EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
TYRIMŲ IR DOKUMENTACIJOS DIREKTORATAS

Informacijos suvestinė

ASMENS DUOMENŲ APSAUGA

Teisė į asmens duomenų apsaugą yra pagrindinė teisė, kurios užtikrinimas – svarbus Europos Sąjungos tikslas.

Ji įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje (toliau – Chartija); šios Chartijos 8 straipsnyje nustatyta:

„1. Kiekvienas turi teisę į savo asmens duomenų apsaugą.

2. Tokie duomenys turi būti tinkamai tvarkomi ir naudojami tik konkretiems tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais. Kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei į tai, kad jie būtų ištaisomi.

3. Nepriklausoma institucija kontroliuoja, kaip laikomasi šių taisyklių.“

Be to, ši pagrindinė teisė yra glaudžiai susijusi su Chartijos 7 straipsnyje įtvirtinta teise į privatų ir šeimos gyvenimą.

Teisė į asmens duomenų apsaugą taip pat numatyta Sutarties dėl Europos Sąjungos veikimo (SESV) 16 straipsnio, kuris šiuo atžvilgiu pakeitė EB 286 straipsnį, 1 dalyje.

Kiek tai susiję su antrine teise, pažymėtina, kad nuo XX a. paskutinio dešimtmečio vidurio Europos bendrija priėmė įvairių dokumentų, skirtų asmens duomenų apsaugai užtikrinti. Remiantis EB 100A straipsniu priimta Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų[1] judėjimo šiuo aspektu yra pagrindinis Sąjungos teisės aktas šioje srityje. Joje nustatytos bendros šių duomenų tvarkymo teisėtumo sąlygos ir atitinkamų asmenų teisės ir, be kita ko, numatyta, kad valstybėse narėse turi būti įsteigtos nepriklausomos kontrolės institucijos.

[1] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46 dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k., 13 sk., 15 t., p. 355), 2003 m. lapkričio 20 d. konsoliduota redakcija, kuri panaikinta nuo 2018 m. gegužės 25 d. (žr. 5 išnašą).

Vėliau buvo priimta Direktyva 2002/58[2], papildanti Direktyvą 95/46, suderinant valstybių narių teisės aktų nuostatas dėl teisės į privatų gyvenimą apsaugos užtikrinimo, be kita ko, kiek tai susiję su asmens duomenų tvarkymu elektroninių ryšių sektoriuje[3]. Reikia pažymėti, kad Sąjungos teisės aktų leidėjas numato šios direktyvos peržiūrą. Šiuo klausimu 2017 m. sausio 10 d. Komisija pateikė pasiūlymą pakeisti šią direktyvą Reglamentu dėl privatumo ir elektroninių ryšių[4].

Be to, laisvės, saugumo ir teisingumo erdvės srityje (anksčiau ESS 30 ir 31 straipsniai) Pamatiniu sprendimu 2008/977/TVR[5] iki 2018 m. gegužės mėn. buvo reglamentuojama asmens duomenų apsauga vykdant teisminį ir policijos bendradarbiavimą baudžiamosiose bylose.

2016 m. Europos Sąjunga pakeitė bendrą teisinę sistemą šioje srityje. Šiuo tikslu 2016 m. ji priėmė Reglamentą (ES) 2016/679[6] dėl duomenų apsaugos (toliau – BDAR), kuriuo panaikinama Direktyva 95/46 ir kuris taikomas nuo 2018 m. gegužės 25 d.; taip pat Direktyvą (ES) 2016/680[7] dėl tokių duomenų apsaugos baudžiamosiose bylose, kuria panaikinamas Pamatinis sprendimas 2008/977/TVR ir kurią valstybės narės į nacionalinę teisę turėjo perkelti iki 2018 m. gegužės 6 d.

Galiausiai ES institucijoms ir organams tvarkant asmens duomenis, šių duomenų apsauga iš pradžių buvo užtikrinama Reglamentu (EB) Nr. 45/2001[8]. Šis reglamentas, be kita ko, leido 2004 m. sukurti Europos duomenų apsaugos priežiūros pareigūno įstaigą. 2018 m. Europos Sąjunga patvirtino naują teisinę sistemą šioje srityje, be kita ko, priimdama Reglamentą (ES) 2018/1725[9], kuriuo panaikinamas Reglamentas Nr. 45/2001 ir Sprendimas Nr. 1247/2002 [10] ir kuris taikomas nuo 2018 m. gruodžio 11 d. Siekiant nuoseklaus požiūrio į asmens duomenų apsaugą visoje Sąjungoje, šiuo naujuoju reglamentu siekiama kiek įmanoma suderinti šios srities taisykles su Reglamente (ES) 2016/679 nustatyta tvarka.

---

2 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58 dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002, p. 37; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 514), 2009 m. gruodžio 19 d. konsoliduota redakcija.

3 Direktyva 2002/58 buvo iš dalies pakeista 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24 dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančia Direktyvą 2002/58 (OL L 105, 2006, p. 54). Šią direktyvą Teisingumo Teismas panaikino 2014 m. balandžio 8 d. Sprendimu *Digital Rights Ireland ir Seitlinger ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238), motyvuodamas tuo, kad ja buvo rimtai pažeistos teisės į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą (žr. šios suvestinės I.1 skyrių „Sąjungos antrinės teisės suderinamumas su teise į asmens duomenų apsaugą“).

4 Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58 (Reglamentas dėl privatumo ir elektroninių ryšių), COM(2017) 03 *final* – 2017/03 (COD).

5 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (OL L 350, 2008, p. 60), panaikintas nuo 2018 m. gegužės 6 d. (žr. 6 išnašą).

6 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46 (OL L 119, 2016, p. 1).

7 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89).

8 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001, p. 1; 2004 m. specialusis leidimas lietuvių k., 13 sk., 26 t., p. 102).

9 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002.

10 2002 m. liepos 1 d. Europos Parlamento, Tarybos ir Komisijos sprendimas Nr. 1247/2002 dėl Europos duomenų apsaugos priežiūros pareigūno pareigų atlikimą reglamentuojančių nuostatų ir bendrųjų sąlygų (OL L 183, 2002, p. 1; 2004 m. specialusis leidimas lietuvių k., 1 sk., 4 t., p. 43).

