GENERALINIO ADVOKATO
YVES BOT IŠVADA,
pateikta 2015 m. rugsėjo 23 d.[1]

Byla C-362/14

Maximillian Schrems
prieš
Data Protection Commissioner

(High Court (Airija) pateiktas prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą — Asmens duomenys — Fizinių asmenų apsauga tvarkant šiuos duomenis — Europos Sąjungos pagrindinių teisių chartija — 7, 8 ir 47 straipsniai — Direktyva 95/46/EB — 25 straipsnis — Sprendimas 2000/520/EB — Asmens duomenų perdavimas į Jungtines Amerikos Valstijas — Apsaugos lygio adekvatumo arba neadekvatumo įvertinimas — Fizinio asmens, kurio duomenys buvo perduoti į trečiąją šalį, skundas — Nacionalinė priežiūros institucija — Įgaliojimai“

I – **Įžanga**

1. Kaip Europos Komisija pripažino savo 2013 m. lapkričio 27 d. komunikate[2], „[p]lėtojant transatlantinius ryšius, asmens duomenų perdavimas yra svarbus ir būtinas. Tai neatsiejama nuo komercinių mainų abipus Atlanto, įskaitant naujas besivystančias skaitmeninio verslo įmones, kaip antai socialinius tinklus arba debesijos kompiuteriją, perduodant iš ES į JAV daugybę duomenų“[3].

2. Dėl komercinių mainų buvo priimtas 2000 m. liepos 26 d. Komisijos sprendimas 2000/520/EB dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“[4]. Šis sprendimas suteikia teisinį pagrindą perduoti asmens duomenis iš Sąjungos Jungtinėse Amerikos Valstijose įsteigtoms įmonėms, kurios laikosi „saugaus uosto“ principų.

3. Šiuo metu įgyvendinant minėtą sprendimą nuolat susiduriama su iššūkiu leisti duomenų srautus tarp Sąjungos ir Jungtinių Amerikos Valstijų, kartu užtikrinant aukštą šių duomenų apsaugos lygį, kaip to reikalaujama pagal Sąjungos teisę.

4. Iš tiesų neseniai tam tikri faktai parodė, kad amerikiečiai įgyvendina didelio masto duomenų rinkimo programas. Tai atskleidus, kilo abejonių, ar laikomasi Sąjungos teisės normų, kai perduodami asmens duomenys Jungtinėse Amerikos Valstijose įsteigtoms įmonėms, ir išryškėjo „saugaus uosto“ sistemos trūkumai.

1 — Originalo kalba: prancūzų.

2 — Komisijos komunikatas Europos Parlamentui ir Tarybai „Pasitikėjimo ES ir JAV duomenų mainais atkūrimas“ [COM(2013) 846 *final*].

3 — p. 2.

4 — OL L 215, p. 7, ir klaidų ištaisymas OL L 115, 2001, p. 14; 2004 m. specialusis leidimas lietuvių k., 16 sk., 1 t., p. 119.

5. Šiuo prašymu priimti prejudicinį sprendimą Teisingumo Teismo prašoma patikslinti, kokio požiūrio turi laikytis nacionalinės priežiūros institucijos ir Komisija, susidūrusios su sunkumais taikyti Sprendimą 2000/520.

6. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo [5] IV skyriuje numatytos taisyklės, susijusios su asmens duomenų perdavimu į trečiąsias šalis.

7. Pagal šio skyriaus 25 straipsnio 1 dalyje įtvirtintą principą asmens duomenys, kurie yra tvarkomi arba kuriuos juos perdavus ketinama tvarkyti, gali būti perduodami į trečiąją šalį tik tuo atveju, jeigu ši trečioji šalis užtikrina adekvatų šių duomenų apsaugos lygį.

8. Ir, atvirkščiai, kaip Sąjungos teisės aktų leidėjas nurodo minėtos direktyvos 57 konstatuojamojoje dalyje, turi būti uždrausta perduoti asmens duomenis į trečiąją šalį, kuri neužtikrina adekvataus apsaugos lygio.

9. Direktyvos 95/46 25 straipsnio 2 dalyje nustatyta: „apsaugos, kurią suteikia trečioji šalis, lygio adekvatumas įvertinamas atsižvelgiant į 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“.

10. Pagal šios direktyvos 25 straipsnio 6 dalį Komisija gali konstatuoti, kad adekvatų asmens duomenų apsaugos lygį trečioji šalis užtikrina savo šalies įstatymais arba tarptautiniais įsipareigojimais. Taigi, jeigu Komisija šiuo klausimu priima sprendimą, asmens duomenys gali būti perduodami į atitinkamą trečiąją šalį.

11. Taikydama šią nuostatą Komisija priėmė Sprendimą 2000/520. Iš šio sprendimo 1 straipsnio 1 dalies matyti, kad „saugaus uosto privatumo principai“, taikomi laikantis „Dažnai užduodamų klausimų“ nurodymų [6], laikomi užtikrinančiais pakankamą Jungtinėse Valstijose įsikūrusioms organizacijoms iš Sąjungos perduodamų asmens duomenų apsaugos lygį.

12. Todėl pagal Sprendimą 2000/520 asmens duomenis iš valstybių narių Jungtinėse Valstijose įsikūrusioms įmonėms leidžiama perduoti, jeigu šios įmonės yra įsipareigojusios laikytis „saugaus uosto“ principų.

13. Sprendimo 2000/520 I priede nurodyti tam tikri principai, kurių įmonės gali įsipareigoti laikytis savanoriškai, taip pat nustatyti apribojimai ir speciali kontrolės sistema. Įmonių, įsipareigojusių laikytis vadinamojo „elgesio kodekso“, 2013 m. buvo daugiau kaip 3 200.

14. „Saugaus uosto“ sistema grindžiama sprendimu, apimančiu privačiųjų įmonių įsipareigojimą, savęs vertinimą ir viešosios valdžios įsikišimą.

15. Šie „saugaus uosto“ principai buvo sukurti „pasikonsultavus su pramonės ir visuomenės atstovais ir skirti prekybai bei komercijai tarp Jungtinių Valstijų ir Europos Sąjungos palengvinti <...>. Jie tinka naudoti tik JAV organizacijoms, gaunančioms asmens duomenis iš Europos Sąjungos, kad jos galėtų gauti „saugaus uosto“ ir jo sukuriamos „pakankamumo“ prezumpcijos teises“ [7].

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

6 — *Frequently asked questions*, toliau – FAQ.

7 — Sprendimo 2000/520 I priedo antra pastraipa.

16. „Saugaus uosto“ principuose, išdėstytuose Sprendimo 2000/520 I priede, visų pirma numatyta:

— informavimo pareiga, pagal kurią „organizacija privalo pranešti asmenims priežastis, dėl kurių ji renka ir naudoja informaciją apie juos, kaip kreiptis į organizaciją su prašymais ar skundais, apie trečiąsias šalis, kurioms ji atskleidžia tą informaciją, ir apie informacijos naudojimui ir atskleidimui apriboti skirtas galimybes bei priemones, kurias organizacija siūlo asmenims. Toks pranešimas turi būti pateiktas aiškia ir suprantama kalba tada, kai asmenų pirmą kartą prašoma suteikti asmeninę informaciją organizacijai arba kiek įmanoma greičiau po to, tačiau bet kuriuo atveju prieš organizacijai panaudojant tokią informaciją kitais tikslais nei tie, dėl kurių duomenis perduodančioji organizacija ją iš pradžių surinko ar tvarkė, arba prieš pirmą kartą ją atskleidžiant trečiajai šaliai“ [8];

— organizacijos pareiga suteikti atitinkamiems asmenims galimybę pasirinkti, ar jų asmeninė informacija gali būti atskleista trečiajai šaliai arba naudojama tikslais, neatitinkančiais tų tikslų, dėl kurių ji buvo iš pradžių surinkta, ar vėliau buvo gautas asmens sutikimas ją naudoti. Dėl ypatingos informacijos „turi būti suteikta pritariamoji arba aiški (*opt in* būdu) galimybė pasirinkti, ar informacija gali būti atskleista trečiajai šaliai arba naudojama tikslais, neatitinkančiais tų tikslų, dėl kurių ji buvo iš pradžių surinkta ar vėliau pasirenkant (*opt in* būdu) buvo gautas asmens sutikimas ją naudoti“ [9];

— taisyklės, susijusios su tolimesniu duomenų perdavimu. Taigi „norėdamos atskleisti informaciją trečiajai šaliai, organizacijos privalo taikyti pranešimo ir pasirinkimo principus“ [10];

— kalbant apie duomenų saugumą, pareiga, pagal kurią „asmeninę informaciją formuojančios, laikančios, naudojančios ar platinančios organizacijos privalo imtis pagrįstų apsaugos priemonių, saugančių, kad tokia informacija nebūtų prarasta, naudojama ne pagal paskirtį ar asmenims, prieinantiems prie jos neautorizuotu būdu, ji nebūtų, atskleista, pakeista ar sunaikinta“ [11];

— kalbant apie duomenų vientisumą, organizacijų pareiga „<...> imtis pagrįstų priemonių užtikrinti, kad duomenys atitiktų numatomą jų naudojimo paskirtį, būtų tikslūs, išsamūs ir naujausi“ [12];

— kad asmuo, kurio duomenis turi organizacija, iš principo turi turėti „galimybę prieiti prie organizacijos laikomos asmeninės informacijos apie juos, ją pataisyti, pakeisti ar sunaikinti, jei ji būtų netiksli“ [13];

— pareiga numatyti „mechanizmus, užtikrinančius [„saugaus uosto“] Principų laikymąsi, regreso teisę asmenims, kurių duomenims turėjo įtakos principų nesilaikymas, ir Principų nesilaikančios organizacijos atsakomybė“ [14].

17. Amerikos organizacija, kuri nori laikytis „saugaus uosto“ principų, įgyvendindama savo privataus gyvenimo apsaugos politiką, privalo viešai paskelbti, kad laikosi šių principų ir juos tikrai įgyvendina, taip pat pranešti Jungtinių Amerikos Valstijų komercijos departamentui apie įsipareigojimą laikytis šių principų [15].

8 — Žr. I priedo dalį „Pranešimas“.

9 — Žr. I priedo dalį „Pasirinkimas“.

10 — Žr. I priedo dalį „Tolesnis perdavimas“.

11 — Žr. I priedo dalį „Saugumas“.

12 — Žr. I priedo dalį „Duomenų vientisumas“.

13 — Žr. I priedo dalį „Priėjimas“.

14 — Žr. I priedo dalį „Vykdymas“.

15 — Sprendimo 2000/520 1 straipsnio 2 ir 3 dalys. Taip pat žr. II priedo FAQ 6.

18. Organizacijos turi keletą priemonių laikytis „saugaus uosto“ principų. Taigi jos gali, pavyzdžiui, „prisijungti prie savireguliacinės privatumo programos, kuri laikosi Principų [prisijungti prie privataus sektoriaus administruojamos konfidencialumo apsaugos programos, kuri atitinka šiuos principus] arba sukurti nuosavas savireguliacines privatumo taisykles [savo duomenų apsaugos taisykles], jei jos atitinka Principus. <...> Be to, teises naudotis „saugaus uosto“ privilegijomis gali gauti ir organizacijos, kurias saisto norminiai, administraciniai ar kitokie teisės aktai (ar taisyklės), veiksmingai saugantys asmens privatumą [asmens duomenis]“ [16].

19. Siekiant patikrinti, ar laikomasi „saugaus uosto“ principų, taikomi keli mechanizmai, apimantys privatų arbitražą ir viešosios valdžios institucijų kontrolę. Taigi kontrolė taip pat gali būti užtikrinta taikant neteisminio ginčų sprendimo sistemą, pasitelkus nepriklausomą trečiąjį asmenį. Be to, įmonės gali įsipareigoti bendradarbiauti su Sąjungos duomenų apsaugos darbo grupe. Galiausiai kompetenciją nagrinėti skundus turi Federalinė prekybos komisija (*Federal Trade Commission*, toliau – FTC), remdamasi įgaliojimais, kurie jai yra suteikti pagal Federalinės prekybos komisijos įstatymo (*Federal Trade Commission Act*) 5 straipsnį, ir Transporto ministerija (*Department of Transportation*), remdamasi įgaliojimais, kurie jai suteikti pagal Jungtinių Amerikos Valstijų kodekso (*United States Code*) 41712 straipsnį, esantį jo 49 antraštinėje dalyje.

20. Sprendimo 2000/520 I priedo ketvirtoje pastraipoje numatyta, kad „saugaus uosto“ principų laikymasis gali būti ribojamas visų pirma „tiek, kiek tai būtina atsižvelgiant į nacionalinio saugumo, visuomenės interesus arba [JAV] teisės aktų vykdymo reikalavimus [į reikalavimus, susijusius su nacionaliniu saugumu, viešuoju interesu ir Jungtinių Amerikos Valstijų teisės aktų laikymusi]“ ir „įstatymais, Vyriausybės nutarimais arba precedentine teise, dėl kurių atsiranda prieštaringų įsipareigojimų ar aiškių įgaliojimų, jei vykdydama tokius įgaliojimus organizacija gali įrodyti, kad Principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos palaikomus viršesnius teisėtus interesus“ [17].

21. Be to, valstybių narių kompetentingų institucijų galimybei sulaikyti duomenų srautus yra taikomos tam tikros Sprendimo 2000/520 3 straipsnio 1 dalyje numatytos sąlygos.

22. Nagrinėjant šį prašymą priimti prejudicinį sprendimą reikia išsiaiškinti Sprendimo 2000/520 taikymo sritį atsižvelgiant į Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7, 8 ir 47 straipsnius ir Direktyvos 95/46 25 straipsnio 6 dalį ir 28 straipsnį. Šis prašymas buvo pateiktas nagrinėjant M. Schrems ir Duomenų apsaugos komisaro (*Data Protection Commissioner*) ginčą dėl šios institucijos atsisakymo ištirti M. Schrems skundą dėl to, kad *Facebook Ireland Ltd*. (toliau – *Facebook Ireland*) savo registruotų naudotojų asmens duomenis laiko Jungtinėse Amerikos Valstijose esančiuose serveriuose.

23. M. Schrems yra Austrijos pilietis ir joje gyvena. Nuo 2008 m. jis yra socialinio tinklo *Facebook* registruotas naudotojas.

24. Visų Sąjungos teritorijoje gyvenančių *Facebook* registruotų naudotojų prašoma pasirašyti sutartį su *Facebook Ireland*, Jungtinėse Amerikos Valstijose įsikūrusios patronuojančiosios bendrovės *Facebook Inc*. (toliau – *Facebook USA*) dukterine bendrove. Visi Sąjungos teritorijoje gyvenančių *Facebook Ireland* registruotų naudotojų duomenys arba jų dalis perduodama *Facebook USA* serveriams, kurie yra Jungtinių Amerikos Valstijų teritorijoje, ir šie duomenys ten saugomi.

16 — I priedo trečia pastraipa.

17 — Taip pat žr. IV priedo B antraštinę dalį.

25. 2013 m. birželio 25 d. M. Schrems pateikė skundą Duomenų apsaugos komisarui, iš esmės teigdamas, kad pagal Jungtinių Amerikos Valstijų teisę ir praktiką Jungtinių Amerikos Valstijų teritorijoje saugomiems duomenims nuo valstybės sekimo nesuteikiama jokia reali apsauga. Tai paaiškėjo po to, kai E. Snowden nuo 2013 m. gegužės mėn. ėmė viešinti Amerikos saugumo tarnybų, visų pirma Nacionalinės saugumo agentūros (*National Security Agency*, toliau – NSA), veiklą.

26. Iš minėtos atskleistos informacijos visų pirma matyti, kad NSA sukūrė vadinamąją PRISM programą, pagal kurią ši agentūra gaudavo laisvą prieigą prie masinių duomenų, kurie saugomi Jungtinėse Amerikos Valstijose esančiuose serveriuose ir priklauso arba yra kontroliuojami įvairių interneto ir technologijų srityje veikiančių bendrovių, kaip antai *Facebook USA*.

27. Duomenų apsaugos komisaro nuomone, jis neprivalėjo tirti skundo, nes šis neturėjo teisinio pagrindo. Duomenų apsaugos komisaras manė, jog nėra įrodymų, kad NSA susipažino su M. Schrems duomenimis. Be to, jo nuomone, skundą reikia atmesti dėl Sprendimo 2000/520, kuriuo Komisija pripažino, kad Jungtinės Amerikos Valstijos, taikydamos „saugaus uosto“ sistemą, užtikrina adekvatų perduodamų asmens duomenų apsaugos lygį. Bet koks klausimas, susijęs su adekvačiu šių duomenų apsaugos Jungtinėse Amerikos Valstijose pobūdžiu, turėtų būti analizuojamas laikantis šio sprendimo, kuris neleidžia Duomenų apsaugos komisarui nagrinėti skunde iškelto klausimo.

28. Nacionalinės teisės aktai, kuriais remdamasis Duomenų apsaugos komisaras atmetė skundą, yra šie.

29. 1988 m. Duomenų apsaugos įstatymo (*Data Protection (Amendment) Act 1988*), iš dalies pakeisto 2003 m. Duomenų apsaugos įstatymu (*Data Protection Act 2003*, toliau – Duomenų apsaugos įstatymas), 10 straipsnio 1 dalyje jam suteikiami įgaliojimai nagrinėti skundus ir nurodyta:

„a) Duomenų apsaugos komisaras gali nagrinėti arba pasirūpinti, kad būtų išnagrinėta, ar šio įstatymo nuostatos buvo, yra arba gali būti pažeistos atitinkamo asmens atžvilgiu, jeigu šis asmuo paduoda jam skundą dėl bet kurios šio įstatymo nuostatos pažeidimo arba jeigu Duomenų apsaugos komisaras mano, kad toks pažeidimas gali būti padarytas.

b) Jeigu asmuo pateikia skundą Duomenų apsaugos komisarui pagal šio straipsnio 1 dalies a punktą, Duomenų apsaugos komisaras:

i) išnagrinėja skundą arba pasirūpina, kad jis būtų išnagrinėtas, nebent jis nuspręstų, kad skundas yra nerimtas ar nepagrįstas; ir

ii) jeigu jis negali per pagrįstą terminą pasiekti, kad atitinkamos šalys susitartų draugiškai dėl skundo dalyko, raštu praneša skundą pateikusiam asmeniui apie savo sprendimą dėl skundo, nurodydamas, kad jeigu skundą pateikusio asmens šis sprendimas netenkina, jis gali apskųsti jį teismui pagal šio įstatymo 26 straipsnį per 21 dieną nuo pranešimo gavimo.“

30. Šioje byloje Duomenų apsaugos komisaras padarė išvadą, kad M. Schrems skundas yra „nerimtas ir nepagrįstas“, t. y. pasmerktas nesėkmei, nes neturi teisinio pagrindo. Tad jis atsisakė nagrinėti šį skundą remdamasis būtent šiuo pagrindu.

