausybė, jeigu ombudsmeno atliktas tyrimas atskleistų, kad buvo pažeistos FISC patvirtintos numatomų stebėti asmenų tikslingo pasirinkimo ir minimalios informacijos procedūros, šis pažeidimas turėtų būti perduotas nagrinėti šiam teismui. Tada FISC atliktų nepriklausomą tyrimą ir prireikus nurodytų atitinkamai žvalgybos agentūrai ištaisyti minėtą pažeidimą. Žr. Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, 2019 m. spalio 23 d., SWD(2019) 390 *final*, p. 28. Komisija šiame dokumente nurodė dokumentą „Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure“, pateikiamą adresu https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (p. 4 ir 5).

340. Galiausiai pagal jurisprudenciją, kad būtų laikomasi Chartijos 47 straipsnyje užtikrinamos teisės, administracinės institucijos sprendimui, kuris pats neatitinka nepriklausomumo ir nešališkumo sąlygų, turi būti taikoma paskesnė teismo, kuris visų pirma turi turėti kompetenciją nagrinėti visus svarbius klausimus, kontrolė[220]. Vis dėlto, remiantis sprendime dėl „privatumo skydo“ pateikta informacija, ombudsmeno sprendimams netaikoma nepriklausomo teismo kontrolė.

341. Tokiomis aplinkybėmis, pritardamas DPC, M. Schrems, EPIC ir Lenkijos bei Portugalijos vyriausybėms, abejoju, ar JAV teisės sistemoje numatyta teisminė gynyba asmenims, kurių duomenys perduodami į šią šalį iš Sąjungos, yra iš esmės tokia pati kaip ir teisminė gynyba, užtikrinama pagal BDAR, aiškinamą atsižvelgiant į Chartijos 47 straipsnį ir EŽTK 8 straipsnį.

342. Atsižvelgiant į visa tai, kas išdėstyta, man kyla tam tikrų abejonių dėl sprendimo dėl „privatumo skydo“ atitikties BDAR 45 straipsnio 1 daliai, aiškinamai atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius ir EŽTK 8 straipsnį.

V. Išvada

343. Siūlau Teisingumo Teismui taip atsakyti į *High Court* (Aukštasis Teismas, Airija) pateiktus prejudicinius klausimus:

Prejudicinių klausimų analizė neatskleidė jokios aplinkybės, kuri paveiktų 2010 m. vasario 5 d. Komisijos sprendimo 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas, iš dalies pakeisto 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimu (ES) 2016/2297, galiojimą.

220 Žr. 2017 m. gegužės 16 d. Sprendimą *Berlioz Investment Fund* (C-682/15, EU:C:2017:373, 55 punktas) ir 2017 m. gruodžio 13 d. Sprendimą *El Hassani* (C-403/16, EU:C:2017:960, 39 punktas).