TURINYS

I. EUROPOS SĄJUNGOS PAGRINDINIŲ TEISIŲ CHARTIJOJE PRIPAŽINTA TEISĖ Į ASMENS DUOMENŲ APSAUGĄ 4

1. Sąjungos antrinės teisės suderinamumas su teise į asmens duomenų apsaugą 4

2. Teisės į asmens duomenų apsaugą užtikrinimas įgyvendinant Sąjungos teisę 7

II. ASMENS DUOMENŲ TVARKYMAS, KAIP TAI SUPRANTAMA PAGAL DIREKTYVĄ 95/46 9

1. Asmens duomenų tvarkymas, nepatenkantis į Direktyvos 95/46 taikymo sritį 9

2. Sąvoka „asmens duomenys“ 11

3. Sąvoka „asmens duomenų tvarkymas“ 13

4. Sąvoka „asmens duomenų susistemintas rinkinys“ 18

5. Sąvoka „asmens duomenų valdytojas“ 18

6. Asmens duomenų tvarkymo teisėtumo sąlygos, atsižvelgiant į Direktyvos 95/46 7 straipsnį 21

III. ASMENS DUOMENŲ TVARKYMAS, KAIP TAI SUPRANTAMA PAGAL DIREKTYVĄ 2002/58 29

IV. ASMENS DUOMENŲ PERDAVIMAS Į TREČIĄSIAS ŠALIS 35

V. ASMENS DUOMENŲ APSAUGA INTERNETE 41

1. Teisė prieštarauti asmens duomenų tvarkymui („Teisė būti pamirštam“) 42

2. Asmens duomenų tvarkymas ir teisė į intelektinę nuosavybę 43

3. Asmens duomenų pašalinimas 46

4. Interneto svetainės naudotojo sutikimas saugoti informaciją arba suteikti prieigą prie informacijos naudojant slapukus 50

VI. NACIONALINĖS PRIEŽIŪROS INSTITUCIJOS **51**

1. Nepriklausomumo reikalavimo apimtis 51

2. Taikytinos teisės ir kompetentingos priežiūros institucijos nustatymas 53

3. Nacionalinių priežiūros institucijų įgaliojimai 54

VII. SĄJUNGOS TEISĖS AKTŲ TAIKYMAS TERITORINIU ASPEKTU 58

VIII. VISUOMENĖS TEISĖ SUSIPAŽINTI SU EUROPOS SĄJUNGOS INSTITUCIJŲ DOKUMENTAIS IR ASMENS DUOMENŲ APSAUGA 59

I. Europos Sąjungos pagrindinių teisių chartijoje pripažinta teisė į asmens duomenų apsaugą

1. Sąjungos antrinės teisės suderinamumas su teise į asmens duomenų apsaugą

2010 m. lapkričio 9 d. didžiosios kolegijos Sprendimas „Volker und Markus Schecke ir Eifert" (C-92/09 ir C-93/09, EU:C:2010:662)[11]

Kiek tai susiję su šia byla, pažymėtina, kad pagrindinėse bylose buvo nagrinėjami žemės ūkio subjektų ir Heseno žemės ginčai dėl asmens duomenų, susijusių su jais, kaip paramos iš Europos žemės ūkio garantijų fondo (EŽŪGF) ir Europos žemės ūkio fondo kaimo plėtrai (EŽŪFKP) gavėjais, paskelbimo *Bundesanstalt für Landwirtschaft und Ernährung* (Federalinė žemės ūkio ir mitybos tarnyba) interneto svetainėje. Šie subjektai prieštaravo dėl tokio paskelbimo, visų pirma teigdami, kad jo negalima pateisinti svarbesniu viešuoju interesu. Savo ruožtu Heseno žemė manė, kad šiuos duomenis galima skelbti remiantis reglamentais (EB) Nr. 1290/2005[12] ir 259/2008[13], reglamentuojančiais bendrosios žemės ūkio politikos finansavimą ir įpareigojančiais skelbti informaciją apie fizinius asmenis, gaunančius paramą iš EŽŪGF ir EŽŪFKP.

Tokiomis aplinkybėmis *Verwaltungsgericht Wiesbaden* (Vysbadeno administracinis teismas, Vokietija) pateikė Teisingumo Teismui kelis klausimus dėl tam tikrų Reglamento Nr. 1290/2005 nuostatų ir Reglamento Nr. 259/2008 galiojimo; šiuose reglamentuose įpareigojama pateikti visuomenei tokią informaciją, be kita ko, nacionalinių tarnybų administruojamose interneto svetainėse.

Teisingumo Teismas pažymėjo, kad, kiek tai susiję su Chartijoje pripažįstamos teisės į asmens duomenų apsaugą ir skaidrumo pareigos Europos lėšų srityje suderinamumu, su asmenvardžiais susijusių duomenų apie paramos gavėjus ir jų gautas sumas paskelbimas interneto svetainėje, dėl ko šie duomenys tampa prieinami tretiesiems asmenims, yra atitinkamų

---

11 Šis sprendimas pristatytas 2010 m. metiniame pranešime, p. 11.

12 2005 m. birželio 21 d. Tarybos reglamentas (EB) Nr. 1290/2005 dėl bendrosios žemės ūkio politikos finansavimo (OL L 209, 2005, p. 1), panaikintas 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1306/2013 dėl bendros žemės ūkio politikos finansavimo, valdymo ir stebėsenos (OL L 347, 2013, p. 549).

13 2008 m. kovo 18 d. Komisijos reglamentas (EB) Nr. 259/2008, kuriuo nustatomos išsamios Tarybos reglamento (EB) Nr. 1290/2005 nuostatų dėl informacijos apie EŽŪGF ir EŽŪFKP paramos gavėjus skelbimo taikymo taisyklės (OL L 76, 2008, p. 28), panaikintas 2014 m. rugpjūčio 6 d. Komisijos įgyvendinimo reglamentu (ES) Nr. 908/2014, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 1306/2013 taikymo taisyklės, susijusios su mokėjimo agentūromis ir kitomis įstaigomis, finansų valdymu, sąskaitų patvirtinimu, patikrų taisyklėmis, užstatais ir skaidrumu (OL L 255, 2014, p. 59).

gavėjų teisės į privatų gyvenimą apskritai, o konkrečiai – teisės į jų asmens duomenų apsaugą apribojimas (56–64 punktai).

Kad tokį apribojimą būtų galima pateisinti, jis turi būti numatytas įstatymuose, nekeisti šių teisių esmės ir, remiantis proporcingumo principu, turi būti būtinas bei iš tikrųjų atitikti Sąjungos pripažįstamus bendrojo intereso tikslus, o naudojimosi šiomis teisėmis išimtys ir apribojimai neturi viršyti to, kas būtina (65 punktas). Tokiomis aplinkybėmis Teisingumo Teismas laikėsi nuomonės, kad nors demokratinėje visuomenėje mokesčių mokėtojai turi teisę būti informuoti apie viešųjų lėšų panaudojimą, vis dėlto Taryba ir Komisija turėjo subalansuotai įvertinti įvairius nagrinėjamus interesus, todėl prieš priimant ginčijamas nuostatas reikėjo patikrinti, ar valstybės narės atliktas šių duomenų paskelbimas vienoje interneto svetainėje neviršija to, kas būtina įgyvendinant siekiamus teisėtus tikslus (77, 79, 85 ir 86 punktai).