31. Duomenų apsaugos įstatymo 11 straipsnyje reglamentuojamas asmens duomenų perdavimas už šalies teritorijos ribų. Jo 2 straipsnio a punkte numatyta:

„Jeigu per bet kurią šiame įstatyme reglamentuojamą procedūrą yra pateikiamas klausimas:

i) siekiant nustatyti, ar Europos ekonominei erdvei [(EEE)] nepriklausanti šalis ar teritorija, į kurią bus perduoti asmens duomenys, užtikrina šio straipsnio 1 dalyje minėtą adekvatų apsaugos lygį; ir

ii) Sąjunga padarė išvadą dėl nagrinėjamų duomenų perdavimų tipo,

šis klausimas bus nagrinėjamas pagal šią išvadą.“

32. Duomenų apsaugos įstatymo 11 straipsnio 2 dalies b punkte Sąjungos išvados sąvoka apibrėžiama taip:

„Šios dalies a punkte „Sąjungos išvada“ reiškia išvadą, kurią Komisija padarė <...> pagal Direktyvos [95/46] 25 straipsnio 4 arba 6 dalis per [jos] 31 straipsnio 2 dalyje numatytą procedūrą siekdama nustatyti, ar už [EEE] ribų esanti šalis ar teritorija užtikrina šio straipsnio 1 dalyje patikslintą adekvatų apsaugos lygį.“

33. Duomenų apsaugos komisaras pažymėjo, kad Sprendimas 2000/520 reiškė „Sąjungos išvadą“ pagal Duomenų apsaugos įstatymo 11 straipsnio 2 dalies a punktą, todėl pagal šį įstatymą visi klausimai, susiję su duomenų apsaugos trečiosiose šalyse, į kurias jie perduodami, adekvatumu, turi būti sprendžiami laikantis šios išvados. Kadangi tai buvo M. Schrems skundo esmė, t. y. kad asmens duomenys buvo perduodami į trečiąją šalį, kuri praktiškai neužtikrino adekvataus apsaugos lygio, Duomenų apsaugos komisaras nusprendė, kad dėl Sprendimo 2000/520 dėl „saugaus uosto“ pobūdžio ir paties šio sprendimo buvimo šis klausimas negali būti nagrinėjamas.

34. M. Schrems apskundė Duomenų apsaugos komisaro sprendimą atmesti jo skundą *High Court* (Aukščiausiasis Teisingumo Teismas). Išnagrinėjęs pagrindinėje byloje pateiktus įrodymus, minėtas teismas padarė išvadą, kad asmens duomenų elektroninis sekimas ir perėmimas atitinka būtinus ir neišvengiamus viešojo intereso tikslus, t. y. nacionalinio saugumo išlaikymo ir sunkių nusikaltimų prevencijos tikslus. *High Court* šiuo atžvilgiu nurodė, kad asmens duomenų, perduodamų iš Sąjungos į Jungtines Amerikos Valstijas, sekimu ir perėmimu siekiama teisėtų tikslų, susijusių su kova su terorizmu.

35. To paties teismo teigimu, vis dėlto E. Snowden atskleista informacija parodė, kad NSA ir kitos panašios institucijos gerokai viršijo savo įgaliojimus. Nors *Foreign Intelligence Surveillance Court* (toliau – FISC), kuris veikia pagal 1978 m. Įstatymą dėl užsienio saugumo tarnybų stebėjimo (*Foreign Intelligence Surveillance Act of 1978*) [18], vykdo priežiūrą, vis dėlto jame vykstantis procesas yra slaptas ir neparemtas rungimosi principu. Be to, greta to, kad sprendimai, susiję su galimybe susipažinti su asmens duomenimis, priimami remiantis Amerikos teise, Sąjungos piliečiai neturi jokios realios teisės būti išklausyti dėl jų duomenų sekimo ir perėmimo.

36. Iš daugelio dokumentų, pridėtų prie oficialių pareiškimų, padarytų pagrindinėje byloje, aiškiai matyti, kad daugelio E. Snowden atskleistos informacijos teisingumu neabejojama. Taigi *High Court* padarė išvadą, kad, perdavus asmens duomenis Jungtinėms Amerikos Valstijoms, siekdamos masinio nediferencijuoto duomenų sekimo ir perėmimo tikslų su jais gali susipažinti NSA ir kitos Amerikos saugumo tarnybos, pavyzdžiui, Federalinis tyrimų biuras (*Federal Bureau of Investigation (FBI)*).

37. *High Court* konstatuoja, kad pagal Airijos teisę, atsižvelgiant į konstitucinių teisių į privatų gyvenimą ir būsto neliečiamumą svarbą, reikalaujama, kad bet koks šių teisių ribojimas atitiktų įstatyme numatytus reikalavimus ir būtų proporcingas. Masinė ir nediferencijuota prieiga prie asmens duomenų niekaip neatitinka proporcingumo reikalavimo, todėl ją reikia laikyti prieštaraujančia Airijos Konstitucijai [19].

18 — Žr. šio įstatymo 702 straipsnį su pakeitimais, padarytais 2008 m. įstatymu (*Foreign Intelligence Surveillance Act of 2008*). Būtent pagal šį straipsnį NSA tvarko duomenų bazę, vadinamą PRISM (žr. 2013 m. lapkričio 27 d. *Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*).

19 — *High Court* visų pirma nurodo pagarbą žmogaus orumui ir asmens laisvei (preambulė), asmens autonomijai (40 straipsnio 3 dalies 1 ir 2 punktai), būsto neliečiamumui (40 straipsnio 5 dalis) ir šeiminio gyvenimo apsaugai (41 straipsnį).

38. High Court pažymi: tam, kad elektroninių pranešimų perėmimą būtų galima laikyti atitinkančiu Konstituciją, turi būti įrodyta, jog konkretus pranešimų perėmimas ir tam tikrų asmenų ar jų grupių sekimas yra objektyviai pateisinami nacionalinio saugumo ir nusikalstamumo užkardymo interesais ir kad yra tinkamos ir patikrinamos garantijos.

39. Todėl *High Court* nurodo, kad nors šią bylą reikia nagrinėti remiantis vien Airijos teise, kyla didelė problema dėl klausimo, ar Jungtinės Amerikos Valstijos „užtikrina adekvatų privataus gyvenimo bei pagrindinių laisvių ir teisių apsaugos lygį“, kaip tai suprantama pagal Duomenų apsaugos įstatymo 11 straipsnio 1 dalį. Remiantis tuo darytina išvada, kad pagal Airijos teisę, visų pirma pagal jos Konstitucijos reikalavimus, Duomenų apsaugos komisaras negalėjo atmesti M. Schrems skundo ir privalėjo ištirti šį klausimą.

40. Tačiau *High Court* daro išvadą, kad jo nagrinėjama byla yra susijusi su Sąjungos teisės įgyvendinimu, kaip tai suprantama pagal Chartijos 51 straipsnio 1 dalį, tad Duomenų apsaugos komisaro sprendimo teisėtumą reikia vertinti atsižvelgiant į Sąjungos teisę.

41. High Court taip paaiškina problemą, su kuria susidūrė Duomenų apsaugos komisaras. Duomenų apsaugos įstatymo 11 straipsnio 2 dalies a punkte numatyta, kad Duomenų apsaugos komisaras turi išspręsti apsaugos adekvatumo trečiojoje šalyje klausimą „pagal“ Sąjungos išvadą, kurią Europos Komisija padarė pagal Direktyvos 95/46 25 straipsnio 6 dalį. Iš to matyti, kad Duomenų apsaugos komisaras negalėjo nesilaikyti tokios išvados. Komisijai Sprendime 2000/520 konstatavus, kad Jungtinės Amerikos Valstijos užtikrina adekvatų apsaugos lygį, susijusį su įmonių, kurios laikosi „saugaus uosto“ principų, atliekamu duomenų tvarkymu, Duomenų apsaugos komisaras turi neišvengiamai atmesti skundą, kuriame nurodomas neadekvatus tokios apsaugos pobūdis.

42. Pripažinęs, jog Duomenų apsaugos komisaras šitaip parodė, kad tiksliai laikosi Direktyvos 95/46 ir Sprendimo 2000/520, *High Court* pažymi, kad iš tikrųjų M. Schrems labiau nesutinka su pačios „saugaus uosto“ sistemos sąlygomis nei su tuo, kaip Duomenų apsaugos komisaras ją taikė, ir pabrėžia, kad jis tiesiogiai neginčijo nei Direktyvos 95/46, nei Sprendimo 2000/520 galiojimo.

43. Taigi, *High Court* teigimu, esminis klausimas yra tas, ar pagal Sąjungos teisę ir atsižvelgiant visų pirma į paskesnį Chartijos 7 ir 8 straipsnių įsigaliojimą, Duomenų apsaugos komisaras yra absoliučiai saistomas Sprendime 2000/520 padarytos Komisijos išvados, susijusios su asmens duomenų apsaugos srities teisės ir praktikos tinkamu pobūdžiu Jungtinėse Amerikos Valstijose.

44. Be to, *High Court* patikslina, kad jo nagrinėjamame ieškinyje nepateiktas joks kaltinimas dėl pačių *Facebook Ireland* ir *Facebook USA* veiksmų. Minėtas teismas atkreipė dėmesį į tai, kad Sprendimo 2000/520 3 straipsnio 1 dalies b punktas, kuriame kompetentingoms nacionalinėms institucijoms leidžiama įpareigoti įmonę sulaikyti duomenų srautus į trečiąją šalį, yra taikomas tik tokiomis aplinkybėmis, kai skundas yra paduodamas dėl atitinkamos įmonės elgesio, o šioje byloje nagrinėjamu atveju taip nebuvo.

45. Taigi *High Court* pažymi, kad tikrasis kaltinimas yra pateiktas ne dėl paties *Facebook USA* elgesio, bet dėl to, kad Komisija laikėsi nuomonės, kad Jungtinių Valstijų duomenų apsaugos srities teise ir praktika užtikrinama adekvati apsauga, nors E. Snowden atskleisti duomenys aiškiai parodo, kad Amerikos valdžios institucijos gali masiškai ir nediferencijuotai susipažinti su Sąjungos teritorijoje gyvenančių asmenų asmens duomenimis [20].

20 — *High Court* šiuo atžvilgiu nurodo, kad pagrindinis argumentas, kurį jam pateikė M. Schrems, buvo susijęs su teiginiu, kad, atsižvelgiant į E. Snowden neseniai atskleistą informaciją ir tai, kad Jungtinių Amerikos Valstijų saugumo tarnyboms buvo dideliu mastu pateikiami asmens duomenys, Duomenų apsaugos komisaras negalėjo padaryti pagrįstos išvados, kad šioje trečiojoje šalyje yra adekvatus šių duomenų apsaugos lygis.

46. Šiuo klausimu *High Court* mano, kad sunku suvokti, kaip Sprendimas 2000/520 praktiškai galėtų atitikti Chartijos 7 ir 8 straipsnių reikalavimus, *a fortiori* jeigu atsižvelgiama į principus, kuriuos Teisingumo Teismas suformulavo Sprendime *Digital Rights Ireland ir kt.*[21] Visų pirma Chartijos 7 straipsnyje numatyta ir valstybių narių tradicijoms bendroms esminėms vertybėms būdinga garantija būtų pažeista, jeigu viešosios valdžios institucijoms būtų leidžiama atsitiktinai ir bendrai susipažinti su elektroniniais pranešimais, neprivalant pateikti objektyvių motyvų, grindžiamų nacionalinio saugumo ar nusikalstamumo prevencijos priežastimis, konkrečiai susijusiomis su konkrečiais individais, ir nepateikiant jokios tinkamos ir patikrinamos garantijos. Kadangi, kaip matyti iš M. Schrems ieškinio, Sprendimas 2000/520 galėtų būti *in abstracto* nesuderinamas su Chartijos 7 ir 8 straipsniais, Teisingumo Teismas galėtų manyti, kad Direktyvą 95/46, visų pirma jos 25 straipsnio 6 dalį, ir Sprendimą 2000/520 galima aiškinti taip, kad nacionalinėms institucijoms leidžiama pačioms atlikti savo tyrimus siekiant nustatyti, ar asmens duomenų perdavimas į trečiąją šalį ir jų laikymas ten atitinka iš Chartijos 7 ir 8 straipsnių kylančius reikalavimus.

47. Šiomis aplinkybėmis *High Court* nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„Ar atsižvelgiant į Europos Sąjungos pagrindinių teisių chartijos 7, 8 ir 47 straipsnius ir nepažeidžiant to, kas numatyta Direktyvos 95/46 25 straipsnio 6 dalies nuostatose, Duomenų apsaugos pareigūnas, nagrinėdamas skundą, susijusį su asmens duomenų perdavimu trečiajai šaliai (šiuo atveju – Jungtinėms Amerikos Valstijoms), kurios įstatymuose ir praktikoje, pareiškėjo teigimu, nenumatyta adekvačių atitinkamo asmens apsaugos priemonių, yra absoliučiai saistomas priešingos Sąjungos išvados, padarytos Sprendime 2000/520?

Jei taip nėra, ar šis pareigūnas gali arba privalo pats ištirti šį klausimą, atsižvelgdamas į per laikotarpį nuo tada, kai minėtas Sprendimas 2000/520 buvo pirmą kartą paskelbtas, pasikeitusias faktines aplinkybes?“

II – **Analizė**

48. High Court pateiktais dviem klausimais Teisingumo Teismo prašoma patikslinti nacionalinių priežiūros institucijų turimus įgaliojimus, kai jos nagrinėja skundą, susijusį su asmens duomenų perdavimu trečiojoje šalyje įsikūrusiai įmonei, ir kai siekiant pagrįsti šį skundą teigiama, kad ši trečioji šalis neužtikrina adekvataus perduodamų duomenų apsaugos lygio, nors Komisija, remdamasi Direktyvos 95/46 25 straipsnio 6 dalimi, priėmė sprendimą, kuriame pripažino šios trečiosios šalies užtikrinamos apsaugos lygį adekvačiu.

49. Reikia pabrėžti, kad skundą, kurį M. Schrems pateikė Duomenų apsaugos komisarui, sudaro du aspektai. Juo siekiama ginčyti *Facebook Ireland* asmens duomenų perdavimą bendrovei *Facebook USA*. M. Schrems reikalauja šį perdavimą nutraukti, nes, jo teigimu, Jungtinės Amerikos Valstijos neužtikrina adekvataus pagal „saugaus uosto“ sistemą perduodamų asmens duomenų apsaugos lygio. Tiksliau kalbant, jis kaltina šią trečiąją šalį įdiegus PRISM programą, pagal kurią NSA leidžiama laisvai gauti masinius duomenis, saugomus Jungtinėse Amerikos Valstijose esančiuose serveriuose. Taigi skundas yra konkrečiai susijęs su *Facebook Ireland* turimų asmens duomenų perdavimu *Facebook USA*, pažeidžiant bendrą pagal „saugaus uosto“ sistemą užtikrinamą tokių duomenų apsaugos lygį.

50. Duomenų apsaugos komisaro nuomone, vien tai, kad yra Komisijos sprendimas, kuriuo pripažinta, kad Jungtinės Amerikos Valstijos pagal „saugaus uosto“ sistemą užtikrina adekvatų apsaugos lygį, neleidžia tirti skundo.

21 — C-293/12 ir C-594/12, EU:C:2014:238, 65–69 punktai.

51. Taigi reikia kartu išnagrinėti du klausimus, kuriais iš esmės siekiama sužinoti, ar Direktyvos 95/46 28 straipsnį, aiškinamą atsižvelgiant į Chartijos 7 ir 8 straipsnius, būtina aiškinti taip, kad jeigu pagal šios direktyvos 25 straipsnio 6 dalį yra priimtas Komisijos sprendimas, nacionalinė priežiūros institucija negali tirti skundo, kuriame teigiama, kad trečioji šalis neužtikrina adekvataus perduodamų asmens duomenų apsaugos lygio, ir prireikus sustabdyti ginčijamą duomenų perdavimą.

52. Chartijos 7 straipsnyje užtikrinama teisė į privataus gyvenimo gerbimą, o Chartijos 8 straipsnyje aiškiai skelbiama teisė į asmens duomenų apsaugą. Pastarojo straipsnio 2 ir 3 dalyse patikslinta, kad tokie duomenys turi būti tvarkomi teisingai, nurodytais tikslais ir tik atitinkamam asmeniui sutikus ar kitais įstatyme nustatytais teisėtais pagrindais, kad kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis ir teisę į tai, kad jie būtų ištaisomi, be to, ten nurodyta, kad nepriklausoma institucija kontroliuoja, kaip laikomasi šių taisyklių.

A – *Dėl nacionalinių priežiūros institucijų įgaliojimų esant Komisijos sprendimui dėl adekvatumo*

53. Kaip savo pastabose nurodo M. Schrems, svarbiausias klausimas pagal pagrindinėje byloje nagrinėjamą skundą yra susijęs su *Facebook Ireland* turimų asmens duomenų perdavimu *Facebook USA* atsižvelgiant į NSA ir kitų Amerikos saugumo agentūrų bendrą galimybę susipažinti su *Facebook USA* saugomais duomenimis pagal įgaliojimus, kurie joms suteikti pagal JAV teisės aktus.