Taigi, Teisingumo Teismas pripažino negaliojančiomis tam tiktas Reglamento Nr. 1290/2005 nuostatas ir visą Reglamentą Nr. 259/2008, nes, kiek tai susiję su fiziniais asmenimis, gaunančiais paramą iš EŽŪGF ir EŽŪFKP, šiomis nuostatomis įpareigojama paskelbti asmens duomenis, susijusius su visais paramos gavėjais, neskirstant jų pagal reikšmingus kriterijus, kaip antai tokios paramos gavimo laikotarpį, jos mokėjimo dažnį, rūšį ar dydį (92 punktas, rezoliucinės dalies 1 punktas). Vis dėlto Teisingumo Teismas nekvestionavo tokios paramos gavėjų sąrašų paskelbimo, kurį nacionalinės valdžios institucijos atliko laikotarpiu iki to sprendimo paskelbimo dienos, poveikio (94 punktas, rezoliucinės dalies 2 punktas).

2013 m. spalio 17 d. Sprendimas „Schwarz“ (C-291/12, EU:C:2013:670)

M. Schwarz paprašė Bochumo miesto (Vokietija) išduoti pasą, tačiau nesutiko, kad būtų paimti jo pirštų antspaudai. Kadangi šis miestas atmetė jo prašymą, M. Schwarz pateikė skundą *Verwaltungsgericht Gelsenkirchen* (Gelzenkircheno administracinis teismas, Vokietija), prašydamas įpareigoti šią savivaldybę išduoti jam pasą nepaimant pirštų anspaudų. Tame teisme M. Schwarz ginčijo Reglamento Nr. 2252/2004[14], kuriame buvo nustatyta pareiga paimti pasų prašytojų pirštų antspaudus, galiojimą, be kita ko, teigdamas, kad šis reglamentas pažeidžia teisę į asmens duomenų apsaugą ir teisę į privatų gyvenimą.

Tokiomis aplinkybėmis *Verwaltungsgericht Gelsenkirchen* pateikė Teisingumo Teismui prašymą priimti prejudicinį sprendimą, siekdamas išsiaiškinti, ar šis reglamentas, kiek juo paso prašytojas įpareigojamas duoti savo pirštų antspaudus ir kiek jame numatytas jų saugojimas pase, yra galiojantis, be kita ko, atsižvelgiant į Chartiją.

Teisingumo Teismas atsakė teigiamai ir nusprendė, kad nors nacionalinių valdžios institucijų vykdomu pirštų antspaudų paėmimu ir saugojimu, reglamentuojamais Reglamento Nr. 2252/2004 1 straipsnio 2 dalyje, apribojama teisė į privatų gyvenimą ir į asmens duomenų apsaugą, šis apribojimas pateisinamas siekiu apsaugoti pasus nuo nesąžiningo naudojimo.

Visų pirma tokiu įstatymuose numatytu apribojimu siekiama Sąjungos pripažinto bendrojo intereso tikslo, nes juo, be kita ko, norima užkirsti kelią neteisėtam asmenų patekimui į Sąjungos

[14] 2004 m. gruodžio 13 d. Tarybos reglamentas (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų (OL L 385, 2004, p. 1), iš dalies pakeistas 2009 m. gegužės 6 d. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 444/2009 (OL L 142, 2009, p. 1).

teritoriją (35–38 punktai). Be to, pirštų antspaudų paėmimas ir saugojimas yra tinkami šiam tikslui pasiekti. Viena vertus, nors tapatybės tikrinimo pagal pirštų antspaudus metodas nėra visiškai patikimas, jis labai sumažina neturinčių leidimo asmenų priėmimo riziką. Kita vertus, tai, kad paso turėtojo pirštų antspaudai neatitinka į šį dokumentą integruotų duomenų, reiškia ne tai, jog atitinkamą asmenį bus automatiškai atsisakoma įleisti į Sąjungos teritoriją, o tik tai, kad bus atliktas išsamus patikrinimas, skirtas jo tapatybei galutinai nustatyti (42–45 punktai).

Galiausiai, kiek tai susiję su tokio tvarkymo būtinybe, Teisingumo Teismui nebuvo pateikta informacijos apie tai, kad esama pakankamai veiksmingų priemonių, kurios ne taip ribotų Chartijos 7 ir 8 straipsniuose pripažįstamas teises, palyginti su pirštų antspaudais grindžiamu metodu (53 punktas). Reglamento Nr. 2252/2004 1 straipsnio 2 dalyje nėra numatyta tokio paimtų pirštų atspaudų tvarkymo, kuris viršytų tai, kas yra būtina nustatytam tikslui pasiekti. Tame reglamente aiškiai nurodyta, kad pirštų atspaudai gali būti naudojami tik paso autentiškumui ir jo turėtojo tapatybei patikrinti. Be to, šio reglamento 1 straipsnio 2 dalyje užtikrinama apsauga nuo rizikos, kad pirštų atspaudų duomenis nuskaitys leidimo neturintys asmenys, ir numatyta pirštų atspaudus saugoti vien pačiame pase, kurį turi tik jo savininkas (54–57, 60, 63 punktai).

2014 m. balandžio 8 d. didžiosios kolegijos Sprendimas „Digital Rights Ireland ir Seitlinger ir kt.“ (sujungtos bylos C-293/12 ir C-594/12, EU:C:2014:238)[15]

Šis sprendimas priimtas išnagrinėjus prašymus įvertinti Direktyvos 2006/24 dėl duomenų apsaugos galiojimą, atsižvelgiant į pagrindines teises į privatų gyvenimą ir į asmens duomenų apsaugą, pateiktus nagrinėjant nacionalines bylas Airijos ir Austrijos teismuose. Byloje C-293/12 *High Court* (Aukštasis teismas, Airija) nagrinėjo bendrovės *Digital Rights* ir Airijos valdžios institucijų ginčą dėl nacionalinių priemonių, susijusių su elektroninių ryšių duomenų apsauga, teisėtumo. Byloje C-594/12 *Verfassungsgerichtshof* (Konstitucinis Teismas, Austrija) nagrinėjo kelis su Konstitucija susijusius skundus, kuriais buvo prašoma panaikinti nacionalinės teisės nuostatas, perkeliančias Direktyvą 2006/24 į Austrijos teisę.

Savo prašymuose priimti prejudicinį sprendimą Airijos ir Austrijos teismai pateikė Teisingumo Teismui klausimus dėl Direktyvos 2006/14 galiojimo, atsižvelgiant į Chartijos 7, 8 ir 11 straipsnius. Konkrečiau kalbant, šie teismai Teisingumo Teismo klausė, ar pagal šią direktyvą viešai prieinamų elektroninių ryšių paslaugų ar viešųjų ryšių tinklų teikėjams tenkančia pareiga tam tikrą laikotarpį saugoti duomenis, susijusius su privačiu asmens gyvenimu ir jo ryšiais, ir leisti su jais susipažinti kompetentingoms nacionalinėms institucijoms buvo nepateisinamai apribotos šios pagrindinės teisės. Atitinkamų duomenų rūšys – tai ryšio šaltiniui ir paskirties taškui išsiaiškinti ir nustatyti, taip pat ryšio datai, laikui, trukmei ir tipui, naudotojų ryšio įrangai, judriojo ryšio įrangos vietai nustatyti būtini duomenys, prie kurių priskiriamas, be kita ko, abonento ar registruoto naudotojo vardas ir pavardė arba pavadinimas, taip pat adresas, telefono numeriai, į kuriuos ir iš kurių skambinta, ir IP adresas interneto paslaugų teikimo atveju. Šie duomenys leidžia, be kita ko, nustatyti asmenį, su kuriuo vyko abonento ar registruoto naudotojo komunikacija, komunikacijos būdą, laiką ir vietą, iš kurios ji vykdyta. Be to, jie leidžia sužinoti, ar dažnai abonentas arba registruotas naudotojas ir tam tikri asmenys komunikavo konkrečiu laikotarpiu.

[15] Šis sprendimas pristatytas 2014 m. metiniame pranešime, p. 60.

Teisingumo Teismas visų pirma nusprendė, kad, Direktyvos 2006/24 nuostatomis šiems teikėjams nustačius tokias pareigas, jomis buvo labai apribotos pagrindinės teisės į privatų gyvenimą ir asmens duomenų apsaugą, užtikrinamos Chartijos 7 ir 8 straipsniuose. Tiesa, šiomis aplinkybėmis Teisingumo Teismas konstatavo, kad šį apribojimą galima pateisinti bendrojo intereso tikslu, kaip antai kova su organizuotu nusikalstamumu. Šiuo aspektu Teisingumo Teismas nurodė, kad, pirma, toje direktyvoje reikalaujama duomenų apsauga negali kelti pavojaus pagrindinių teisių į privatų gyvenimą ir asmens duomenų apsaugą esmei, nes neleidžia sužinoti paties elektroninių ryšių turinio, ir joje numatyta, kad paslaugų ar tinklų teikėjai turi laikytis tam tikrų apsaugos ir duomenų saugumo principų. Antra, Teisingumo Teismas pažymėjo, kad duomenų apsauga, siekiant juos galimai perduoti kompetentingoms nacionalinėms institucijoms, iš tikrųjų atitinka bendrojo intereso tikslą, t. y. kovą su dideliu nusikalstamumu, o galiausiai – visuomenės saugumą (38–44 punktai).

Vis dėlto Teisingumo Teismas laikėsi nuomonės, kad priimdamas direktyvą dėl duomenų apsaugos Sąjungos teisės aktų leidėjas peržengė ribas, kurios nustatomos pagal proporcingumo principą. Todėl šią direktyvą jis pripažino negaliojančia, konstatuodamas, kad joje nustatytas plataus masto ir ypač didelis pagrindinių teisių apribojimas nebuvo pakankamai reglamentuotas, siekiant užtikrinti, kad šis apribojimas neviršytų to, kas griežtai būtina (65 punktas). Direktyva 2006/24 bendrai taikoma visiems asmenims ir visoms elektroninio ryšio priemonėms, taip pat visiems srauto duomenims visiškai jų nediferencijuojant, nenumatant kokių nors ribojimų ar išimčių pagal kovos su sunkiais nusikaltimais tikslo kriterijų (57–59 punktai). Be to, šioje direktyvoje nenumatyta nei jokio objektyvaus kriterijaus, leidžiančio užtikrinti, kad kompetentingos nacionalinės institucijos galėtų susipažinti su duomenimis ir juos naudoti tik siekdamos užkirsti kelią nusikaltimams, kurie gali būti laikomi pakankamai sunkiais, kad būtų pateisintas toks apribojimas, juos nustatyti ar dėl jų vykdyti baudžiamąjį persekiojimą, nei materialinių ir procedūrinių tokios galimybės ar tokio naudojimo sąlygų (60–62 punktai). Galiausiai, kiek tai susiję su duomenų apsaugos laikotarpiu, toje direktyvoje nustatytas ne mažiau kaip šešių mėnesių laikotarpis ir nedaroma jokio skirtumo tarp duomenų kategorijų, atsižvelgiant į atitinkamus asmenis ar galimą duomenų naudingumą siekiamo tikslo atžvilgiu (63, 64 punktai).

Be to, kiek tai susiję su reikalavimais, kylančiais iš Chartijos 8 straipsnio 3 dalies, Teisingumo Teismas konstatavo, kad Direktyvoje 2006/24 nenumatyta pakankamai garantijų, leidžiančių užtikrinti veiksmingą duomenų apsaugą nuo piktnaudžiavimo rizikos ir nuo neteisėto susipažinimo su duomenimis ir jų naudojimo, taip pat joje nėra reikalavimo saugoti duomenis Sąjungos teritorijoje.

Taigi minėtoje direktyvoje nėra visapusiškai užtikrinta nepriklausomos institucijos atliekama apsaugos ir saugumo reikalavimų laikymosi kontrolė, kaip to aiškiai reikalaujama Chartijoje (66–68 punktai).

2. Teisės į asmens duomenų apsaugą užtikrinimas įgyvendinant Sąjungos teisę

2016 m. gruodžio 21 d. didžiosios kolegijos Sprendimas „Tele2 Sverige“ (sujungtos bylos C-203/15 ir C-698/15, EU:C:2016:970)[16]

Po to, kai Sprendimu *Digital Rights Ireland ir Seitlinger ir kt.* Direktyva 2006/24 buvo pripažinta negaliojančia (žr. pirmesnę dalį), Teisingumo Teismas išnagrinėjo dvi bylas dėl Švedijoje ir Jungtinėje Karalystėje elektroninių ryšių paslaugų teikėjams nustatytos bendros pareigos saugoti duomenis, susijusius su šiais ryšiais (šių duomenų saugojimas buvo numatytas negaliojančia pripažintoje direktyvoje).

Kitą dieną po to, kai buvo paskelbtas Sprendimas *Digital Rights Ireland ir Seitlinger ir kt.*, telekomunikacijų įmonė *Tele2 Sverige* pranešė Švedijos pašto ir telekomunikacijų priežiūros institucijai apie savo sprendimą nebesaugoti duomenų ir apie ketinimą ištrinti jau įrašytuosius (byla C-203/15). Elektroninių ryšių paslaugų teikėjus Švedijos teisė įpareigojo sistemingai ir nuolat, nedarant jokių išimčių, saugoti visus jų abonentų ir registruotų naudotojų srauto bei vietos nustatymo duomenis, susijusius su visomis elektroninio ryšio priemonėmis. Byloje C-698/15 trys asmenys pateikė skundą dėl Jungtinės Karalystės duomenų saugojimo tvarkos, kuri vidaus reikalų ministrui suteikė teisę įpareigoti viešuosius telekomunikacijų operatorius saugoti visus ryšių duomenis ne daugiau kaip dvylika mėnesių, tačiau šis įpareigojimas negalėjo būti taikomas šių ryšių turiniui.