54. M. Schrems teigimu, gavusi skundą, kuriuo siekiama paneigti išvadą, kad trečioji šalis užtikrina adekvatų perduotų duomenų apsaugos lygį, nacionalinė priežiūros institucija, jeigu turi duomenų, patvirtinančių šiame skunde pateiktų kaltinimų pagrįstumą, yra įgaliota įpareigoti šiame skunde nurodytą įmonę sulaikyti atliekamą duomenų perdavimą.

55. Atsižvelgiant į Duomenų apsaugos komisaro pareigas saugoti pagrindines M. Schrems teises, M. Schrems teigia, kad Duomenų apsaugos komisaras privalo ne tik tirti skundą, bet ir, jeigu jis būtų patenkintas, pasinaudoti įgaliojimais sulaikyti duomenų srautus iš *Facebook Ireland* į bendrovę *Facebook USA*.

56. Tačiau Duomenų apsaugos komisaras atmetė skundą remdamasis Duomenų apsaugos įstatymo nuostatomis, kuriose yra nurodyti jo įgaliojimai. Ši išvada buvo grindžiama Duomenų apsaugos komisaro nuomone, kad jam yra privalomas Sprendimas 2000/520.

57. Vadinasi, pagrindinis klausimas šioje byloje yra tas, ar Komisijos atliktas ir Sprendime 2000/520 pateiktas apsaugos lygio adekvatumo vertinimas yra absoliučiai privalomas nacionalinei duomenų apsaugos institucijai ir neleidžia tirti argumentų, kuriais siekiama paneigti šią išvadą. Taigi prejudiciniai klausimai yra susiję su nacionalinių duomenų apsaugos institucijų tyrimo įgaliojimų apimtimi, kai yra priimtas Komisijos sprendimas dėl adekvatumo.

58. Komisijos teigimu, reikia atsižvelgti į jos ir nacionalinių duomenų apsaugos institucijų įgaliojimų tarpusavio ryšį. Nacionalinių duomenų apsaugos institucijų įgaliojimai daugiausia susiję su šios srities teisės aktų taikymu konkrečiais atvejais, o bendra Sprendimo 2000/520 taikymo peržiūra, įskaitant bet kokį sprendimą sustabdyti jo taikymą ar jį panaikinti, priklauso Komisijos kompetencijai.

59. Komisija tvirtina, kad M. Schrems nepateikė konkrečių argumentų, kurie leistų manyti, kad jam kilo tiesioginė grėsmė patirti didelę žalą dėl duomenų perdavimo iš *Facebook Ireland* bendrovei *Facebook USA*. Atvirkščiai, dėl M. Schrems išreikštų nuogąstavimų, susijusių su JAV saugumo organizacijų įdiegtomis sekimo programomis, abstraktaus ir bendro pobūdžio pažymėtina, kad jie yra tokie patys, dėl kurių Komisija inicijavo Sprendimo 2000/520 peržiūrą.

60. Komisijos teigimu, nacionalinės priežiūros institucijos kėsintųsi į įgaliojimus, kuriuos ji turi, kad iš naujo derėtųsi dėl šio sprendimo sąlygų su Jungtinėmis Amerikos Valstijomis arba prireikus – kad sustabdytų jo taikymą, jeigu jos imtųsi priemonių pagal skundus, kuriuose išreiškiami tik struktūriniai ir abstraktūs nuogąstavimai.

61. Nepritariu Komisijos nuomonei. Manau, jeigu yra sprendimas, kurį Komisija priėmė remdamasi Direktyvos 95/46 25 straipsnio 6 dalimi, jis niekaip nepanaikina ir nesumažina įgaliojimų, kuriuos nacionalinės priežiūros institucijos turi pagal šios direktyvos 28 straipsnį. Priešingai Komisijos teiginiams, jeigu nacionalinės priežiūros institucijos nagrinėja individualius skundus, mano nuomone, tai joms netrukdo, įgyvendinant savo tyrimo įgaliojimus ir nepriklausomumą, pareikšti savo nuomonę dėl bendro trečiosios šalies užtikrinamo apsaugos lygio ir iš to kildinti padarinius, kai jos priima sprendimą dėl individualių atvejų.

62. Pagal nusistovėjusią Teisingumo Teismo praktiką aiškinant Sąjungos teisės nuostatą reikia atsižvelgti ne tik į jos formuluotę, bet ir į kontekstą bei teisės akto, kuriame ji įtvirtinta, tikslus [22].

63. Iš Direktyvos 95/46 62 konstatuojamosios dalies matyti, kad „valstybėse narėse įsteigus priežiūros institucijas, savo funkcijas vykdančias visiškai nepriklausomai, šios institucijos sudarys esminę asmenų apsaugos tvarkant asmens duomenis dalį“.

64. Pagal minėtos direktyvos 28 straipsnio 1 dalies pirmą pastraipą „kiekviena valstybė narė numato, kad viena ar daugiau valdžios institucijų privalo kontroliuoti, kaip jos teritorijoje yra taikomos pagal šią direktyvą valstybių narių priimtos nuostatos“. Tos pačios direktyvos 28 straipsnio 1 dalies antroje pastraipoje nustatyta, kad „šios valdžios institucijos veikia visiškai nepriklausomai, vykdydamos joms patikėtas funkcijas“.

65. Direktyvos 95/46 28 straipsnio 3 dalyje išvardyti kiekvienos priežiūros institucijos turimi įgaliojimai, t. y. įgaliojimai tirti, įgaliojimai veiksmingai įsikišti, leidžiantys jai visų pirma laikinai arba galutinai uždrausti tvarkyti duomenis, taip pat įgaliojimai dalyvauti teismo procesuose [kreiptis į teismą], jeigu yra pažeidžiamos pagal šią direktyvą priimtos nacionalinės nuostatos, arba įgaliojimai atkreipti teismo institucijos dėmesį į šiuos pažeidimus.

66. Be to, pagal Direktyvos 95/46 28 straipsnio 4 dalies pirmą pastraipą „kiekviena priežiūros institucija nagrinėja bet kurio asmens <...> iškeltus ieškinius [pateiktus prašymus] dėl jo teisių ir laisvių apsaugos tvarkant asmens duomenis“. Šios direktyvos 28 straipsnio 4 dalies antroje pastraipoje patikslinta, kad „kiekviena priežiūros institucija taip pat nagrinėja bet kurio asmens iškeltus ieškinius [pateiktus prašymus], reikalaujant patikrinti duomenų tvarkymo teisėtumą tais atvejais, kai taikomos pagal šios direktyvos 13 straipsnį priimtos nacionalinės nuostatos“. Patikslinu, kad pagal pastarąją nuostatą valstybėms narėms leidžiama imtis teisėkūros priemonių, kuriomis apribojama tam tikrų Direktyvoje 95/46 numatytų teisių ir pareigų taikymo sritis, kai šis apribojimas yra reikalingas visų pirma dėl nacionalinio saugumo, gynybos, visuomenės saugumo ir nusikaltimų prevencijos, tyrimo, išaiškinimo ir baudžiamojo persekiojimo.

67. Kaip jau yra pažymėjęs Teisingumo Teismas, reikalavimas, kad Sąjungos normų, kuriomis reglamentuojama fizinių asmenų apsauga tvarkant asmens duomenis, laikymosi kontrolę užtikrintų nepriklausoma institucija, kyla ir iš pirminės Sąjungos teisės, visų pirma Chartijos 8 straipsnio 3 dalies ir SESV 16 straipsnio 2 dalies [23]. Jis taip pat priminė, kad „nepriklausomų priežiūros institucijų įsteigimas valstybėse narėse yra esminis asmenų apsaugos tvarkant asmens duomenis elementas“ [24].

22 — Visų pirma žr. Sprendimą *Koushkaki* (C-84/12, EU:C:2013:862, 34 punktas ir nurodyta teismo praktika).

23 — Žr. sprendimus *Komisija / Austrija* (C-614/10, EU:C:2012:631, 36 punktas) ir *Komisija / Vengrija* (C-288/12, EU:C:2014:237, 47 punktas).

24 — Visų pirma žr. sprendimus *Komisija / Vengrija* (C-288/12, EU:C:2014:237, 48 punktas ir nurodyta teismo praktika). Šiuo klausimu taip pat žr. Sprendimą *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, 68 punktas ir nurodyta teismo praktika).

68. Teisingumo Teismas taip pat jau yra nusprendęs, jog „Direktyvos 95/46 28 straipsnio 1 dalies antra pastraipa turi būti aiškinama taip, kad kompetentingos asmens duomenų priežiūros institucijos turi turėti tiek nepriklausomumo, kad galėtų vykdyti joms pavestas užduotis be išorinės įtakos. Šis nepriklausomumas reiškia, kad šios institucijos turi būti apsaugotos nuo bet kokio kišimosi ir išorinės įtakos, tiesioginės ar netiesioginės, galinčios pakreipti jų sprendimus kuria nors linkme ir taip sutrukdyti joms vykdyti pavestą užduotį nustatyti teisingą teisės į privatų gyvenimą apsaugos ir laisvo asmens duomenų judėjimo pusiausvyrą“ [25].

69. Teisingumo Teismas taip pat patikslino, kad „nacionalinių priežiūros institucijų nepriklausomumo garantija siekiama užtikrinti veiksmingą ir patikimą nuostatų, susijusių su fizinių asmenų apsauga tvarkant asmens duomenis, laikymosi kontrolę“ [26]. Ši nepriklausomumo garantija buvo nustatyta, „kad būtų sustiprinta su [šių nacionalinių priežiūros institucijų] sprendimais susijusių asmenų ir organizacijų apsauga“ [27].

70. Kaip visų pirma matyti iš Direktyvos 95/46 10 konstatuojamosios dalies ir 1 straipsnio, ja Sąjungoje siekiama „tvarkant asmens duomenis garantuoti aukštą pagrindinių laisvių ir teisių apsaugos lygį“ [28]. Teisingumo Teismo teigimu, „Direktyvos 95/46 28 straipsnyje numatytos priežiūros institucijos yra šių teisių ir pagrindinių laisvių saugotojos“ [29].

71. Atsižvelgiant į nacionalinių priežiūros institucijų atliekamo vaidmens svarbą fizinių asmenų apsaugos tvarkant asmens duomenis srityje, jų įgaliojimai imtis veiksmų turi išlikti nepakitę, net jeigu Komisija yra priėmusi sprendimą remdamasi Direktyvos 95/46 25 straipsnio 6 dalimi.

72. Šiuo atžvilgiu reikia pabrėžti, jog niekas nerodo, kad asmens duomenų perdavimo į trečiąsias šalis sistemos nepatenka į Chartijos 8 straipsnio 3 dalies materialinę taikymo sritį, kurioje aukščiausiu Sąjungos teisės normų hierarchijos lygiu įtvirtinama nepriklausomos institucijos atliekamos priežiūros, susijusios su asmens duomenų apsaugos taisyklių laikymusi, svarba.

73. Jeigu Komisijos priimti sprendimai būtų absoliučiai privalomi nacionalinėms priežiūros institucijoms, taip būtų neišvengiamai ribojamas jų visiškas nepriklausomumas. Atsižvelgiant į nacionalinių priežiūros institucijų, kaip pagrindinių teisių saugotojų, vaidmenį, jos turi galėti visiškai nepriklausomai tirti joms paduotus skundus, siekdamos viršesnio asmenų apsaugos tvarkant asmens duomenis tikslo.

74. Be to, kaip per teismo posėdį teisingai pažymėjo Belgijos vyriausybė ir Europos Parlamentas, tarp Direktyvos 95/46 IV skyriaus, susijusio su asmens duomenų perdavimu į trečiąsias šalis, ir jos VI skyriaus, visų pirma susijusio su nacionalinių priežiūros institucijų vaidmeniu, nėra jokio hierarchinio ryšio. Jos VI skyriuje nėra jokios nuostatos, kuri leistų manyti, kad nuostatos, susijusios su nacionalinėmis priežiūros institucijomis, kaip nors priklauso nuo Direktyvos 95/46 IV skyriuje įtvirtintų atskirų nuostatų, susijusių su duomenų perdavimu.

75. Atvirkščiai, iš minėtos direktyvos 25 straipsnio 1 dalies, esančios jos IV skyriuje, aiškiai matyti, kad leidimas perduoti asmens duomenis į trečiąją šalį, užtikrinančią adekvatų apsaugos lygį, duodamas tik su išlyga, kad yra laikomasi nacionalinių nuostatų, priimtų pagal kitas šios direktyvos nuostatas.

25 — Visų pirma žr. Sprendimą *Komisija / Vengrija* (C-288/12, EU:C:2014:237, 51 punktas ir nurodyta teismo praktika).

26 — Sprendimas *Komisija / Vokietija* (C-518/07, EU:C:2010:125, 25 punktas).

27 — Ten pat.

28 — Ten pat, 22 punktas ir nurodyta teismo praktika.

29 — Ten pat, 23 punktas. Šiuo klausimu taip pat žr. sprendimus *Komisija / Austrija* (C-614/10, EU:C:2012:631, 52 punktas) ir *Komisija / Vengrija* (C-288/12, EU:C:2014:237, 53 punktas).

76. Šiuo atžvilgiu reikia priminti, kad pagal šią nuostatą valstybės narės savo nacionalinės teisės aktuose turi numatyti, kad asmens duomenys, kurie yra tvarkomi arba kuriuos numatoma tvarkyti po perdavimo, gali būti perduodami į trečiąją šalį tik jeigu atitinkama trečioji šalis užtikrina adekvatų apsaugos lygį, su sąlyga, kad yra laikomasi nacionalinių nuostatų, priimtų pagal kitas Direktyvos 95/46 nuostatas.

77. Pagal minėtos direktyvos 28 straipsnio 1 dalį nacionalinės priežiūros institucijos privalo prižiūrėti, kaip kiekvienos valstybės narės teritorijoje yra taikomos pagal šią direktyvą valstybių narių priimtos nuostatos.

78. Sugretinus minėtas dvi nuostatas galima manyti, kad Direktyvos 95/46 25 straipsnio 1 dalyje įtvirtinta taisyklė, pagal kurią asmens duomenys gali būti perduodami tik jeigu trečioji šalis, į kurią jie perduodami, užtikrina adekvatų šių duomenų apsaugos lygį, yra tarp taisyklių, kurių taikymą turi prižiūrėti nacionalinės priežiūros institucijos.

79. Pagal Chartijos 8 straipsnio 3 dalį nacionalinių priežiūros institucijų įgaliojimus visiškai nepriklausomai tirti skundus, kurie joms yra pateikti pagal Direktyvos 95/46 28 straipsnį, reikia aiškinti plačiai. Taigi šių įgaliojimų negali riboti Sąjungos teisės aktų leidėjo pagal šios direktyvos 25 straipsnio 6 dalį Komisijai suteikti įgaliojimai konstatuoti adekvatų trečiosios šalies užtikrinamą apsaugos lygį.

80. Atsižvelgiant į esminį nacionalinių priežiūros institucijų vaidmenį asmens duomenų apsaugos srityje, jos turi galėti tirti gautą skundą, kuriame nurodytos aplinkybės, galinčios priversti vėl suabejoti trečiosios šalies užtikrinamu apsaugos lygiu, taip pat tais atvejais, kai Komisija sprendime, priimtame remiantis Direktyvos 95/46 25 straipsnio 6 dalimi, konstatuoja, kad atitinkama trečioji šalis užtikrina adekvatų apsaugos lygį.

81. Jeigu užbaigusi atliktus tyrimus nacionalinė priežiūros institucija mano, kad ginčijamas duomenų perdavimas kenkia apsaugai, kuri turi būti suteikiama Sąjungos piliečiams tvarkant jų duomenis, ji gali sulaikyti nagrinėjamų duomenų perdavimą, nepaisydama to, kokį bendrą vertinimą Komisija yra atlikusi savo sprendime.

82. Iš tiesų pagal Direktyvos 95/46 25 straipsnio 2 dalį neginčijama, kad trečiosios šalies užtikrinamo apsaugos lygio adekvatumas vertinamas atsižvelgiant į visas tiek faktines, tiek teisines aplinkybes. Jeigu viena iš šių aplinkybių pakinta ir paaiškėja, kad dėl jos galima suabejoti trečiosios šalies užtikrinamu adekvačiu apsaugos lygiu, skundą nagrinėjanti nacionalinė priežiūros institucija turi galėti nustatyti to padarinius atsižvelgdama į ginčijamą duomenų perdavimą.

83. Aišku, kaip pažymėjo Airija, Duomenų apsaugos komisarui, kaip ir kitoms valstybės institucijoms, Sprendimas 2000/520 yra privalomas. Iš tiesų iš SESV 288 straipsnio ketvirtos pastraipos darytina išvada, kad Sąjungos institucijos priimtas sprendimas yra privalomas visas. Todėl Sprendimas 2000/520 privalomas valstybėms narėms, kurioms jis yra skirtas.

84. Šiuo atžvilgiu reikia atkreipti dėmesį, jog paties Sprendimo 2000/520 5 straipsnyje nustatyta, kad „valstybės narės ne vėliau kaip per 90 dienų po pranešimo pateikimo valstybėms narėms imasi visų priemonių, būtinų, kad būtų laikomasi šio sprendimo“. Be to, šio sprendimo 6 straipsnyje patvirtinama, kad „[jis] skirtas valstybėms narėms“.

85. Tačiau manau, kad, atsižvelgiant į minėtas Direktyvos 95/46 ir Chartijos nuostatas, privalomas Sprendimo 2000/520 poveikis nereiškia, kad Duomenų apsaugos komisaras negali atlikti jokio tyrimo dėl skundų, kuriuose teigiama, kad perduodant asmens duomenis į Jungtines Amerikos Valstijas pagal šį sprendimą neužtikrinamos būtinos apsaugos garantijos, kurių reikalaujama pagal Sąjungos teisę. Kitaip tariant, toks privalomasis poveikis nereiškia, kad kiekvienas tokio pobūdžio skundas turi būti atmetamas apskritai, t. y. iš karto ir visiškai neištyrus jo pagrįstumo.

86. Norėčiau pridurti, jog, be kita ko, iš Direktyvos 95/46 25 straipsnio struktūros matyti, kad išvadą dėl to, ar trečioji šalis užtikrina adekvatų apsaugos lygį, ar ne, gali padaryti valstybės narės arba Komisija. Taigi ši kompetencija yra pasidalijamoji.

87. Iš šios direktyvos 25 straipsnio 6 dalies matyti, kad jeigu Komisija konstatuoja, kad trečioji šalis užtikrina adekvatų apsaugos lygį, kaip tai suprantama pagal šios direktyvos 25 straipsnio 2 dalį, valstybės narės turi imtis būtinų priemonių, kad laikytųsi Komisijos sprendimo.

88. Taigi, jeigu tokiu sprendimu leidžiama asmens duomenis perduoti į trečiąją šalį, kurios teikiamos apsaugos lygį Komisija laiko adekvačiu, valstybės narės iš principo turi leisti, kad šiuos duomenis perduotų jų teritorijoje įsteigtos įmonės.

89. Tačiau pagal Direktyvos 95/46 25 straipsnį ne vien Komisija gali pripažinti, ar perduodamų asmens duomenų apsaugos lygis yra adekvatus, ar ne. Šio straipsnio struktūra liudija tai, kad vaidmuo šioje srityje tenka ir valstybėms narėms. Komisijos sprendimui iš tiesų tenka reikšmingas vaidmuo vienodinant valstybėse narėse taikomas duomenų perdavimo sąlygas. Tačiau šis suvienodinimas galioja tik kol šis pripažinimas nėra paneigtas.

90. Manau, argumentas dėl asmens duomenų perdavimo į trečiąją šalį sąlygų būtino vienodinimo tokiu atveju, kaip nagrinėjamasis pagrindinėje byloje, nebegali būti pateikiamas ne tik tuomet, kai Komisijai pranešama, kad jos išvada yra kritikuotina, bet ir tuo atveju, kai ji pati pareiškia tokią kritiką ir veda derybas siekdama ištaisyti padėtį.

91. Vertindamos trečiosios šalies užtikrinamos apsaugos lygio adekvatumą arba neadekvatumą valstybės narės ir Komisija taip pat gali bendradarbiauti. Šiuo atžvilgiu Direktyvos 95/46 25 straipsnio 3 dalyje numatyta, kad „valstybės narės ir Komisija praneša vienos kitoms apie tokius atvejus, kai jos mano, kad kuri nors trečioji šalis neužtikrina adekvataus apsaugos lygio, kaip numatyta šio straipsnio 2 dalyje“. Kaip pažymi Parlamentas, tai rodo, kad valstybės narės ir Komisija atlieka lygiavertį vaidmenį taisydamos padėtį tais atvejais, kai trečioji šalis neužtikrina adekvataus apsaugos lygio.

92. Sprendimo dėl adekvatumo tikslas – leisti perduoti asmens duomenis į atitinkamą trečiąją šalį. Tai nereiškia, kad Sąjungos piliečiai negali pateikti nacionalinėms priežiūros institucijoms prašymų apsaugoti jų asmens duomenis. Šiuo atžvilgiu reikia pabrėžti, kad Direktyvos 95/46 28 straipsnio 4 dalies pirmoje pastraipoje, pagal kurią „kiekviena priežiūros institucija nagrinėja bet kurio asmens <...> iškeltus ieškinius [pateiktus prašymus] dėl jo teisių ir laisvių apsaugos tvarkant asmens duomenis“, nenumatyta šio principo išimtis, jeigu Komisija yra priėmusi sprendimą pagal šios direktyvos 25 straipsnio 6 dalį.

93. Taigi, jeigu pagal Komisijos sprendimą, priimtą jai naudojantis minėta nuostata suteiktais įgyvendinimo įgaliojimais, leidžiama perduoti asmens duomenis į trečiąją šalį, vis dėlto dėl šio sprendimo valstybės narės, visų pirma jų nacionalinės priežiūros institucijos, neturi netekti visų įgaliojimų, ir šie įgaliojimai netgi neturi būti ribojami, jeigu jos susiduria su kaltinimais dėl pagrindinių teisių pažeidimo.

94. Nacionalinė priežiūros institucija turi galėti naudotis Direktyvos 95/46 28 straipsnio 3 dalyje numatytais įgaliojimais, įskaitant įgaliojimus laikinai arba galutinai uždrausti tvarkyti asmens duomenis. Nors tarp šioje nuostatoje išvardytų įgaliojimų aiškiai nenumatyti įgaliojimai, susiję su duomenų perdavimu iš valstybės narės į trečiąją šalį, mano nuomone, tokį perdavimą reikia laikyti

duomenų tvarkymu [30]. Be to, kaip matyti iš šios nuostatos teksto, įgaliojimų sąrašas nėra išsamus. Bet kuriuo atveju atsižvelgiant į esminį vaidmenį, kurį nacionalinės priežiūros institucijos atlieka Direktyva 95/46 nustatytoje sistemoje, jos turi turėti įgaliojimus sulaikyti duomenų perdavimą, jeigu įrodyta žala pagrindinėms teisėms arba šios žalos grėsmė.

95. Norėčiau pridurti, kad jeigu tokiomis aplinkybėmis, kokios susiklostė šioje byloje, iš nacionalinės priežiūros institucijos būtų atimti tyrimo įgaliojimai, tai prieštarautų ne tik nepriklausomumo principui, bet ir Direktyvos 95/46 tikslui, kuris matyti iš jos 1 straipsnio 1 dalies.

96. Kaip yra pažymėjęs Teisingumo Teismas, „iš Direktyvos 95/46 3, 8 ir 10 konstatuojamųjų dalių matyti, kad derindamas valstybių narių teisės aktus Sąjungos teisės aktų leidėjas siekė palengvinti asmens duomenų judėjimą, užtikrindamas asmenų pagrindinių teisių, visų pirma teisės į privatų gyvenimą, aukšto lygio apsaugą Sąjungoje Šios direktyvos 1 straipsnyje numatyta, kad valstybės narės turi užtikrinti fizinių asmenų pagrindinių teisių ir laisvių, ypač jų privataus gyvenimo tvarkant asmens duomenis, apsaugą“ [31].

97. Taigi Direktyvos 95/46 nuostatas reikia aiškinti pagal jos tikslą, kuriuo tvarkant asmens duomenis Sąjungoje siekiama užtikrinti aukštą fizinių asmenų pagrindinių laisvių ir teisių, visų pirma jų privataus gyvenimo apsaugos, lygį.

98. Šio tikslo ir valstybių narių vaidmens, kurį jos turi atlikti jo siekdamos, svarba reiškia, kad jeigu dėl ypatingų aplinkybių kyla rimta abejonė, ar, perduodant asmens duomenis į trečiąją šalį, yra laikomasi Chartijoje užtikrinamų pagrindinių teisių, valstybės narės, taigi ir jų nacionalinės priežiūros institucijos, negali būti absoliučiai saistomos Komisijos priimto sprendimo dėl adekvatumo.

99. Teisingumo Teismas jau yra nusprendęs, kad „Direktyvos 95/46 nuostatas, reglamentuojančias asmens duomenų tvarkymą ir galinčias pažeisti pagrindines laisves, visų pirma teisę į privatų gyvenimą, būtina aiškinti atsižvelgiant į pagrindines teises, kurios, vadovaujantis nusistovėjusia teismo praktika, yra sudedamoji bendrųjų teisės principų, kurių laikymąsi užtikrina Teisingumo Teismas, ir kurios dabar yra įtrauktos į Chartiją, dalis“ [32].

100. Be to, reikia nurodyti teismo praktiką, pagal kurią „valstybės narės ne tik privalo savo nacionalinę teisę aiškinti taip, kad ji atitiktų Sąjungos teisę, bet ir nesivadovauti tokiu antrinės teisės akto aiškinimu, kuriuo būtų pažeidžiamos Sąjungos teisės sistemos saugomos pagrindinės teisės arba kiti bendrieji Sąjungos teisės principai“ [33].

101. Teisingumo Teismas Sprendime *N. S. ir kt.* [34] taip pat yra nusprendęs, kad „Reglamento [(EB)] Nr. 343/2003 [35] taikymas remiantis nenuginčijama prezumpcija, jog įprastomis aplinkybėmis už prieglobsčio prašytojo prašymo nagrinėjimą atsakingoje valstybėje narėje bus gerbiamos jo pagrindinės teisės, yra nesuderinamas su valstybės narės pareiga aiškinti ir taikyti Reglamentą Nr. 343/2003 atsižvelgiant į pagrindines teises“ [36].

30 — Žr. generalinio advokato P. Léger išvadą byloje *Parlamentas / Taryba ir Komisija* (C-317/04, EU:C:2005:710, 92–95 punktai). Taip pat žr. Sprendimą *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346, 56 punktas).

31 — Visų pirma žr. Sprendimą *IPI* (C-473/12, EU:C:2013:715, 28 punktas ir nurodyta teismo praktika).

32 — Visų pirma žr. Sprendimą *Google Spain ir Google* (C-131/12, EU:C:2014:317, 68 punktas ir nurodyta teismo praktika).

33 — Visų pirma žr. Sprendimą *N. S. ir kt.* (C-411/10 ir C-493/10, EU:C:2011:865, 77 punktas ir nurodyta teismo praktika).

34 — C-411/10 ir C-493/10, EU:C:2011:865.

35 — 2003 m. vasario 18 d. Tarybos reglamentas, nustatantis valstybės narės, atsakingos už trečiosios šalies piliečio vienoje iš valstybių narių pateikto prieglobsčio prašymo nagrinėjimą, nustatymo kriterijus ir mechanizmus (OL L 50, p. 1; 2004 m. specialusis leidimas lietuvių k., 19 t., 6 sk., p. 109).

36 — Šio sprendimo 99 punktas.

102. Šiuo atžvilgiu Teisingumo Teismas, nagrinėdamas valstybių narių, kaip saugių kilmės šalių, statusą viena kitos atžvilgiu teisiniais ir praktiniais klausimais, susijusiais su prieglobsčio teise, pripažino, jog reikia daryti prielaidą, kad prieglobsčio prašytojams kiekvienoje valstybėje narėje numatytas vertinimas atitinka Chartijos, 1951 m. liepos 28 d. Ženevoje pasirašytos Konvencijos dėl pabėgėlių statuso [37] ir 1950 m. lapkričio 4 d. Romoje pasirašytos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos reikalavimus. Tačiau Teisingumo Teismas yra nusprendęs, jog „negalima atmesti galimybės, kad konkrečioje valstybėje narėje faktiškai gali kilti didelių tokios sistemos veikimo problemų, o tai reiškia, kad yra rimtas pavojus, jog perdavimo tokiai valstybei narei atveju su prieglobsčio prašytojais bus elgiamasi neatsižvelgiant į jų pagrindines teises“ [38].

103. Todėl Teisingumo Teismas nusprendė, kad „Chartijos 4 straipsnį reikia aiškinti taip, kad valstybės narės, įskaitant nacionalinius teismus, privalo neperduoti prieglobsčio prašytojo „atsakingai valstybei narei“, kaip tai suprantama pagal Reglamentą Nr. 343/2003, kai negali nežinoti, kad sisteminiai prieglobsčio procedūros ir prieglobsčio prašytojų priėmimo sąlygų tokioje valstybėje narėje trūkumai yra rimta ir pagrįsta priežastis manyti, jog prašytojui kils reali nežmoniško ar žeminamo elgesio grėsmė, kaip tai suprantama pagal šią nuostatą“ [39].

104. Manau, Sprendimą *N. S. ir kt.* [40] galima pritaikyti tokiam atvejui, kaip nagrinėjamasis pagrindinėje byloje. Taigi Sąjungos išvestinės teisės aiškinimą, grindžiamą nepaneigiama prielaida, kad yra laikomasi pagrindinių teisių, – ar tai būtų valstybė narė, Komisija ar trečioji šalis, – reikia laikyti neatitinkančiu valstybių narių pareigos aiškinti ir taikyti Sąjungos išvestinę teisę laikantis pagrindinių teisių. Tad Direktyvos 95/46 25 straipsnio 6 dalyje nenustatyta tokia nepaneigiama pagrindinių teisių laikymosi prielaida, kiek tai susiję su Komisijos atliekamu trečiosios šalies užtikrinamo apsaugos lygio adekvatumo vertinimu. Atvirkščiai, prielaidą, kuria yra grindžiama ši nuostata, kad perduodant duomenis į trečiąją šalį yra laikomasi pagrindinių teisių, reikia laikyti prielaida, kurią galima paneigti [41]. Todėl minėtos nuostatos nereikia aiškinti kaip paneigiančios garantijas, visų pirma įtvirtintas Direktyvos 95/46 28 straipsnio 3 dalyje ir Chartijos 8 straipsnio 3 dalyje, kuriomis siekiama apsaugoti teisę į asmens duomenų apsaugą ir užtikrinti jos laikymąsi.

105. Taigi iš minėto sprendimo [42] reikia daryti išvadą, kad jeigu trečiojoje šalyje, į kurią perduodami asmens duomenys, yra nustatoma sisteminių trūkumų, valstybės narės turi galėti imtis būtinų priemonių, kad apsaugotų Chartijos 7 ir 8 straipsniuose ginamas pagrindines teises.

106. Be to, kaip savo pastabose pažymi Italijos vyriausybė, Komisijos sprendimo dėl adekvatumo priėmimas negali sumažinti Sąjungos piliečių apsaugos tvarkant jų asmens duomenis, kai jie yra perduodami į trečiąją šalį, palyginti su apsaugos lygiu, taikomu šiems asmenims, kai jų duomenys yra tvarkomi Sąjungos viduje. Todėl nacionalinės priežiūros institucijos turi galėti įsikišti ir įgyvendinti savo įgaliojimus dėl duomenų perdavimo į trečiąsias šalis, dėl kurių priimtas sprendimas dėl adekvatumo. Antraip Sąjungos piliečiai būtų apsaugoti mažiau, nei tvarkant jų duomenis Sąjungos viduje.

107. Taigi Komisijos sprendimo priėmimas pagal Direktyvos 95/46 25 straipsnio 6 dalį reiškia tik tai, kad yra panaikinamas bendras draudimas eksportuoti asmens duomenis į trečiąją šalį, kuri neužtikrina apsaugos lygio, panašaus į užtikrinamą šioje direktyvoje. Kitaip tariant, taip nėra sukuriama speciali išimtinė sistema, kuri Sąjungos piliečius apsaugotų mažiau, nei pagal šioje direktyvoje numatytą bendrą Sąjungos viduje cirkuliuojančių duomenų tvarkymo sistemą.

37 — *Jungtinių Tautų sutarčių rinkinys*, 189 t., p. 150, Nr. 2545 (1954 m.).

38 — Žr. Sprendimą *N. S. ir kt.* (C-411/10 ir C-493/10, EU:C:2011:865, 80 punktas).

39 — Ten pat, 81 punktas.

40 — Ten pat, 94 punktas.

41 — C-411/10 ir C-493/10, EU:C:2011:865.

42 — Šio sprendimo 104 punktas.

108. Teisingumo Teismas Sprendimo *Lindqvist*[43] 63 punkte tikrai nurodė, kad „Direktyvos 95/46 IV skyriuje, kuriame yra 25 straipsnis, <...> įtvirtinama speciali tvarka“. Tačiau, mano nuomone, tai nereiškia, kad ši sistema turi suteikti mažesnę apsaugą. Atvirkščiai, norint pasiekti Direktyvos 95/46 1 straipsnio 1 dalyje įtvirtintą duomenų apsaugos tikslą, jos 25 straipsnyje valstybėms narėms ir Komisijai nustatomi tam tikri įpareigojimai[44], o 25 straipsnyje įtvirtinamas principas, pagal kurį, jeigu trečioji šalis neužtikrina adekvataus apsaugos lygio, asmens duomenų perdavimą į šią šalį reikia uždrausti[45].

109. Konkrečiau kalbant apie „saugaus uosto“ sistemą, pažymėtina, kad Komisija numato nacionalinių priežiūros institucijų įsikišimą ar jų galimybę sulaikyti duomenų srautą tik kaip apibrėžta Sprendimo 2000/520 3 straipsnio 1 dalies b punkte.

110. Pagal minėto sprendimo 8 konstatuojamąją dalį, „siekiant skaidrumo ir norint apsaugoti valstybių narių kompetentingų institucijų gebėjimą užtikrinti asmenų apsaugą tvarkant jų asmens duomenis, šiame sprendime būtina tiksliai apibrėžti išskirtines aplinkybes, kuriomis būtų pateisinamas tam tikrų ypatingų duomenų srautų perdavimo sulaikymas, nepaisant to, kad yra pakankama apsauga“.

111. Šioje byloje buvo diskutuojama būtent dėl minėto sprendimo 3 straipsnio 1 dalies b punkto taikymo. Taigi pagal šią nuostatą nacionalinės priežiūros institucijos gali priimti sprendimą dėl duomenų srauto sulaikymo tais atvejais, kai „yra didelė tikimybė, kad Principai yra pažeisti; galima pagrįstai manyti, kad naudojant atitinkamą vykdymo priežiūros mechanizmą nesiimama ar nebus imtasi pakankamų ir savalaikių priemonių išspręsti kilusią problemą; tęsiant duomenų perdavimą susidarytų neišvengiamas pavojus rimtai pakenkti duomenų subjektams; valstybės narės kompetentingos institucijos ėmėsi pagrįstų pastangų tokiomis aplinkybėmis pranešti apie tai organizacijai ir suteikti jai galimybę nurodyti priežastis“.