Kammarrätten i Stockholm (Stokholmo apeliacinis administracinis teismas, Švedija) ir *Court of Appeal (England and Wales) (Civil Division)* (Anglijos ir Velso apeliacinio teismo civilinių bylų skyrius, Jungtinė Karalystė) kreipėsi į Teisingumo Teismą prašydami išaiškinti Direktyvos 2002/58 (vadinamos Direktyva dėl privatumo ir elektroninių ryšių) 15 straipsnio 1 dalį, pagal kurią valstybėms narėms suteikiama teisė nustatyti tam tikras šioje direktyvoje įtvirtintos pareigos užtikrinti elektroninių ryšių ir su jais susijusių srauto duomenų konfidencialumą išimtis.

Savo sprendime Teisingumo Teismas visų pirma konstatavo, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, draudžia nacionalinės teisės aktus, kaip antai galiojančius Švedijoje, kuriuose kovos su nusikalstamumu tikslais numatyta pareiga bendrai ir nediferencijuotai saugoti su visais abonentais ir registruotais naudotojais susijusius visus srauto ir vietos nustatymo duomenis, nesvarbu, kuriomis elektroninio ryšio priemonėmis jie perduoti. Anot Teisingumo Teismo, tokie teisės aktai viršija tai, kas griežtai būtina, ir negali būti laikomi pateisinamais demokratinėje visuomenėje, kaip to reikalaujama pagal minėto 15 straipsnio 1 dalį, siejamą su nurodytais Chartijos straipsniais (99–105, 107, 112 punktai ir rezoliucinės dalies 1 punktas).

Ta pati nuostata, siejama su tais pačiais Chartijos straipsniais, taip pat draudžia nacionalinės teisės aktus, reglamentuojančius srauto ir vietos nustatymo duomenų apsaugą ir saugumą, ypač kompetentingų nacionalinių institucijų prieigą prie saugomų duomenų, jeigu kovojant su nusikalstamumu tokia prieiga neapribojama tik kovos su sunkiais nusikaltimais tikslais, jai netaikoma išankstinė teismo ar nepriklausomos administracinės institucijos kontrolė ir nereikalaujama, kad nagrinėjami duomenys būtų saugomi Sąjungos teritorijoje (118–122, 125 punktai ir rezoliucinės dalies 2 punktas).

[16] Šis sprendimas pristatytas 2016 m. metiniame pranešime, p. 62.

Vis dėlto Teisingumo Teismas konstatavo, kad Direktyvos 2002/58 15 straipsnio 1 dalis nedraudžia teisės aktų, pagal kuriuos siekiant prevencijos leidžiamas tikslinis tokių duomenų saugojimas kovos su sunkiais nusikaltimais tikslais, su sąlyga, kad, kiek tai susiję su saugotinų duomenų kategorijomis, konkrečiomis ryšio priemonėmis, atitinkamais asmenimis ir numatyta saugojimo trukme, duomenų saugojimas būtų apribotas tuo, kas griežtai būtina. Tam, kad būtų tenkinami šie reikalavimai, tokiuose nacionalinės teisės aktuose visų pirma turi būti numatytos aiškios ir tikslios taisyklės, leidžiančios veiksmingai apsaugoti duomenis nuo piktnaudžiavimo pavojų. Juose konkrečiai turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis galima siekiant prevencijos numatyti duomenų saugojimo priemonę, taip užtikrinant, kad tokia priemonė neviršytų to, kas griežtai būtina. Antra, kiek tai susiję su materialinėmis sąlygomis, kurias turi tenkinti nacionalinės teisės aktai, pažymėtina, jog siekiant užtikrinti, kad tokie teisės aktai neviršytų to, kas griežtai būtina, duomenų saugojimas visada turi tenkinti objektyvius kriterijus, kuriais saugotini duomenys būtų susieti su siekiamu tikslu. Konkrečiai kalbant, tokios sąlygos turi leisti praktiškai veiksmingai nubrėžti priemonės dydžio ribas, o vėliau – nustatyti atitinkamą visuomenę. Kiek tai susiję su šiuo apribojimu, nacionalinės teisės aktai turi būti grindžiami objektyviais kriterijais, leidžiančiais nustatyti asmenis, kurių duomenys gali bent netiesiogiai atskleisti ryšį su sunkia nusikalstama veika, vienaip ar kitaip prisidėti prie kovos su sunkiais nusikaltimais arba užkirsti kelią dideliam pavojui visuomenės saugumui (108–111 punktai).

II. Asmens duomenų tvarkymas, kaip tai suprantama pagal Direktyvą 95/46

1. Asmens duomenų tvarkymas, nepatenkantis į Direktyvos 95/46 taikymo sritį

2006 m. gegužės 30 d. didžiosios kolegijos Sprendimas „Parlamentas / Taryba“ (C-317/04 ir C-318/04, EU:C:2006:346)

Po to, kai 2001 m. rugsėjo 11 d. buvo įvykdyti teroristiniai išpuoliai, Jungtinės Amerikos Valstijos (JAV) priėmė teisės aktus, kuriuose nustatyta, kad vežėjai oro transportu, teikiantys paslaugas maršrutais į JAV teritoriją, iš jos arba per ją, privalo suteikti JAV valdžios institucijoms elektroninę prieigą prie duomenų, esančių jų rezervacijos ir išvykimų kontrolės sistemose, vadinamose *Passenger Name Records* (PNR).

Manydama, kad šios nuostatos gali prieštarauti Sąjungos ir valstybių narių teisės aktams duomenų apsaugos srityje, Komisija pradėjo derybas su JAV valdžios institucijomis. Pasibaigus šioms deryboms, Komisija 2004 m. gegužės 14 d. priėmė Sprendimą 2004/535[17], jame konstatavo, kad Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnyba (*United States Bureau of Customs and Border Protection*, toliau – CBP) užtikrina tinkamą Bendrijos perduodamų PNR duomenų apsaugą (toliau – sprendimas dėl tinkamos apsaugos). Tada 2004 m. gegužės

[17] 2004 m. gegužės 14 d. Komisijos sprendimas 2004/535 dėl Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnybai perduodamų oro keleivių asmens duomenų, nurodytų Keleivio duomenų įraše (OL L 235, 2004, p. 11).

17 d. Taryba priėmė Sprendimą 2004/496[18], kuriuo sudaromas Europos bendrijos ir JAV susitarimas dėl Bendrijos valstybių narių teritorijoje įsteigtų vežėjų oro transportu PNR duomenų tvarkymo ir perdavimo CBP.

Europos Parlamentas paprašė Teisingumo Teismo panaikinti abu minėtus sprendimus, be kita ko, teigdamas, kad sprendimas dėl tinkamos apsaugos buvo priimtas *ultra vires*, kad EB 95 straipsnis (dabar SESV 114 straipsnis) nėra tinkamas sprendimo, kuriuo sudaromas tas susitarimas, teisinis pagrindas ir kad abiem atvejais buvo pažeistos pagrindinės teisės.