112. Minėtoje nuostatoje nustatyta daugiau sąlygų, kurias šalys nagrinėjant šią bylą aiškina įvairiai[46]. Nedetalizuojant šių aiškinimų, darytina išvada, kad šiomis sąlygomis yra griežtai apibrėžiami nacionalinių priežiūros institucijų įgaliojimai sulaikyti duomenų srautus.

113. Tačiau, priešingai Komisijos teiginiams, Sprendimo 2000/520 3 straipsnio 1 dalies b punktą reikia aiškinti laikantis pagal Direktyvą 95/46 siekiamo asmens duomenų apsaugos tikslo, taip pat atsižvelgiant į Chartijos 8 straipsnį. Reikalavimas pateikti pagrindines teises atitinkantį aiškinimą rodo, kad ši nuostata turi būti aiškinama plačiai.

114. Remiantis tuo darytina išvada, kad, mano nuomone, Sprendimo 2000/520 3 straipsnio 1 dalies b punkte numatytos sąlygos negali kliudyti nacionalinei priežiūros institucijai visiškai nepriklausomai įgyvendinti įgaliojimus, kurie jai suteikti pagal Direktyvos 95/46 28 straipsnio 3 dalį.

115. Kaip per teismo posėdį iš esmės nurodė Belgijos ir Austrijos vyriausybės, Sprendimo 2000/520 3 straipsnio 1 dalies b punkte numatyta ekstremali išeitis yra tokia siaura, kad ją sunku įgyvendinti praktiškai. Jame reikalaujama kumuliacinių kriterijų ir pernelyg aukštai užkeliama kartelė. Tačiau, atsižvelgiant į Chartijos 8 straipsnio 3 dalį, negali būti, kad nacionalinių priežiūros institucijų diskrecija, susijusi su prerogatyvomis, kylančiomis iš Direktyvos 95/46 28 straipsnio 3 dalies, būtų ribojama taip, kad jos nebegalėtų ja naudotis.

43 — C-101/01, EU:C:2003:596.

44 — 65 punktas.

45 — 64 punktas.

46 — Kaip teigia M. Schrems, pirmoji sąlyga, pagal kurią „yra didelė tikimybė, kad Principai yra pažeisti“, nėra įvykdyta. Tačiau neteigiama, kad *Facebook USA*, kaip įsipareigojimą prisiėmusi bendrovė, kuriai yra perduodami duomenys, pati pažeidė „saugaus uosto“ principus, nes JAV valdžios institucijos masiškai ir nediferencijuotai gavo jos turimus duomenis. Iš tiesų „saugaus uosto“ principai yra aiškiai ribojami Amerikos teisės, kuri Sprendimo 2000/520 I priedo ketvirtoje pastraipoje apibrėžiama pateikiant nuorodą į įstatymų ir kitų teisės aktų bei teismų praktikos tekstus.

116. Šiuo atžvilgiu Parlamentas teisingai pažymėjo, kad būtent Sąjungos teisės aktų leidėjas nusprendė, kokius įgaliojimus reikia perduoti nacionalinėms priežiūros institucijoms. Tačiau įgyvendinimo įgaliojimai, kuriuos Sąjungos teisės aktų leidėjas suteikė Komisijai pagal Direktyvos 95/46 25 straipsnio 6 dalį, nepaveikia įgaliojimų, kuriuos šis teisės aktų leidėjas suteikė nacionalinėms priežiūros institucijoms pagal šios direktyvos 28 straipsnio 3 dalį. Kitaip tariant, Komisija neturi kompetencijos riboti nacionalinių priežiūros institucijų įgaliojimų.

117. Todėl, siekiant užtikrinti tinkamą fizinių asmenų teisių apsaugą tvarkant asmens duomenis, nacionalinės priežiūros institucijos, jeigu yra pateikiami kaltinimai šių teisių pažeidimu, turi būti įgaliotos atlikti tyrimus. Jeigu užbaigusios šiuos tyrimus minėtos institucijos mano, kad trečiojoje šalyje, kuriai taikomas sprendimas dėl adekvatumo, yra rimtų požymių, rodančių, kad pažeidžiama Sąjungos piliečių teisė į jų asmens duomenų apsaugą, jos turi galėti sulaikyti duomenų perdavimą toje trečiojoje šalyje įsteigtam duomenų gavėjui.

118. Kitaip tariant, nacionalinės priežiūros institucijos turi galėti atlikti savo tyrimus ir prireikus sulaikyti duomenų perdavimą, nepaisydamos Sprendimo 2000/520 3 straipsnio 1 dalies b punkte nustatytų ribojamųjų sąlygų.

119. Be to, turėdamos Direktyvos 95/46 28 straipsnio 3 dalyje numatytus įgaliojimus keiptis į teismą nacionalinių nuostatų, priimtų pagal šią direktyvą, pažeidimų atveju arba įgaliojimus atkreipti teismo institucijos dėmesį į šiuos pažeidimus, nacionalinės priežiūros institucijos, sužinojusios apie faktines aplinkybes, įrodančias, kad trečioji šalis neužtikrina adekvataus apsaugos lygio, turi galėti kreiptis į nacionalinį teismą, kuris pats prireikus galėtų nuspręsti pateikti prašymą priimti prejudicinį sprendimą Teisingumo Teismui, kad šis įvertintų Komisijos sprendimo dėl adekvatumo galiojimą.

120. Iš visų šių aplinkybių matyti, kad Direktyvos 95/46 28 straipsnį, aiškinamą atsižvelgiant į Chartijos 7 ir 8 straipsnius, reikia aiškinti taip, kad Komisijos sprendimo, priimto remiantis šios direktyvos 25 straipsnio 6 dalimi, buvimas nereiškia, kad nacionalinė priežiūros institucija negali tirti skundo, kuriame teigiama, kad trečioji šalis neužtikrina adekvataus perduodamų asmens duomenų apsaugos lygio, ir prireikus sulaikyti šių duomenų perdavimą.

121. Nors *High Court* savo sprendime pabrėžia, kad M. Schrems formaliai neginčijo nei Direktyvos 95/46, nei Sprendimo 2000/520 galiojimo, iš jo sprendimo dėl prašymo priimti prejudicinį sprendimą matyti, kad pagrindiniais M. Schrems argumentais siekiama suabejoti dėl išvados, kad Jungtinės Amerikos Valstijos pagal „saugaus uosto“ sistemą užtikrina adekvatų perduodamų asmens duomenų apsaugos lygį.

122. Be to, iš Duomenų apsaugos komisaro pastabų matyti, kad M. Schrems skunde tiesiogiai kvestionuojamas Sprendimas 2000/520. Pateikdamas savo skundą M. Schrems siekė ginčyti pačios „saugaus uosto“ sistemos sąlygas ir veikimą remdamasis tuo, jog masinis asmens duomenų, perduodamų į Jungtines Amerikos Valstijas, sekimas įrodo, kad pagal šioje trečiojoje šalyje galiojančią teisę ir praktiką nėra tikros šių duomenų apsaugos.

123. Be to, prašymą priimti prejudicinį sprendimą pateikęs teismas pats pažymi, kad Chartijos 7 straipsnyje numatytai garantijai ir valstybių narių konstitucinėms tradicijoms bendroms esminėms vertybėms būtų pakenkta, jeigu valdžios institucijoms būtų leista atsitiktinai ir bendrai susipažinti su elektroniniais pranešimais, nesant reikalo nurodyti objektyvių motyvų, grindžiamų nacionalinio saugumo ar nusikalstamumo prevencijos priežastimis, konkrečiai susijusiomis su atitinkamais individais, ir nepateikiant jokios tinkamos bei patikrinamos garantijos[47]. Taip prašymą priimti prejudicinį sprendimą pateikęs teismas netiesiogiai abejoja Sprendimo 2000/520 galiojimu.

47 — Sprendimo dėl prašymo priimti prejudicinį sprendimą 24 punktas.

124. Taigi vertinant, ar Jungtinės Amerikos Valstijos pagal „saugaus uosto“ sistemą užtikrina adekvatų perduodamų asmens duomenų apsaugos lygį, neišvengiamai reikia išnagrinėti šio sprendimo galiojimo klausimą.

125. Šiuo atžvilgiu reikia pažymėti, kad, atsižvelgiant į Teisingumo Teismo ir nacionalinių teismų bendradarbiavimo priemonę, įtvirtintą SESV 267 straipsnyje, nors Teisingumo Teismas gauna prejudicinį klausimą tik dėl Sąjungos teisės išaiškinimo, esant tam tikroms ypatingoms aplinkybėms jis gali patikrinti, ar išvestinės teisės nuostatos galioja.

126. Taigi Teisingumo Teismas jau daug kartų yra savo iniciatyva pripažinęs negaliojančiu aktą, kurį buvo prašoma tik išaiškinti [48]. Jis taip pat yra nusprendęs, jog „jeigu paaiškėja, kad tikrasis nacionalinio teismo pateiktų klausimų tikslas labiau sietinas su [Sąjungos] aktų galiojimu, o ne išaiškinimu, Teisingumo Teismui reikėtų iš karto pateikti nacionaliniam teismui savo nuomonę, neįpareigojant laikytis visiškai formalių procesą prailginančių reikalavimų, neatitinkančių paties [SESV 267] straipsniu nustatytų mechanizmų pobūdžio“ [49]. Be to, Teisingumo Teismas jau yra pareiškęs, kad prašymą priimti prejudicinį sprendimą pateikusio teismo išreikštas abejones dėl išvestinės teisės akto atitikties taisyklėms, susijusioms su pagrindinių teisių apsauga, reikia suprasti kaip abejones dėl šio akto galiojimo Sąjungos teisės atžvilgiu [50].

127. Be to, reikia priminti, jog iš Teisingumo Teismo praktikos taip pat matyti, kad Sąjungos institucijų, įstaigų ir organų aktams taikoma galiojimo prezumpcija, o tai reiškia, kad jie sukelia teisinių pasekmių, kol nėra pripažinti netekusiais galios, panaikinti patenkinus ieškinį dėl panaikinimo, paskelbti negaliojančiais išnagrinėjus prašymą priimti prejudicinį sprendimą arba netaikytinais patenkinus neteisėtumu grindžiamą prieštaravimą. Tik Teisingumo Teismas yra kompetentingas pripažinti Sąjungos tesės aktą negaliojančiu, o šia kompetencija siekiama garantuoti teisinį saugumą užtikrinant vienodą Sąjungos teisės taikymą. Kol sprendimas nepripažintas negaliojančiu, kol Komisija jo iš dalies nepakeitė arba nepanaikino, jis lieka privalomas visas ir tiesiogiai taikytinas visose valstybėse narėse [51].

128. Manau, kad, siekiant pateikti išsamų atsakymą prašymą priimti prejudicinį sprendimą pateikusiam teismui ir panaikinti šioje byloje išreikštas abejones dėl Sprendimo 2000/520 galiojimo, Teisingumo Teismas turėtų įvertinti šio sprendimo galiojimą.

129. Atsižvelgiant į tai, taip pat reikia patikslinti, kad nagrinėjant, ar Sprendimas 2000/520 galioja, ar ne, reikia apsiriboti tik tais kaltinimais, dėl kurių buvo diskutuojama šioje byloje. Iš tiesų šiuo atžvilgiu nebuvo diskutuojama visais aspektais, susijusiais su „saugaus uosto“ sistemos veikimu, todėl nemanau, kad šiuo atveju yra įmanoma išsamiai išnagrinėti šios sistemos trūkumus.

130. Tačiau nagrinėjant šią bylą Teisingumo Teisme buvo diskutuojama dėl to, ar bendra ir netikslinė Jungtinių Amerikos Valstijų saugumo tarnybų prieiga prie perduodamų duomenų gali turėti įtakos Sprendimo 2000/520 teisėtumui. Taigi šio sprendimo galiojimą galima įvertinti šiuo požiūriu.

48 — Visų pirma žr. sprendimus *Strehl* (62/76, EU:C:1977:18, 10–17 punktai); *Roquette Frères* (145/79, EU:C:1980:234, 6 punktas) ir *Schutzverband der Spirituosen-Industrie* (C-457/05, EU:C:2007:576, 32–39 punktai).

49 — Sprendimas *Schwarze* (16/65, EU:C:1965:117, p. 1094).

50 — Žr. Sprendimą *Hauer* (44/79, EU:C:1979:290, 16 punktas).

51 — Visų pirma žr. Sprendimą *CIVAD* (C-533/10, EU:C:2012:347, 39 ir 41 punktai ir nurodyta teismo praktika).

B – *Dėl Sprendimo 2000/520 galiojimo*

1. Dėl aplinkybių, į kurias reikia atsižvelgti vertinant Sprendimo 2000/520 galiojimą

131. Reikia priminti teismų praktiką, pagal kurią, „nagrinėjant ieškinį dėl panaikinimo, akto teisėtumą reikia vertinti atsižvelgiant į faktines ir teisines aplinkybes, buvusias šio akto priėmimo dieną, o Komisijos vertinimas gali būti kritikuojamas tik paaiškėjus, kad jis yra akivaizdžiai klaidingas, atsižvelgiant į aplinkybes, kurios jai buvo žinomos nagrinėjamo akto priėmimo metu“ [52].

132. Sprendime *Gaz de France – Berliner Investissement* [53] Teisingumo Teismas priminė principą, pagal kurį „akto galiojimo vertinimas, kurį Teisingumo Teismas turi atlikti nagrinėdamas prašymą priimti prejudicinį sprendimą, paprastai turi būti grindžiamas situacija, esančia priimant šį aktą“ [54]. Tačiau, atrodo, jis pripažino, kad „akto galiojimas tam tikrais atvejais gali būti vertinamas atsižvelgiant į naujas aplinkybes, atsiradusias po šio akto priėmimo“ [55].

133. Man atrodo, kad tokia Teisingumo Teismo pozicija yra ypač reikšminga nagrinėjant šią bylą.

134. Iš tiesų Komisijos pagal Direktyvos 95/46 25 straipsnio 6 dalį priimami sprendimai turi ypatingų savybių. Jie skirti įvertinti, ar trečiosios šalies užtikrinamas asmens duomenų apsaugos lygis yra adekvatus, ar ne. Tad tai yra vertinimas, kuris turi keistis, atsižvelgiant į trečiojoje šalyje vyraujančias faktines ir teisines aplinkybes.

135. Turint omenyje tai, kad sprendimas dėl adekvatumo yra ypatingos rūšies sprendimas, taisyklė, kad jo galiojimas gali būti vertinamas tik atsižvelgiant į priimant šį sprendimą buvusias aplinkybes, šioje byloje turi būti taikoma su tam tikromis išlygomis. Antraip ši taisyklė lemtų tai, kad, praėjus keleriems metams po sprendimo dėl adekvatumo priėmimo, atliekant galiojimo vertinimą, kurį turi atlikti Teisingumo Teismas, nebūtų galima atsižvelgti į vėlesnius įvykius, net jei prašymą priimti prejudicinį sprendimą dėl galiojimo vertinimo galima pateikti bet kada, ir jei toks vertinimas gali būti pradėtas būtent dėl paskesnių aplinkybių, atskleidžiančių nagrinėjamo akto trūkumus.

136. Šioje byloje Sprendimo 2000/520 galiojimo išlaikymas maždaug 15 metų rodo, kad Komisija netiesiogiai patvirtina savo 2000 m. atliktą vertinimą. Jeigu gavęs prašymą priimti prejudicinį sprendimą Teisingumo Teismas turi įvertinti Komisijos ilgainiui išlaikyto vertinimo galiojimą, būtų gerai, jeigu jis ne tik galėtų, bet ir turėtų patikrinti šį vertinimą atsižvelgdamas į naujas aplinkybes, susiklosčiusias po sprendimo dėl adekvatumo priėmimo.

137. Atsižvelgiant į sprendimo dėl adekvatumo ypatingą pobūdį, Komisija turi jį reguliariai peržiūrėti. Jeigu, per tą laiką paaiškėjus naujoms aplinkybėms, Komisija nepakeičia savo sprendimo, taip ji netiesiogiai, bet neabejotinai patvirtina savo atliktą pradinį vertinimą. Taigi ji pakartojo savo išvadą, kad atitinkama trečioji šalis užtikrina adekvatų perduodamų asmens duomenų apsaugos lygį. Teisingumo Teismas turi patikrinti, ar ši išvada ir toliau galioja, nepaisant vėliau susiklosčiusių aplinkybių.

138. Taigi manau, kad, siekiant užtikrinti veiksmingą tokio pobūdžio sprendimo teisminę kontrolę, jo galiojimą reikia vertinti atsižvelgiant į esamas faktines ir teisines aplinkybes.

52 — Visų pirma žr. Sprendimą *BVGD / Komisija* (T-104/07 ir T-339/08, EU:T:2013:366, 291 punktas), kuriame daroma nuoroda į Sprendimą *IECC / Komisija* (C-449/98 P, EU:C:2001:275, 87 punktas).

53 — C-247/08, EU:C:2009:600.

54 — 49 punktas ir nurodyta teismo praktika.

55 — 50 punktas ir nurodyta teismų praktika. Šiuo klausimu žr. K. Lenaerts, I. Maselis ir K. Gutman „EU Procedural Law“, Oxford University Press, 2014, kurie nurodo, kad „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court“ (10.16 punktas, p. 471).

2. Dėl adekvataus apsaugos lygio sąvokos

139. Visas Direktyvos 95/46 25 straipsnis yra grindžiamas principu, kad asmens duomenys gali būti perduodami į trečiąją šalį tik jeigu ši trečioji šalis užtikrina adekvatų šių duomenų apsaugos lygį. Taigi šio straipsnio tikslas yra užtikrinti pagal šią direktyvą suteikiamos apsaugos tęstinumą asmens duomenų perdavimo į trečiąją šalį atveju. Šiuo atžvilgiu reikia priminti, kad minėta direktyva užtikrina aukštą Sąjungos piliečių apsaugos lygį tvarkant jų asmens duomenis.

140. Turint omenyje svarbų asmens duomenų apsaugos vaidmenį atsižvelgiant į pagrindinę teisę į privataus gyvenimo gerbimą, toks aukštas apsaugos lygis turi taip pat turi būti užtikrinamas ir tais atvejais, kai asmens duomenys yra perduodami į trečiąją šalį.

141. Dėl šios priežasties manau, kad Komisija, remdamasi Direktyvos 95/46 25 straipsnio 6 dalimi, gali konstatuoti, kad trečioji šalis užtikrina adekvatų apsaugos lygį, tik jeigu, įvertinusi visą nagrinėjamos trečiosios šalies teisę ir praktiką, ji gali nustatyti, kad ši trečioji šalis užtikrina tokį apsaugos lygį, kuris iš esmės lygiavertis pagal šią direktyvą užtikrinamam apsaugos lygiui, nors šios apsaugos tvarka gali skirtis nuo Sąjungoje paprastai taikomos tvarkos.

142. Nors lingvistiniu požiūriu anglišką žodį „adequate“ galima suprasti kaip nurodantį patenkinamą arba pakankamą apsaugos lygį ir semantiniu požiūriu jis gali skirtis nuo prancūziško žodžio „adéquat“, reikia pažymėti, kad vienintelis kriterijus, kuriuo reikia vadovautis aiškinant šį žodį, yra tikslas pasiekti aukštą pagrindinių teisių apsaugos lygį, kaip to reikalaujama Direktyvoje 95/46.

143. Nagrinėjant trečiosios šalies užtikrinamą apsaugos lygį turi būti analizuojami du pagrindiniai aspektai, t. y. taikytinų taisyklių turinys ir priemonės, skirtos šių taisyklių laikymuisi užtikrinti [56].

144. Mano nuomone, norint pasiekti tokį apsaugos lygį, kuris būtų iš esmės lygiavertis Sąjungoje galiojančiam apsaugos lygiui, „saugaus uosto“ sistema, kuri yra daugiausia grindžiama šioje sistemoje savanoriškai dalyvaujančių įmonių prisiimtu įsipareigojimu ir savęs įvertinimu, turi būti taikoma numatant tinkamas garantijas ir pakankamą kontrolės mechanizmą. Taigi perduodant asmens duomenis į trečiąsias šalis neturi būti taikoma silpnesnė apsauga nei asmens tvarkant duomenis Sąjungos viduje.

145. Šiuo atžvilgiu iš pradžių reikia pažymėti, kad pagal Sąjungoje vyraujančią sampratą išorinės kontrolės mechanizmas, t. y. nepriklausoma institucija, yra būtina bet kurios sistemos, pagal kurią siekiama užtikrinti, kad būtų laikomasi taisyklių, susijusių su asmens duomenų apsauga, dalis.

146. Be to, siekiant užtikrinti Direktyvos 95/46 25 straipsnio 1–3 dalių veiksmingumą, reikia atsižvelgti į tai, kad trečiosios šalies užtikrinamo apsaugos lygio adekvatumas yra kintantis dalykas, kuris dėl įvairių veiksnių ilgainiui gali keistis. Taigi valstybės narės ir Komisija turi nuolat atidžiai stebėti visus aplinkybių pokyčius, dėl kurių gali būti būtina pakartotinai įvertinti šio trečiosios šalies užtikrinamos apsaugos lygio adekvatumą. Šios apsaugos adekvatumo įvertinimas tikrai negali būti užfiksuotas konkrečiu momentu ir paskui išlaikomas neapibrėžtą laiką, nors visi aplinkybių pokyčiai rodytų, kad iš tikrųjų užtikrinamas apsaugos lygis nebėra adekvatus.

147. Taigi trečiosios šalies pareiga užtikrinti adekvatų apsaugos lygį yra tęstinis įpareigojimas. Jeigu vertinimas yra atliekamas konkrečiu momentu, sprendimo dėl adekvatumo palikimas galioti suponuoja, kad nė viena vėliau atsiradusi aplinkybė negali priversti suabejoti Komisijos atliktu pradiniu vertinimu.

56 — Žr. Komisijos darbo grupės WP 12 darbo dokumentą „Asmens duomenų perdavimas į trečiąsias šalis. Duomenų apsaugos direktyvos 25 ir 26 straipsnių taikymas“, kurį 1998 m. liepos 24 d. priėmė Asmenų apsaugos tvarkant asmens duomenis darbo grupė.

148. Iš tiesų nereikia pamiršti, kad Direktyvos 95/46 25 straipsnio tikslas – neleisti, kad asmens duomenys būtų perduodami į trečiąją šalį, kuri neužtikrina adekvataus apsaugos lygio, pažeidžiant Chartijos 8 straipsnyje užtikrinamą pagrindinę teisę į asmens duomenų apsaugą.

149. Reikia pažymėti, kad Sąjungos teisės aktų leidėjo Direktyvos 95/46 25 straipsnio 6 dalyje Komisijai suteiktiems įgaliojimams konstatuoti, kad ši trečioji šalis užtikrina adekvatų apsaugos lygį, yra nustatytas aiškus reikalavimas, kad ši šalis užtikrintų tokį lygį, kaip tai suprantama pagal šio straipsnio 2 dalį. Jeigu naujos aplinkybės leidžia abejoti pradiniu vertinimu, Komisija dėl to turi pritaikyti savo sprendimą.

3. Vertinimas

150. Primenu, kad pagal Direktyvos 95/46 25 straipsnio 6 dalį „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“. Aiškinant šios direktyvos 25 straipsnio 6 dalį atsižvelgiant į jos 25 straipsnio 2 dalį, pirmoji nuostata rodo, jog, norėdama konstatuoti, kad trečioji šalis užtikrina adekvatų apsaugos lygį, Komisija turi įvertinti visas šioje trečiojoje šalyje galiojančias teisės normas ir jų taikymą.

151. Kaip jau tapo aišku, jeigu Komisija išlaikė savo Sprendimą 2000/520 galiojantį nepaisydama atsiradusių naujų faktinių ir teisinių aplinkybių, tai reikia suprasti kaip jos valią patvirtinti savo pradinį vertinimą.

152. Teisingumo Teismas, gavęs prašymą priimti prejudicinį sprendimą, neturi vertinti ginčo, kurį nagrinėdamas nacionalinis teismas pateikė šį prašymą, faktinių aplinkybių [57].

153. Taigi remsiuosi faktinėmis aplinkybėmis, kurias prašymą priimti prejudicinį sprendimą pateikęs teismas nurodė savo prašyme priimti prejudicinį sprendimą ir kurias pati Komisija iš esmės pripažįsta įrodytomis [58].

154. Aplinkybes, kurios buvo nurodytos Teisingumo Teisme siekiant ginčyti Komisijos vertinimą, kad su „saugiu uostu“ susijusia sistema yra užtikrinamas adekvatus iš Sąjungos į Jungtines Amerikos Valstijas perduodamų asmens duomenų apsaugos lygis, galima apibūdinti taip.

155. Prašyme priimti prejudicinį sprendimą jį pateikęs teismas remiasi dviem konstatuotais faktais. Pirma, su asmens duomenimis, kuriuos tokios įmonės, kokia yra *Facebook Ireland*, perduoda Jungtinėse Amerikos Valstijose įsteigtai savo patronuojančiajai bendrovei, gali susipažinti NSA ir kitos Amerikos saugumo tarnybos, vykdydamos masinio ir netikslinio duomenų sekimo ir perėmimo veiklą. Iš tiesų po E. Snowden atskleistos informacijos iš turimų įrodymų šiuo metu neįmanoma daryti jokios kitos įtikinamos išvados [59]. Antra, Sąjungos piliečiai neturi jokios veiksmingos teisės būti išklausyti dėl NSA ir kitų Amerikos saugumo tarnybų atliekamo jų duomenų sekimo ir perėmimo [60].

156. Šiuos *High Court* konstatuotus faktus patvirtina pačios Komisijos padarytos išvados.

57 — Visų pirma žr. Sprendimą *Fallimento Traghetti del Mediterraneo* (C-140/09, EU:C:2010:335, 22 punktas ir nurodyta teismo praktika).

58 — Žr. šios išvados 2 išnašoje minėtą Komisijos komunikatą ir Komisijos komunikatą Europos Parlamentui ir Tarybai dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu [COM(2013) 847 *final*].

59 — Sprendimo dėl prašymo priimti prejudicinį sprendimą 7 punkto c papunktis.

60 — Sprendimo dėl prašymo priimti prejudicinį sprendimą 7 punkto b papunktis.

157. Taigi komunikate dėl „saugaus uosto“ sistemos veikimo Komisija, atsižvelgdama į Sąjungos piliečius ir jos teritorijoje įsteigtas įmones, remiasi išvada, kad 2013 m. paviešinta informacija apie Amerikos sekimo programų apimtį ir mastą sukėlė abejonių, ar tebėra užtikrinama asmens duomenų, teisėtai perduotų Jungtinėms Valstijoms pagal „saugaus uosto“ sistemą, apsauga. Ji pažymėjo, kad visos bendrovės, dalyvaujančios programoje PRISM, kuri suteikia Amerikos valdžios institucijoms prieigą prie visų Jungtinėse Valstijose saugomų ar tvarkomų duomenų, yra įsipareigojusios pagal „saugaus uosto“ sistemą. Jos teigimu, taip „saugaus uosto“ sistema tapo informacijos kanalu, per kurį Jungtinių Amerikos Valstijų žvalgybos tarnybos gali rinkti asmens duomenis, prieš tai tvarkytus Sąjungoje [61].

158. Iš šių aplinkybių matyti, kad pagal Jungtinių Amerikos Valstijų teisę ir praktiką leidžiama dideliu mastu rinkti Sąjungos piliečių asmens duomenis, kurie yra perduodami pagal „saugaus uosto“ sistemą, ir šiems piliečiams nesuteikiama veiksminga teisminė apsauga.

159. Mano nuomone, šios faktinės išvados įrodo, kad Sprendime 2000/520 nėra pakankamų garantijų. Nesant šių garantijų, šis sprendimas įgyvendintas nesilaikant Chartijoje ir Direktyvoje 95/46 nustatytų reikalavimų.

160. Tačiau remiantis Direktyvos 95/46 25 straipsnio 6 dalimi priimto Komisijos sprendimo tikslas yra konstatuoti, kad trečioji šalis „užtikrina“ adekvatų apsaugos lygį. Žodis „užtikrina“, vartojamas esamuoju laiku, reiškia, kad, norint išlaikyti tokį sprendimą galiojantį, jis turi būti susijęs su trečiąja šalimi, kuri ir po šio sprendimo priėmimo užtikrina adekvatų apsaugos lygį.

161. Iš tikrųjų atskleidus informaciją apie NSA veiksmus, kad ji naudojo pagal „saugaus uosto“ sistemą perduotus duomenis, paaiškėjo teisinio pagrindo, t. y. Sprendimo 2000/520, trūkumai.

162. Nagrinėjant šią bylą paaiškėję trūkumai pirmiausia yra šio sprendimo I priedo ketvirtoje pastraipoje.

163. Primenu, kad pagal šią nuostatą „[„saugaus uosto“] [p]rincipų laikymasis gali būti ribojamas: a) tiek, kiek tai būtina atsižvelgiant į nacionalinio saugumo, visuomenės interesus arba [JAV] teisės aktų vykdymo reikalavimus [į reikalavimus, susijusius su nacionaliniu saugumu, viešuoju interesu ir Jungtinių Amerikos Valstijų teisės aktų laikymusi]; b) įstatymais, Vyriausybės nutarimais arba precedentine teise, dėl kurių atsiranda prieštaringų įsipareigojimų ar aiškių įgaliojimų, jei vykdydama tokius įgaliojimus organizacija gali įrodyti, kad Principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos palaikomus viršesnius teisėtus interesus“.

164. Problema iš esmės susijusi su tuo, kaip Jungtinių Valstijų valdžios institucijos taiko minėtoje nuostatoje numatytas leidžiančias nukrypti nuostatas. Kadangi jos suformuluotos pernelyg bendrai, minėtos institucijos gali įgyvendinti šias leidžiančias nukrypti nuostatas tik tiek, kiek tai yra griežtai būtina.

165. Prie šios pernelyg bendros formuluotės dar prisideda aplinkybė, kad Sąjungos piliečiai neturi teisių gynimo priemonių, kurios tiktų apsiginti nuo jų asmens duomenų tvarkymo kitais tikslais nei tie, dėl kurių šie duomenys buvo iš pradžių surinkti ir vėliau perduoti į Jungtines Amerikos Valstijas.

166. Sprendime 2000/520 numatytos nuostatos, leidžiančios nukrypti nuo „saugaus uosto“ principų, visų pirma dėl nacionalinio saugumo reikalavimų, turėjo būti taikomos kartu įgyvendinant nepriklausomą kontrolės mechanizmą, kuris būtų tinkamas konstatuotiems teisės į privatų gyvenimą pažeidimams išvengti.

61 — Jos komunikato p. 19.

167. Taigi paaiškėjus informacijai apie Jungtinių Amerikos Valstijų saugumo tarnybų praktiką, susijusią su bendru pagal „saugaus uosto“ sistemą perduodamų duomenų sekimu, atsiskleidė kai kurie paties Sprendimo 2000/520 trūkumai.

168. Šioje byloje patiekti kaltinimai nėra susiję su tuo, kad *Facebook* pažeidė „saugaus uosto“ principus. Jeigu tokia patvirtinta įmonė, kokia yra *Facebook USA*, suteikia Jungtinių Amerikos Valstijų valdžios institucijoms galimybę susipažinti su duomenimis, kurie jai buvo perduoti iš valstybės narės, galima manyti, kad ji tai daro siekdama laikytis Jungtinių Amerikos Valstijų teisės aktų. Atsižvelgiant į tai, kad tokia padėtis yra aiškiai leidžiama Sprendime 2000/520 dėl jame esančių plačiai suformuluotų leidžiančių nukrypti nuostatų, šioje byloje iš tikrųjų keliamas klausimas dėl šių leidžiančių nukrypti nuostatų suderinamumo su pirmine Sąjungos teise.

169. Šiuo atžvilgiu reikia pažymėti, kad pagal nusistovėjusią Teisingumo Teismo praktiką pagarba žmogaus teisėms yra Sąjungos teisės aktų teisėtumo sąlyga ir kad Sąjungoje neleidžiamos su pagarba joms nesuderinamos priemonės [62].

170. Beje, iš Teisingumo Teismo praktikos matyti, kad asmens duomenų atskleidimas viešiems ar privatiems tretiesiems asmenims, „neatsižvelgiant į tolesnį pateiktų duomenų naudojimą“, laikomas suinteresuotojo asmens teisės į privatų gyvenimą ribojimu [63]. Be to, Sprendime *Digital Rights Ireland ir kt.* [64] Teisingumo Teismas patvirtino, kad kompetentingų nacionalinių institucijų prieiga prie tokių duomenų yra papildomas šios pagrindinės teisės apribojimas [65].Taip pat Chartijos 8 straipsnyje yra numatytas visų formų asmens duomenų tvarkymas ir jis reiškia teisės į šių duomenų apsaugą ribojimą [66]. Taigi Jungtinių Amerikos Valstijų saugumo tarnybų galimybė susipažinti su perduodamais duomenimis taip pat reiškia Chartijos 8 straipsnyje užtikrinamos pagrindinės teisės į asmens duomenų apsaugą ribojimą, nes ši prieiga reiškia šių duomenų tvarkymą.

171. Panašiai, kaip Teisingumo Teismas konstatavo tame sprendime, šitaip nustatytas ribojimas yra plataus taikymo ir turi būti laikomas labai dideliu, atsižvelgiant į didelį atitinkamų naudotojų skaičių ir perduodamų duomenų kiekį. Dėl šių aplinkybių, siejamų su Jungtinių Amerikos Valstijų valdžios institucijų prieigos prie asmens duomenų, perduodamų Jungtinių Amerikos Valstijų įsteigtoms įmonėms, slaptu pobūdžiu, ribojimas tampa ypač rimtas.

172. Dar prisideda aplinkybė, kad Sąjungos piliečiai, *Facebook* naudotojai, nėra informuoti apie tai, kad jų asmens duomenys yra bendrai prieinami Jungtinių Amerikos Valstijų saugumo tarnyboms.

173. Taip pat reikia pažymėti, jog prašymą priimti prejudicinį sprendimą pateikęs teismas konstatavo, kad Jungtinėse Amerikos Valstijose Sąjungos piliečiai neturi jokios realios teisės būti išklausyti dėl jų duomenų sekimo ir perėmimo klausimo. Kompetentingas FISC vykdo priežiūrą, tačiau jo vykdomas procesas yra slaptas ir neparemtas rungimosi principu [67]. Manau, kad taip yra ribojama Sąjungos piliečių teisė į veiksmingą teisinę gynybą, saugomą Chartijos 47 straipsnyje.

174. Taigi atsiranda pagal Chartijos 7, 8 ir 47 straipsnius saugomų pagrindinių teisių apribojimas, kuris yra leidžiamas pagal Sprendimo 2000/520 I priedo ketvirtoje pastraipoje išdėstytas nuostatas, leidžiančias nukrypti nuo „saugaus uosto“ principų.

175. Dabar reikia patikrinti, ar šis apribojimas yra pateisinamas, ar ne.

62 — Visų pirma žr. Sprendimą *Kadi ir Al Barakaat International Foundation / Taryba ir Komisija* (C-402/05 P ir C-415/05 P, EU:C:2008:461, 284 punktas ir nurodyta teismo praktika).

63 — Sprendimas *Österreichischer Rundfunk ir kt.* (C-465/00, C-138/01 ir C-139/01, EU:C:2003:294, 74 punktas).

64 — C-293/12 ir C-594/12, EU:C:2014:238.

65 — 35 punktas.

66 — 36 punktas.