Kiek tai susiję su sprendimu dėl tinkamos apsaugos, Teisingumo Teismas visų pirma išnagrinėjo, ar Komisija pagrįstai galėjo priimti savo sprendimą, remdamasi Direktyva 95/46. Šiomis aplinkybėmis jis konstatavo, kad iš sprendimo dėl tinkamos apsaugos matyti, jog PNR duomenų perdavimas CBP yra tvarkymo operacija, susijusi su visuomenės saugumu ir su valstybės veiksmais baudžiamosios teisės srityje. Anot Teisingumo Teismo, nors PNR duomenis pirmiausia rinko vežėjai oro transportu Sąjungos teisei priskirtoje veiklos srityje, t. y. parduodami lėktuvo bilietą, kuris suteikia teisę gauti paslaugas, duomenų tvarkymas, į kurį atsižvelgiama sprendime dėl tinkamos apsaugos, yra visai kito pobūdžio. Iš tiesų šis sprendimas yra susijęs ne su duomenų tvarkymu, būtinu suteikti paslaugas, bet su duomenų tvarkymu, būtinu apginti visuomenės saugumui ir nubaudimo tikslais (56 ir 57 punktai).

Šiuo aspektu Teisingumo Teismas pažymėjo, kad tai, jog PNR duomenys komerciniais tikslais buvo renkami privačių subjektų, organizuojančių jų perdavimą į trečiąją valstybę, neužkerta kelio šį perdavimą laikyti duomenų perdavimu, kuriam netaikoma ši direktyva. Iš tiesų šis perdavimas vyksta pagal valstybės institucijų nustatytą tvarką, susijusią su visuomenės saugumu. Todėl Teisingumo Teismas padarė išvadą, kad sprendimas dėl tinkamos apsaugos nepatenka į tos direktyvos taikymo sritį, nes susijęs su asmens duomenų tvarkymu, kuriam ji netaikoma. Dėl šios priežasties Teisingumo Teismas panaikino sprendimą dėl tinkamos apsaugos (58 ir 59 punktai).

Kiek tai susiję su Tarybos sprendimu, Teisingumo Teismas konstatavo, kad EB 95 straipsniu, siejamu su Direktyvos 95/46 25 straipsniu, negali būti grindžiama Bendrijos kompetencija sudaryti nagrinėjamą susitarimą su JAV. Iš tiesų šis susitarimas susijęs su tuo pačiu duomenų perdavimu kaip ir sprendimas dėl tinkamos apsaugos, taigi su duomenų tvarkymu, kuris nepatenka į tos direktyvos taikymo sritį. Todėl Teisingumo Teismas panaikino Tarybos sprendimą, kuriuo sudaromas susitarimas (67–69 punktai).

2014 m. gruodžio 11 d. Sprendimas „Ryneš“ (C-212/13, EU:C:2014:2428)

Imdamasis atsakomųjų veiksmų į pasikartojančius išpuolius F. Ryneš savo name įrengė stebėjimo kamerą. Po naujo išpuolio, susijusio su jo namu, kameros įrašai leido identifikuoti du įtariamuosius; jų atžvilgiu buvo pradėtos baudžiamosios bylos. Vienam iš įtariamųjų Čekijos asmens duomenų apsaugos tarnyboje užginčijus stebėjimo kameros įrašytų duomenų tvarkymo teisėtumą, ši tarnyba konstatavo, kad F. Ryneš pažeidė asmens duomenų apsaugos taisykles, ir skyrė jam baudą.

[18] 2004 m. gegužės 17 d. Tarybos sprendimas 2004/496 dėl Europos bendrijos ir Jungtinių Amerikos Valstijų susitarimo dėl oro vežėjų PNR duomenų tvarkymo ir perdavimo Jungtinių Valstijų vidaus saugumo departamento Muitinių ir sienos apsaugos biurui sudarymo (OL L 183, 2004, p. 83).

Gavęs F. Ryneš skundą dėl *Městský soud v Praze* (Prahos miesto teismas, Čekijos Respublika) sprendimo, kuriuo buvo patvirtintas minėtos tarnybos sprendimas, *Nejvyšší správní soud* (Aukščiausiasis administracinis teismas, Čekijos Respublika) pateikė Teisingumo Teismui klausimą, ar F. Ryneš įrašas, siekiant apsaugoti jo gyvybę, sveikatą ir turtą, yra duomenų tvarkymas, kuriam netaikoma Direktyva 95/46, nes šį įrašą padarė fizinis asmuo, užsiimdamas tik asmenine ar namų ūkio veikla, kaip tai suprantama pagal minėtos direktyvos 3 straipsnio 2 dalies antrą įtrauką.

Teisingumo Teismas nusprendė, kad vaizdo stebėjimo darant asmenų vaizdo įrašus, saugomus nuolatinio įrašymo įrenginyje, kaip antai kietajame diske, sistemos, kurią fizinis asmuo įrengė ant savo šeimos namo, siekdamas apsaugoti namo savininkų turtą, sveikatą ir gyvybę, kai šia sistema stebima ir viešoji erdvė, naudojimas nėra asmens duomenų tvarkymas, atliekamas užsiimant tik asmenine ar namų ūkio veikla (35 punktas ir rezoliucinė dalis).

Šiuo aspektu jis priminė, kad Chartijos 7 straipsnyje užtikrinama pagrindinės teisės į privatų gyvenimą apsauga reikalauja, kad nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neviršytų to, kas yra griežtai būtina. Kadangi Direktyvos 95/46 nuostatas, kiek jomis reglamentuojant asmens duomenų tvarkymą gali būti keliamas pavojus pagrindinėms laisvėms, visų pirma teisei į privatų gyvenimą, būtina aiškinti atsižvelgiant į pagrindines teises, kurios yra įtrauktos į minėtą Chartiją, šios direktyvos 3 straipsnio 2 dalies antroje įtraukoje įtvirtinta nukrypti leidžianti nuostata turi būti aiškinama siaurai (27–29 punktai). Be to, pačia šios nuostatos formuluote iš Direktyvos 95/46 taikymo srities pašalintas duomenų tvarkymas, atliekamas užsiimant „tik“ asmenine ir namų ūkio veikla. Tiek, kiek vaizdo stebėjimas apima, net jei tik iš dalies, viešąją erdvę, ir stebėjimo įrenginys yra nukreiptas už taip duomenis tvarkančio asmens privačios sferos ribų, jis negali būti laikomas tik „asmenine ar namų ūkio“ veikla, kaip tai suprantama pagal minėtą nuostatą (30, 31 ir 33 punktai).