67 — Sprendimo dėl prašymo priimti prejudicinį sprendimą 7 punkto b papunktis.

176. Pagal Chartijos 52 straipsnio 1 dalį bet koks šia Chartija pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės. Remiantis proporcingumo principu, minėtų teisių ir laisvių apribojimai galimi tik tuo atveju, kai jie būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

177. Atsižvelgdamas į tokias sąlygas, kuriomis remiantis galima pripažinti Chartija saugomų teisių ir laisvių įgyvendinimo apribojimus, labai abejoju, ar šioje byloje nagrinėjami apribojimai galėtų būti atitinkančiais Chartijos 7 ir 8 straipsnių esmę. Iš tiesų atrodo, kad Jungtinių Amerikos Valstijų tarnybų galimybė susipažinti su perduodamais duomenimis apima elektroninių pranešimų turinį, o taip pažeidžiama pagrindinės teisės į privataus gyvenimo gerbimą ir kitų Chartijos 7 straipsnyje įtvirtintų teisių esmė. Be to, nors platus Sprendimo 2000/520 I priedo ketvirtoje pastraipoje numatytų apribojimų formulavimas galbūt leidžia netaikyti visų „saugaus uosto“ principų, galima teigti, kad šie apribojimai pažeidžia pagrindinės teisės į asmens duomenų apsaugą esmę [68].

178. Kalbant apie klausimą, ar konstatuotas ribojimas atitinka bendrojo intereso tikslą, pirmiausia reikia priminti, kad pagal Sprendimo 2000/520 I priedo ketvirtos pastraipos b punktą „saugaus uosto“ principų laikymasis gali būti ribojamas „įstatymais, Vyriausybės nutarimais arba precedentine teise, dėl kurių atsiranda prieštaringų įsipareigojimų ar aiškių įgaliojimų, jei vykdydama tokius įgaliojimus organizacija gali įrodyti, kad Principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos palaikomus viršesnius teisėtus interesus“.

179. Reikia pripažinti, kad šioje nuostatoje paminėti „teisėti interesai“ nedetalizuoti. Tai lemia neaiškumą dėl šios leidžiančios nukrypti nuostatos taikymo srities, kuri gali būti labai plati, „saugaus uosto“ principų besilaikančioms įmonėms taikant šiuos principus.

180. Perskaičius Sprendimo 2000/520 IV priedo B antraštinėje dalyje „Aiškūs teisiniai įgaliojimai“ pateiktus paaiškinimus, šis įspūdis pasitvirtina; visų pirma jį patvirtina teiginys, jog „akivaizdu, kad tuomet, kai JAV teisės aktai nustato prieštaraujančius įsipareigojimus, tiek „saugaus uosto“ sistemai priklausančios, tiek nepriklausančios JAV organizacijos privalo laikytis teisės aktų“. Be to, kalbant apie aiškius įgaliojimus, nurodyta, kad „nors „saugaus uosto“ principai skirti įveikti skirtumus tarp JAV ir Europos privatumo apsaugos režimų, mes gerbiame mūsų išrinktų įstatymų leidėjų teisines prerogatyvas“.

181. Mano nuomone, remiantis tuo darytina išvada, kad ši leidžianti nukrypti nuostata prieštarauja Chartijos 7, 8 straipsniams ir 52 straipsnio 1 daliai, kiek ja nesiekiama pakankamai tiksliai apibrėžto bendrojo intereso tikslo.

182. Bet kuriuo atveju paprastumas ir bendrumas, kurie būdingi Sprendimo 2000/520 I priedo ketvirtos pastraipos b punkto ir IV priedo B antraštinės dalies nuostatai, kad „saugaus uosto“ principai gali būti netaikomi pagal Jungtinių Amerikos Valstijų teisės normas, yra nesuderinami su sąlyga, kad nukrypimai nuo taisyklių, susijusių su asmens domenų apsauga, turi būti ribojami tuo, kas yra griežtai būtina. Aišku, yra paminėta būtinumo sąlyga, tačiau nors pareiga įrodyti atitiktį šiai sąlygai nustatyta atitinkamai įmonei, nesuprantu, kaip ši įmonė galėtų išvengti pareigos netaikyti „saugaus uosto“ principų, kylančios iš teisės normų, kurias ji privalo taikyti.

183. Taigi laikausi nuomonės, kad Sprendimą 2000/520 reikia pripažinti negaliojančiu, nes pats leidžiančios nukrypti nuostatos, pagal kurią leidžiama taip bendrai ir nekonkrečiai netaikyti „saugaus uosto“ sistemos principų, buvimas neleidžia manyti, kad šia sistema užtikrinamas adekvatus asmens duomenų, perduodamų iš Sąjungos į Jungtines Amerikos Valstijas, apsaugos lygis.

68 — Šiuo atžvilgiu žr. Sprendimą *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, 39 ir 40 punktai).

184. Dėl Sprendimo 2000/520 I priedo ketvirtos pastraipos a punkte numatytų apribojimų pirmosios kategorijos reikalavimų, susijusių su nacionaliniu saugumu, viešuoju interesu ir Jungtinių Amerikos Valstijų teisės aktų laikymusi, manau, kad tik pirmasis tikslas yra pakankamai tikslus, kad jį būtų galima laikyti Sąjungos pripažįstamu bendro intereso tikslu, kaip tai suprantama pagal Chartijos 52 straipsnio 1 dalį.

185. Dabar reikia patikrinti konstatuoto apribojimo proporcingumą.

186. Šiuo atžvilgiu reikia priminti, kad, remiantis nusistovėjusia Teisingumo Teismo praktika „pagal proporcingumo principą reikalaujama, kad Sąjungos institucijų aktai būtų tinkami atitinkamo reglamentavimo teisėtiems tikslams pasiekti ir neviršytų to, kas tinkama ir būtina jiems įgyvendinti“ [69].

187. Kalbant apie šių sąlygų laikymosi teisminę kontrolę, pažymėtina, kad, „atsižvelgiant į tai, jog ribojamos teisės yra pagrindinės, Sąjungos teisės aktų leidėjo vertinimo diskrecija gali būti apribota pagal kelis kriterijus, įskaitant, be kita ko, atitinkamą sritį, Chartija užtikrintos atitinkamos teisės pobūdį, apribojimo pobūdį, dydį ir tikslą“ [70].

188. Laikausi nuomonės, kad sprendimams, kuriuos Komisija priima pagal Direktyvos 95/46 25 straipsnio 6 dalį, taikoma išsami Teisingumo Teismo kontrolė, kurią atliekant tikrinamas šios institucijos atlikto vertinimo, susijusio su trečiosios šalies užtikrinamo apsaugos lygio adekvatumu dėl „savo šalies [įstatymų] arba [tarptautinių įsipareigojimų]“, proporcingumas.

189. Šiuo atžvilgiu reikia pažymėti, jog Sprendime *Digital Rights Ireland ir kt.* [71] Teisingumo Teismas nutarė, kad „atsižvelgiant, viena vertus, į asmens duomenų apsaugos svarbą pagrindinei teisei į privataus gyvenimo gerbimą ir, kita vertus, į šios teisės apribojimo, kurį lemia [nagrinėjama] direktyva <...>, dydį, Sąjungos teisės aktų leidėjo vertinimo diskrecija yra nedidelė, todėl reikia taikyti griežtą kontrolę“ [72].

190. Tokiu apribojimu turi būti įmanoma pasiekti nagrinėjamu Sąjungos teisės aktu siekiamą tikslą ir jis turi būti būtinas šiam tikslui pasiekti.

191. Šiuo atžvilgiu „dėl teisės į privataus gyvenimo gerbimą reikia pažymėti, kad pagal nusistovėjusią Teisingumo Teismo praktiką <...> [reikalaujama], kad nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neviršytų to, kas yra griežtai būtina“ [73].

192. Atlikdamas kontrolę Teisingumo Teismas taip pat atsižvelgia į tai, kad „iš Chartijos 8 straipsnio 1 dalyje eksplicitiškai įtvirtintos pareigos kylanti asmens duomenų apsauga yra ypač svarbi Chartijos 7 straipsnyje įtvirtintai teisei į privataus gyvenimo gerbimą“ [74].

193. Kaip teigia Teisingumo Teismas, kuris šiuo atžvilgiu nurodo Europos Žmogaus Teisių Teismo praktiką, „atitinkamame Sąjungos teisės akte turi būti numatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojama atitinkamos priemonės apimtis ir taikymas ir nustatomi minimalūs reikalavimai, kad asmenims, kurių duomenys saugomi, būtų suteikta pakankamai garantijų, leidžiančių veiksmingai

69 — Sprendimas *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, 46 punktas ir nurodyta teismo praktika).

70 — Ten pat, 47 punktas ir nurodyta teismo praktika.

71 — C-293/12 ir C-594/12, EU:C:2014:238.

72 — 48 punktas.

73 — Sprendimas *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, 52 punktas ir nurodyta teismo praktika).

74 — Ten pat, 53 punktas.

apsaugoti jų asmens duomenis nuo piktnaudžiavimo pavojų, taip pat bet kokios neteisėtos prieigos prie jų ir neteisėto jų naudojimo“[75]. Teisingumo Teismas nurodo, kad „būtinybė turėti tokias garantijas yra dar svarbesnė tais atvejais, kai asmens duomenys <...> tvarkomi automatiniu būdu ir egzistuoja didelis neteisėtos prieigos prie šių duomenų pavojus“[76].

194. Mano nuomone, tarp Sprendimo 2000/520 I priedo ketvirtos pastraipos a punkto ir Direktyvos 95/46 13 straipsnio 1 dalies yra analogija. Pirmojoje iš šių nuostatų nurodyta, kad „saugaus uosto“ principų laikymasis gali būti ribojamas „tiek, kiek būtina atsižvelgiant į nacionalinio saugumo, visuomenės interesus arba [JAV] teisės aktų vykdymo reikalavimus [į reikalavimus, susijusius su nacionaliniu saugumu, viešuoju interesu ir Jungtinių Amerikos Valstijų teisės aktų laikymusi]“. Antrojoje jų numatyta, kad valstybės narės gali imtis teisėkūros priemonių, kad apribotų šios direktyvos 6 straipsnio 1 dalyje, 10 straipsnyje, 11 straipsnio 1 dalyje bei 12 ir 21 straipsniuose numatytų pareigų ir teisių mastą, kai toks apribojimas yra reikalinga apsaugos priemonė, be kita ko, norint užtikrinti nacionalinį saugumą, gynybą, visuomenės saugumą ir kriminalinių nusikaltimų prevenciją, tyrimą, išaiškinimą ir baudžiamąjį persekiojimą.

195. Kaip Teisingumo Teismas pažymėjo Sprendime *IPI*[77], iš Direktyvos 95/46 13 straipsnio 1 dalies formuluotės matyti, kad valstybės narės šioje nuostatoje numatytų priemonių gali imtis, tik jei jos reikalingos. Priemonių „reikalingumas“ yra sąlyga, su kuria siejama pagal šią nuostatą valstybėms narėms suteikta galimybė[78]. Kalbant apie asmens duomenų tvarkymą Sąjungos viduje, pažymėtina, kad šios direktyvos 13 straipsnyje numatyti apribojimai turi būti suprantami kaip apimantys tik tai, kas yra griežtai būtina numatytam tikslui pasiekti. Mano nuomone, tas pats pasakytina apie Sprendimo 2000/520 I priedo ketvirtoje pastraipoje numatytus „saugaus uosto“ principų apribojimus.

196. Tačiau reikia pripažinti, kad būtinumo kriterijus paminėtas ne visose Sprendimo 2000/520 I priedo ketvirtos pastraipos a punkto teksto kalbinėse versijose. Visų pirma taip yra versijoje prancūzų kalba, kurioje nurodyta, kad „[l]'adhésion aux principes peut être limitée par <...> les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis“, nors, pavyzdžiui, versijoje ispanų, vokiečių ir anglų kalbomis nurodyta, kad nustatyti apribojimai turi būti būtini nurodytiems tikslams pasiekti.

197. Kad ir kaip ten būtų, prašymą priimti prejudicinį sprendimą pateikusio teismo ir Komisijos minėtuose komunikatuose nurodytos faktinės aplinkybės aiškiai rodo, kad praktiškai šių apribojimų įgyvendinimas neapima tik to, kas yra griežtai būtina numatytiems tikslams pasiekti.

198. Šiuo atžvilgiu pažymiu, kad Jungtinių Amerikos Valstijų saugumo tarnybų turima galimybė susipažinti su perduotais asmens duomenimis bendrai apima visus asmenis ir visas elektroninio ryšio priemones, taip pat visus perduodamus duomenis, įskaitant pranešimų turinį, nedarant jokio skirtumo, nenumatant jokių ribojimų ar išimčių pagal siekiamą bendro intereso tikslą[79].

199. Iš tiesų saugumo tarnybų galimybė gauti perduodamus duomenis apskritai susijusi su visais asmenimis, kurie naudojasi elektroninio ryšio paslaugomis, ir nereikalaujama, kad atitinkami asmenys keltų grėsmę nacionaliniam saugumui[80].

200. Toks masinis ir netikslinis sekimas yra iš esmės neproporcingas ir reiškia nepateisinamą Chartijos 7 ir 8 straipsniuose užtikrinamų teisių ribojimą.

75 — Ten pat, 54 punktas ir nurodyta teismo praktika.

76 — Ten pat, 55 punktas ir nurodyta teismo praktika.

77 — C-473/12, EU:C:2013:715.

78 — 32 punktas.

79 — Pagal analogiją žr. Sprendimą *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, 57 punktas ir nurodyta teismo praktika).

80 — Ten pat, 58 ir 59 punktai.

201. Kaip savo pastabose teisingai pažymėjo Parlamentas, kadangi Sąjungos teisės aktų leidėjas arba valstybės narės negali priimti teisės aktų nuostatų, kuriose, pažeidžiant Chartiją, numatomas masinis ir netikslinis sekimas, remiantis tuo neabejotinai darytina išvada, kad *a fortiori* trečiosios šalys bet kuriuo atveju negali būti laikomos užtikrinančiomis adekvatų Sąjungos piliečių asmens duomenų apsaugos lygį, jeigu pagal jų teisės aktus faktiškai leidžiama masiškai ir netikslingai sekti ir perimti šio pobūdžio duomenis.

202. Be to, reikia pabrėžti, kad Sprendime 2000/520 apibrėžta „saugaus uosto“ sistema neapima garantijų, kurios būtų tinkamos siekiant išvengti masinės ir bendros prieigos prie perduodamų duomenų.

203. Šiuo atžvilgiu reikia pažymėti, jog Teisingumo Teismas Sprendime *Digital Rights Ireland ir kt.*[81] pabrėžė, kaip svarbu numatyti „aiškias ir tikslias] Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių apribojimų apimtį reglamentuojančias taisykles“[82]. Teisingumo Teismo teigimu, toks apribojimas turi būti „tiksliai reglamentuotas nuostatomis, leidžiančiomis užtikrinti, kad jis iš tiesų neviršija to, kas yra griežtai būtina“[83]. Teisingumo Teismas tame sprendime pažymėjo būtinybę numatyti „pakankamas garantijas, kaip antai reikalaujam[a]s Chartijos 8 straipsnyje, kurios leistų užtikrinti veiksmingą saugomų [asmens] duomenų apsaugą nuo piktnaudžiavimo rizikos, bet kokios neteisėtos prieigos prie jų ir neteisėto jų naudojimo“[84].

204. Tačiau reikia pripažinti, kad privataus arbitražo mechanizmai ir FTC dėl savo riboto vaidmens komercinio pobūdžio ginčuose nėra priemonės ginčyti Jungtinių Amerikos Valstijų saugumo tarnybų prieigą prie iš Sąjungos perduodamų asmens duomenų.

205. FTC jurisdikcija apima nesąžiningus ir apgaule paremtus veiksmus prekybos srityje ir neapima asmeninės informacijos rinkimo ir naudojimo nekomerciniais tikslais[85]. Ribotos srities FTC jurisdikcija riboja asmenų teisę į jų asmens duomenų apsaugą. FTC buvo įkurtas ne siekiant užtikrinti individualios teisės į privatų gyvenimą apsaugą, kaip Sąjungoje yra nacionalinių priežiūros institucijų atveju, bet garantuoti sąžiningą ir patikimą prekybą vartotojams, tad jo galimybės imtis veiksmų srityje, susijusioje su asmens duomenų apsauga, yra *de facto* ribotos. Taigi FTC neatlieka tokio vaidmens kaip nacionalinės priežiūros institucijos, numatytos Direktyvos 95/46 28 straipsnyje.

206. Sąjungos piliečiai, kurių duomenys buvo perduoti, gali kreiptis į Jungtinėse Amerikos Valstijose įsteigtas specializuotas arbitražo organizacijas, pavyzdžiui, „TRUSTe“ ir „BBBOnline“, ir prašyti patikslinti, ar jų asmens duomenis turinti įmonė pažeidžia įsipareigojimų prisiėmimo sistemos sąlygas. Organizacijų, kaip antai „TRUSTe“, užtikrinamame privačiame arbitraže negali būti nagrinėjami teisės į asmens duomenų apsaugą pažeidimai, kuriuos padaro kitos organizacijos ar institucijos nei įsipareigojimus prisiėmusios įmonės. Šios arbitražo organizacijos neturi jokios kompetencijos priimti sprendimo dėl Amerikos saugumo tarnybų veiklos teisėtumo.

207. Taigi nei FTC, nei privačios arbitražo organizacijos nėra kompetentingi kontroliuoti galimų asmens duomenų apsaugos principų pažeidimų, kuriuos padaro viešieji subjektai, kaip antai Jungtinių Amerikos Valstijų saugumo tarnybos. Tačiau tokia kompetencija yra esminė siekiant visiškai užtikrinti teisę į veiksmingą šių duomenų apsaugą. Taigi Komisija, priimdama Sprendimą 2000/520 ir išlaikydama jį galiojantį, negali konstatuoti, kad visų asmens duomenų, kurie perduodami į Jungtines Amerikos Valstijas, atveju yra užtikrinama adekvati Chartijos 8 straipsnio 3 dalyje įtvirtintos teisės apsauga, t. y. kad nepriklausoma institucija atlieka veiksmingą šių duomenų apsaugos ir saugumo reikalavimų laikymosi kontrolę.