2. Sąvoka „asmens duomenys“

2016 m. spalio 19 d. Sprendimas „Breyer“ (C-582/14, EU:C:2016:779)[19]

P. Breyer pateikė ieškinį Vokietijos civiliniams teismams, prašydamas uždrausti Vokietijos Federacinei Respublikai saugoti arba įpareigoti trečiuosius asmenis saugoti kompiuterinius duomenis, kurie buvo perduodami kiekvieną kartą apsilankius Vokietijos federalinių tarnybų interneto svetainėse. Iš tiesų, siekiant išvengti atakų ir sudaryti galimybę vykdyti „piratų“ baudžiamąjį persekiojimą, Vokietijos federalinių tarnybų elektroninių paslaugų teikėjas įrašinėjo duomenis, kuriuos sudaro „dinaminis“ IP adresas (IP adresas, kintantis kaskart iš naujo jungiantis prie interneto), prisijungimo prie interneto svetainės data ir laikas. Kitaip nei statiniai IP adresai, dinaminiai IP adresai neleido *a priori* pasitelkti viešai prieinamų rinkmenų ir taip susieti konkretų kompiuterį su fizine prieiga prie tinklo, kurią naudoja interneto prieigos teikėjas. Vien įrašyti duomenys elektroninių paslaugų teikėjui nesuteikė galimybės nustatyti naudotojo tapatybės. Tačiau interneto prieigos teikėjas turėjo papildomos informacijos, kuri, jei būtų susieta su šiuo IP adresu, leistų nustatyti tokio naudotojo tapatybę.

[19] Šis sprendimas pristatytas 2016 m. metiniame pranešime, p. 61.

Šiomis aplinkybėmis gavęs kasacinį skundą *Bundesgerichtshof* (Federalinis Aukščiausiasis Teismas, Vokietija) pateikė Teisingumo Teismui klausimą, ar IP adresą, kurį elektroninių paslaugų teikėjas išsaugo asmeniui apsilankius šio teikėjo interneto svetainėje, jis turi laikyti asmens duomenimis.

Visų pirma Teisingumo Teismas pažymėjo, jog tam, kad duomenys būtų laikomi „asmens duomenimis“, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą, nereikalaujama, kad visą informaciją, leidžiančią nustatyti atitinkamo asmens tapatybę, turėtų vienas asmuo. Taigi dėl aplinkybės, kad papildomos informacijos, būtinos interneto svetainės naudotojo tapatybei nustatyti, turi ne elektroninių paslaugų teikėjas, o šio naudotojo interneto prieigos teikėjas, negalima atmesti galimybės, kad elektroninių paslaugų teikėjo išsaugotus dinaminius IP adresus jis turi laikyti asmens duomenimis, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą (43 ir 44 punktai).

Taigi Teisingumo Teismas konstatavo, kad dinaminį IP adresą, elektroninių paslaugų teikėjo išsaugotą asmeniui apsilankius interneto svetainėje, paties teikėjo padarytoje viešai prieinamoje, šis teikėjas turi laikyti asmens duomenimis, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą, jeigu turi teisėtų priemonių atitinkamo asmens tapatybei nustatyti, remdamasis papildoma informacija, kurios turi šio asmens interneto prieigos teikėjas (49 punktas ir rezoliucinės dalies 1 punktas).

2017 m. gruodžio 20 d. Sprendimas „Nowak“ (C-434/16, ECLI:EU:C:2017:994)

Apskaitininkas stažuotojas P. Nowak neišlaikė Airijos licencijuotų apskaitininkų instituto surengto egzamino. Remdamasis Duomenų apsaugos įstatymo 4 straipsniu jis paprašė leisti susipažinti su visais su juo susijusiais asmens duomenimis, kuriuos turėjo licencijuotų apskaitininkų institutas. Šis perdavė P. Nowak tam tikrus dokumentus, tačiau atsisakė perduoti jo egzamino darbo kopiją, motyvuodamas tuo, kad joje nebuvo su juo susijusių asmens duomenų, kaip tai suprantama pagal Duomenų apsaugos įstatymą.

Kadangi duomenų apsaugos komisaras dėl tų pačių motyvų taip pat nepatenkino jo prašymo leisti susipažinti su dokumentais, P. Nowak kreipėsi į nacionalinius teismus. Gavęs P. Nowak skundą *Supreme Court* (Aukščiausiasis Teismas, Airija) pateikė Teisingumo Teismui klausimą, ar Direktyvos 95/46 2 straipsnio a punktą reikia aiškinti taip, kad tokiomis sąlygomis, kaip nagrinėtos pagrindinėje byloje, profesinį egzaminą laikančio asmens raštiški atsakymai ir egzaminuotojo galimai dėl šių atsakymų pateiktos pastabos yra su egzaminuojamuoju susiję asmens duomenys, kaip tai suprantama pagal šią nuostatą.

Pirma, Teisingumo Teismas pažymėjo, jog tam, kad duomenys galėtų būti laikomi „asmens duomenimis“, kaip tai suprantama pagal Direktyvos 95/46 2 straipsnio a punktą, nereikalaujama, kad visą informaciją, leidžiančią nustatyti atitinkamo asmens tapatybę, turėtų vienas asmuo. Be to, tuo atveju, kai egzaminuotojas, vertindamas egzaminuojamojo per egzaminą pateiktus atsakymus, nežino jo tapatybės, egzaminą organizuojantis subjektas, šiuo atveju licencijuotų apskaitininkų institutas, disponuoja būtina informacija, leidžiančia jam lengvai ir aiškiai nustatyti šio egzaminuojamojo tapatybę pagal jo egzamino darbo kopijoje arba ant šios kopijos viršelio nurodytą identifikacijos numerį ir taip priskirti jam jo atsakymus.

Antra, Teisingumo Teismas konstatavo, kad profesinį egzaminą laikančio asmens raštiški atsakymai yra su juo susijusi informacija. Iš tiesų šių atsakymų turinys atspindi egzaminuojamojo žinių lygį ir kompetenciją konkrečioje srityje ir atitinkamai jo mąstymo procesus, vertinimą ir kritiškumą. Be to, gaunant minėtus atsakymus siekiama įvertinti egzaminuojamojo profesinius gebėjimus, ypač jo gebėjimą vykdyti atitinkamas profesines užduotis. Pagaliau šios informacijos panaudojimas, dėl kurio egzaminuojamasis, pavyzdžiui, išlaiko atitinkamą egzaminą arba jo neišlaiko, gali daryti poveikį jo teisėms ir interesams, nes gali nulemti jo galimybes užsiimti pageidaujama profesija ar darbine veikla arba turėti tam įtakos. Išvada, kad profesinį egzaminą laikančio asmens pateikti raštiški atsakymai yra informacija, kuri, atsižvelgiant į jos turinį, tikslą ir poveikį, yra su juo susijusi, galioja ir tuomet, kai egzamine galima naudotis turima medžiaga (31 ir 36–40 punktai).

Trečia, kiek tai susiję su egzaminuotojo pastabomis dėl egzaminuojamojo atsakymų, Teisingumo Teismas laikėsi nuomonės, kad jos, kaip ir egzaminuojamojo per egzaminą pateikti atsakymai, yra su egzaminuojamuoju susijusi informacija, nes atspindi egzaminuotojo nuomonę ar vertinimą dėl asmeninių egzaminuojamojo egzamino rezultatų, konkrečiai – dėl jo žinių ir gebėjimų atitinkamoje srityje. Be to, tokiomis pastabomis konkrečiai siekiama užfiksuoti tai, kaip egzaminuotojas vertina egzaminuojamojo rezultatus, ir jos gali turėti jam poveikį (42 ir 43 punktai).