81 — C-293/12 ir C-594/12, EU:C:2014:238.

82 — 65 punktas.

83 — Ten pat.

84 — Ten pat, 66 punktas.

85 — Šiuo atžvilgiu žr. Sprendimo 2000/520 II priedo 11 FAQ „FPK veikla“ ir jo III, V bei VII priedus.

208. Todėl reikia konstatuoti, kad pagal Sprendime 2000/520 numatytą „saugaus uosto“ sistemą nėra numatyta nepriklausoma institucija, kuri galėtų kontroliuoti, kad nukrypimai nuo „saugaus uosto“ principų įgyvendinimo apimtų tik tai, kas yra griežtai būtina. Tačiau jau tapo aišku, kad tokia Sąjungos teisės pagrindu vykdoma nepriklausomos institucijos kontrolė yra esminis asmenų apsaugos tvarkant asmens duomenis elementas [86].

209. Šiuo atžvilgiu reikia pažymėti vaidmenį, kuris Sąjungoje galiojančioje asmens duomenų apsaugos sistemoje tenka nacionalinėms priežiūros institucijoms, kai jos atlieka Direktyvos 95/46 13 straipsnyje numatytų apribojimų kontrolę. Pagal šios direktyvos 28 straipsnio 4 dalies antrą pastraipą „kiekviena priežiūros institucija taip pat nagrinėja bet kurio asmens iškeltus ieškinius [pateiktus prašymus], reikalaujant patikrinti duomenų tvarkymo teisėtumą tais atvejais, kai taikomos pagal šios direktyvos 13 straipsnį priimtos nacionalinės nuostatos“. Pagal analogiją manau, kad paminėjus „saugaus uosto“ principų taikymo apribojimus Sprendimo 2000/520 I priedo ketvirtoje pastraipoje kartu reikėjo įdiegti kontrolės mechanizmą, kurį užtikrintų nepriklausoma speciali asmens duomenų apsaugos srityje veikianti institucija.

210. Iš tiesų nepriklausomų priežiūros institucijų įsikišimas sudaro Europos asmens duomenų apsaugo sistemos esmę. Taigi natūralu, kad tokių institucijų buvimas nuo pat pradžių buvo laikomas viena iš būtinų sąlygų trečiųjų šalių užtikrinamo apsaugos lygio adekvatumui konstatuoti. Tai yra sąlyga, kad duomenų srautai iš valstybių narių teritorijos į trečiąją šalį nebūtų uždrausti pagal Direktyvos 95/46 25 straipsnį [87]. Kaip yra pažymėta, pagal šios direktyvos 29 straipsnį įsteigtos darbo grupės diskusijų dokumente, Europoje iš esmės sutariama, kad „išorinės kontrolės“ mechanizmas, išreikštas nepriklausoma institucija, yra būtinas bet kurios sistemos, kuria siekiama užtikrinti duomenų apsaugos taisyklių laikymąsi, elementas“ [88].

211. Be to, reikia pažymėti, kad FISC nesuteikia veiksmingos teisminės gynybos Sąjungos piliečiams, kurių asmens duomenys yra perduodami į Jungtines Amerikos Valstijas. Iš tiesų apsaugos nuo vyriausybės tarnybų sekimo priemonės pagal 1978 m. įstatymo dėl užsienio saugumo tarnybų sekimo 702 straipsnį taikomos tik Jungtinių Amerikos Valstijų piliečiams ir užsienio šalių piliečiams, teisėtai ir nuolat gyvenantiems Jungtinėse Amerikos Valstijose. Kaip pažymėjo pati Komisija, Jungtinių Amerikos Valstijų informacijos rinkimo programų kontrolė galėtų būti pagerinta sustiprinus FISC vaidmenį ir nustačius asmenims skirtus teisių gynimo būdus. Šie mechanizmai galėtų sumažinti su Sąjungos piliečiais susijusių asmens duomenų, kurie nėra svarbūs nacionalinio saugumo apsaugos tikslais, tvarkymo apimtis [89].

212. Be to, pati Komisija nurodė, kad Sąjungos piliečiai neturi jokios galimybės susipažinti su duomenimis, jų taisyti ar sunaikinti arba pasinaudoti administracinėmis arba teisminėmis teisių gynimo priemonėmis, jeigu pagal Amerikos sekimo programas yra renkami ir vėliau tvarkomi su jais susiję asmens duomenys [90].

213. Galiausiai reikia paminėti, kad Jungtinių Amerikos Valstijų normos, susijusios su privataus gyvenimo apsauga, gali būti skirtingai taikomos Jungtinių Amerikos Valstijų ir užsienio šalių piliečiams [91].

86 — Žr. Sprendimą *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, 68 punktas ir nurodyta teismo praktika).

87 — Žr. Y. Poullet „L'autorité de contrôle: 'vues' de Bruxelles“, *Revue française d'administration publique*, Nr. 89, 1999 m. sausio–kovo mėn., p. 69, ypač p. 71.

88 — Žr. šios išvados 56 išnašoje minėtą Komisijos darbo grupės WP 12 dokumentą.

89 — 2 išnašoje minėto Komisijos komunikato p. 10 ir 11.

90 — 58 išnašoje minėto Komisijos komunikato 7.2 punktas, p. 20.

91 — Šiuo klausimu žr. C. Kuner „Foreign Nationals and Data Protection Law: A Transatlantic Analysis“, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, p. 213, ypač p. 216 ir paskesnius.

214. Remiantis tuo, kas išdėstyta, darytina išvada, kad Sprendime 2000/520 nenumatyta aiškių ir tikslių Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių apribojimų apimtį reglamentuojančių taisyklių. Taigi, reikia konstatuoti, kad šis sprendimas ir jo taikymas sudaro plataus masto ir ypač didelį šių pagrindinių teisių apribojimą, kuris nėra tiksliai reglamentuotas nuostatomis, leidžiančiomis užtikrinti, kad jis iš tiesų neviršytų to, kas yra griežtai būtina.

215. Taigi priimdama Sprendimą 2000/520 ir išlaikydama jį galiojantį Komisija viršijo ribas, kurios yra būtinos laikantis proporcingumo principo atsižvelgiant į Chartijos 7, 8 straipsnius ir 52 straipsnio 1 dalį. Be to, reikia konstatuoti nepateisinamą Chartijos 47 straipsniu saugomos Sąjungos piliečių teisės į veiksmingą teisinę gynybą apribojimą.

216. Todėl šį sprendimą reikia pripažinti negaliojančiu tiek, kiek dėl pirma apibūdintų pagrindinių teisių pažeidimų negalima manyti, kad jame nustatyta „saugaus uosto“ sistema yra užtikrinamas adekvatus pagal šią sistemą iš Sąjungos į Jungtines Amerikos Valstijas perduodamų asmens duomenų apsaugos lygis.

217. Atsižvelgdamas į tokią išvadą dėl Sąjungos piliečių pagrindinių teisių pažeidimų manau, kad Komisija turėtų sustabdyti Sprendimo 2000/520 taikymą.

218. Šio sprendimo galiojimas yra neribotas. Tačiau ši byla rodo, kad adekvatus trečiosios šalies užtikrinamos apsaugos lygis ilgainiui gali keistis atsižvelgiant į faktinių ir teisinių aplinkybių, pagrindusių šį sprendimą, pokyčius.

219. Pažymiu, kad pačiame Sprendime 2000/520 yra nuostatų, kuriose Komisijai numatyta galimybė pakoreguoti šį sprendimą atsižvelgiant į aplinkybes.

220. Taigi iš šio sprendimo 9 konstatuojamosios dalies matyti, kad „Principais ir FAQ sukurtą „saugų uostą“ gali reikėti patikslinti atsižvelgiant į patirtį, privatumo apsaugos pažangą, kai dėl technologijų tampa vis lengviau perduoti bei tvarkyti asmens duomenis, ir į vykdymo priežiūros institucijų įgyvendinimo ataskaitas“.

221. Be to, pagal to paties sprendimo 3 straipsnio 4 dalį, „jei pagal šio straipsnio 1, 2 ir 3 dalių nuostatas sukaupta informacija suteikia įrodym[ų], kad bet kuri atsakinga už pagal FAQ vykdomų Principų laikymąsi institucija Jungtinėse Valstijose tinkamai neatlieka savo prievolių, Komisija informuoja JAV komercijos departamentą ir, jei būtina <...>, pateikia numatomų šio sprendimo atšaukimo, sustabdymo ar jos taikymo srities apribojimo priemonių projektą“.

222. Be to, pagal Sprendimo 2000/520 4 straipsnio 1 dalį šis sprendimas „gali būti bet kada pakeistas atsižvelgiant į jo vykdymo patirtį ir (arba) tuo atveju, jei JAV teisės aktais būtų reikalaujama didesnio už Principų ir FAQ suteikiamą apsaugos lygį. Praėjus trejiems metams po sprendimo pranešimo valstybėms narėms, Komisija įvertina, kaip šis sprendimas vykdomas, ir remdamasi turima informacija praneša susijusias išvadas pagal Direktyvos 95/46 <...> 31 straipsnį įsteigtam Komitetui, įskaitant visus įrodymus, kurie gali turėti įtakos vertinant, ar šio sprendimo 1 straipsnio nuostatos suteikia pakankamą apsaugą, kaip numato Direktyvos 95/46/EB 25 straipsnis“. Pagal Sprendimo 2000/520 4 straipsnio 2 dalį „jei būtina, Komisija pateikia numatomų priemonių projektą laikydamasi Direktyvos 95/46 31 straipsnyje nustatytos tvarkos“.

223. Komisija savo pastabose konstatavo, jog „yra didelė tikimybė, kad „saugaus uosto“ principų laikymasis buvo apribotas tokiu būdu, kuris nebeatitinka griežtai apibrėžtų nacionalinio saugumo srityje numatytos išimties sąlygų“ [92]. Šiuo atžvilgiu ji pažymi, kad „nagrinėjama atskleista informacija rodo nediferencijuotą ir didelio masto sekimą, kuris nėra suderinamas su šioje išimtyje numatytu būtinumo kriterijumi ir apskritai su Chartijos 8 straipsnyje įtvirtinta teise į asmens duomenų apsaugą“ [93]. Be to, pati Komisija pripažino, kad „sekimo programų, siejamų su nevienodu [Sąjungos] piliečių vertinimu, taikymo sritis kelia abejonių dėl saugumo srityje suteikiamos apsaugos lygio“ [94].

224. Be to, Komisija per teismo posėdį aiškiai pripažino, kad pagal šiuo metu taikomą Sprendimo 2000/520 redakciją nėra garantijos, kad bus užtikrinama Sąjungos piliečių teisė į jų duomenų apsaugą. Tačiau ši išvada savaime negali lemti šio sprendimo negaliojimo. Nors Komisija sutinka su teiginiu, kad ji turi veikti atsižvelgdama į naujas aplinkybes, ji mano, kad ėmėsi priemonių, kurios yra tinkamos ir proporcingos, kai pradėjo derybas su Jungtinėmis Amerikos Valstijomis, kad reformuotų „saugaus uosto“ sistemą.

225. Nepritariu šiai nuomonei. Iš tiesų per tą laiką asmens duomenų perdavimą į Jungtines Amerikos Valstijas turi būti galima sustabdyti nacionalinių priežiūros institucijų iniciatyva arba joms pateikus skundus.

226. Be to, manau, kad, atsižvelgdama į tokias išvadas, Komisija turėtų sustabdyti Sprendimo 2000/520 taikymą. Iš tiesų asmens duomenų apsaugos tikslas, kurio siekiama Direktyva 95/46 ir Chartijos 8 straipsniu, nustato įpareigojimus ne tik valstybėms narėms, bet ir Sąjungos institucijoms, kaip tai matyti iš Chartijos 51 straipsnio 1 dalies.

227. Vertindama trečiosios šalies siūlomą apsaugos lygį Komisija privalo patikrinti ne tik šios trečiosios šalies vidaus teisės aktus ir tarptautinius įsipareigojimus, bet ir tai, kaip asmens duomenų apsauga yra užtikrinama praktiškai. Jeigu išnagrinėjus praktiką nustatomi trūkumai, Komisija privalo reaguoti ir prireikus nedelsdama sustabdyti savo sprendimo taikymą ir (arba) jį pakoreguoti.

228. Kaip jau tapo aišku iš to, kas nurodyta pirma, valstybėms narėms tenkančią pareigą daugiausia sudaro pareiga pasitelkus savo nacionalines priežiūros institucijas užtikrinti Direktyvoje 95/46 numatytų taisyklių laikymąsi.

229. Komisijai tenka pareiga sustabdyti sprendimo, kurį ji priėmė pagal minėtos direktyvos 25 straipsnio 6 dalį, taikymą paaiškėjus, kad atitinkama trečioji šalis daro pažeidimus, kol Komisija derasi su šia trečiąja šalimi, kad šie pažeidimai būtų nutraukti.

230. Primenu, jog remiantis minėta nuostata priimto Komisijos sprendimo tikslas yra konstatuoti, ar trečioji šalis „užtikrina“ adekvatų asmens duomenų, perduodamų į šią trečiąją šalį, apsaugos lygį. Žodis „užtikrina“, vartojamas esamuoju laiku, reiškia, kad, norint išlaikyti tokį sprendimą galiojantį, jis turi būti susijęs su trečiąja šalimi, kuri ir po šio sprendimo priėmimo užtikrina tokį adekvatų apsaugos lygį.

231. Pagal Direktyvos 95/46 57 konstatuojamąją dalį „turi būti uždrausta perduoti asmens duomenis į trečiąją šalį, kuri neužtikrina adekvataus apsaugos lygio“.

92 — 44 punktas.

93 — Ten pat.

94 — 2 išnašoje minėto Komisijos komunikato p. 5.

232. Pagal šios direktyvos 25 straipsnio 4 dalį, „jeigu 31 straipsnio 2 dalyje numatyta tvarka Komisija išsiaiškina, kad kuri nors trečioji šalis neužtikrina adekvataus apsaugos lygio, kaip numatyta šio straipsnio 2 dalyje, valstybės narės imasi reikalingų priemonių, kad to tipo duomenys aptariamai trečiajai šaliai nebūtų perduoti“. Be to, minėtos direktyvos 25 straipsnio 5 dalyje nustatyta, jog „reikiamu metu Komisija pradeda derybas, kad ištaisytų padėtį, susidariusią pagal šio straipsnio 4 dalį išsiaiškinus apsaugos stoką“.

233. Iš pastarosios nuostatos matyti, kad pagal Direktyvos 95/46 25 straipsnyje nustatytą sistemą su trečiąja šalimi pradėtomis derybomis siekiama ištaisyti adekvataus apsaugos lygio nebuvimą, konstatuotą taikant šios direktyvos 31 straipsnio 2 dalyje numatytą procedūrą. Šioje byloje nagrinėjamu atveju Komisija pagal šią procedūrą formaliai nekonstatavo, kad pagal „saugaus uosto“ sistemą nebeužtikrinamas adekvatus apsaugos lygis. Atsižvelgiant į tai, jeigu Komisija nusprendė pradėti derybas su Jungtinėmis Amerikos Valstijomis, ji taip padarė dėl to, kad manė, kad šios šalies užtikrinamas apsaugos lygis nebėra adekvatus.

234. Nors Komisija žinojo apie Sprendimo 2000/520 taikymo trūkumus, ji nesustabdė šio sprendimo taikymo ir jo nepritaikė, ir taip lėmė tolesnį asmenų, kurių asmens duomenys buvo ir yra toliau perduodami pagal „saugaus uosto“ sistemą, pagrindinių teisių pažeidinėjimą.

235. Tačiau Teisingumo Teismas, nors ir kitomis aplinkybėmis, jau yra nusprendęs, jog Komisija turi užtikrinti, kad teisės aktai būtų pakoreguoti atsižvelgiant į naujus duomenis [95].

236. Mano nuomone, toks Komisijos neveikimas, kuriuo tiesiogiai pažeidžiamos Chartijos 7, 8 ir 47 straipsniais saugomos pagrindinės teisės, nagrinėjant šį prašymą priimti prejudicinį sprendimą yra papildomas motyvas pripažinti Sprendimą 2000/520 negaliojančiu [96].

III – **Išvada**

237. Atsižvelgdamas į visa tai, kas išdėstyta, siūlau Teisingumo Teismui taip atsakyti į *High Court* pateiktus klausimus:

1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 28 straipsnį, aiškinamą atsižvelgiant į Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsnius, reikia aiškinti taip, kad jeigu yra priimtas Europos Komisijos sprendimas, grindžiamas Direktyvos 95/46 25 straipsnio 6 dalimi, tai nereiškia, kad nacionalinė priežiūros institucija negali tirti skundo, kuriame teigiama, kad trečioji šalis neužtikrina adekvataus perduodamų asmens duomenų apsaugos lygio, ir prireikus sulaikyti šių duomenų perdavimą.

2000 m. liepos 26 d. Komisijos sprendimas 2000/520/EB dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“ negalioja.

95 — Šiuo klausimu žr. Sprendimą *Agrarproduktion Staebelow* (C-504/04, EU:C:2006:30, 40 punktas).

96 — Nors Teisingumo Teismas sprendime *T. Port* (C-68/95, EU:C:1996:452) nusprendė, kad „Sutartyje nebuvo numatyta nacionalinio teismo galimybė kreiptis į Teisingumo Teismą prašant, kad jis prejudiciniu sprendimu pripažintų institucijos neveikimą“ (53 punktas), atrodo, kad Sprendime *Ten Kate Holding Musselkanaal ir kt.* (C-511/03, EU:C:2005:625, 29 punktas) jis laikėsi palankesnės pozicijos.