Ketvirta, Teisingumo Teismas nusprendė, kad egzaminuojamojo per profesinį egzaminą pateikti raštiški atsakymai ir su jais susijusios galimos egzaminuotojo pastabos gali būti patikrinti, pirmiausia, kiek tai susiję jų tikslumu ir būtinybe juos saugoti, kaip tai suprantama pagal Direktyvos 95/46 6 straipsnio 1 dalies d ir e punktus, ir gali būti pataisyti arba ištrinti, remiantis jos 12 straipsnio b punktu. Tai, kad egzaminuojamajam suteikiama teisė susipažinti su šiais atsakymais ir šiomis pastabomis pagal šios direktyvos 12 straipsnio a punktą, padeda siekti šiame straipsnyje nustatyto tikslo – užtikrinti egzaminuojamojo teisės į privatų gyvenimą apsaugą tvarkant su juo susijusius asmens duomenis, neatsižvelgiant į tai, ar tas egzaminuojamasis turi tokią teisę susipažinti su jo asmens duomenimis ir pagal egzamino procedūrai taikomus nacionalinės teisės aktus. Vis dėlto Teisingumo Teismas pabrėžė, kad teisė susipažinti su informacija ir teisė ją ištaisyti, remiantis Direktyvos 95/46 12 straipsnio a ir b punktais, netaikoma egzamino klausimams, kurie, kaip tokie, nėra egzaminuojamojo asmens duomenys (56 ir 58 punktai).

Atsižvelgdamas į tai, kas išdėstyta, Teisingumo Teismas priėjo prie išvados, kad tokiomis aplinkybėmis, kaip nagrinėtos pagrindinėje byloje, profesinį egzaminą laikančio asmens raštiški atsakymai ir egzaminuotojo galimai dėl šių atsakymų pateiktos pastabos yra asmens duomenys, kaip tai suprantama pagal Direktyvos 95/46 2 straipsnio a punktą (62 punktas ir rezoliucinė dalis).

3. Sąvoka „asmens duomenų tvarkymas“

2003 m. lapkričio 6 d. didžiosios kolegijos Sprendimas „Lindqvist“ (C-101/01, EU:C:2003:596)

Švedijos protestantų bažnyčios parapijos savanorė B. Lindqvist savo kompiuteryje sukūrė interneto puslapius ir juose paskelbė kelių toje parapijoje kaip ir ji dirbančių savanorių asmens duomenis. B. Lindqvist buvo skirta bauda, motyvuojant tuo, kad ji panaudojo asmens duomenis

juos tvarkydama automatiniu būdu, iš anksto raštu nepranešusi Švedijos *Datainspektion* (viešosios teisės reglamentuojama kompiuteriais perduodamų duomenų apsaugos įstaiga), kad be leidimo juos perdavė į trečiąsias šalis ir apskritai tvarkė jautrius asmens duomenis.

Nagrinėdamas B. Lindqvist apeliacinį skundą dėl šio sprendimo *Göta hovrätt* (Apeliacinis teismas, Švedija) Teisingumo Teismui pateikė prašymą priimti prejudicinį sprendimą, visų pirma klausdamas, ar B. Lindqvist „visiškai ar iš dalies automatiniais būdais [tvarkė] asmens duomenis“, kaip tai suprantama pagal Direktyvą 95/46.

Teisingumo Teismas konstatavo, kad operacijos, kai interneto puslapyje minimi įvairūs asmenys, kurių tapatybė atskleidžiama nurodant pavardę arba kitus duomenis, pavyzdžiui, telefono numerį ar su darbo sąlygomis ir pomėgiais susijusią informaciją, yra atliktos „visiškai ar iš dalies automatiniais būdais tvarkant asmens duomenis“, kaip tai suprantama pagal tą direktyvą (27 punktas ir rezoliucinės dalies 1 punktas). Iš tiesų vykdant savanorišką ar religinę veiklą tokiam asmens duomenų tvarkymui netaikoma jokia šios direktyvos taikymo srities išimtis, nes jis nepriskiriamas nei prie su visuomenės saugumu susijusios veiklos kategorijos, nei prie tik asmeninės ar namų ūkio veiklos kategorijų, kurioms ši direktyva netaikoma (38, 43–48 punktai ir rezoliucinės dalies 2 punktas).

2014 m. gegužės 13 d. didžiosios kolegijos Sprendimas „Google Spain ir Google“ (C-131/12, EU:C:2014:317)

2010 m. Ispanijos pilietis pateikė *Agencia Española de Protección de Datos* (Ispanijos duomenų apsaugos agentūra, toliau – IDAA) skundą dėl Ispanijoje populiaraus dienraščio leidėjo *La Vanguardia Ediciones SL* ir dėl *Google Spain* ir *Google*. Šis asmuo teigė, kad kai interneto vartotojas į *Google* grupės paieškos variklį įvesdavo savo pavardę, rezultatų sąraše buvo pateikiamos nuorodos į du 1998 m. dienraščio *La Vanguardia* puslapius, kuriuose, be kita ko, skelbiama apie nekilnojamojo turto, areštuoto siekiant sugrąžinti skolas, pardavimą aukcione. Savo skunde šis asmuo prašė, pirma, nurodyti *La Vanguardia* panaikinti ar pakeisti atitinkamus puslapius arba panaudoti tam tikras paieškos variklių teikiamas priemones tam, kad būtų apsaugoti šie duomenys. Antra, jis prašė nurodyti *Google Spain* ar *Google* pašalinti arba paslėpti jo asmens duomenis, kad jie nebūtų pateikiami paieškos rezultatų sąraše ir nuorodose į *La Vanguardia*.

IDAA atmetė skundą dėl *La Vanguardia*, teigdama, kad leidėjas teisėtai paskelbė nagrinėjamą informaciją, tačiau jį pripažino pagrįstu, kiek jis susijęs su *Google Spain* ir *Google*, ir paprašė šių dviejų bendrovių imtis reikiamų priemonių, kad duomenys būtų pašalinti iš jų rodyklės ir kad neliktų prieigos prie jų. Šioms bendrovėms pateikus du skundus *Audiencia Nacional* (Nacionalinis teismas, Ispanija) ir paprašius panaikinti IDAA sprendimą, šis Ispanijos teismas pateikė Teisingumo Teismui tam tikrus klausimus.

Taip Teisingumo Teismui buvo suteikta galimybė patikslinti sąvoką „asmens duomenų tvarkymas“ internete pagal Direktyvą 95/46.

Teisingumo Teismas nusprendė, kad paieškos variklio operacijos, kurias sudaro internete trečiųjų asmenų paskelbtos ar įkeltos informacijos suradimas, automatiniu būdu atliekamas jos indeksavimas, laikinas laikymas ir galiausiai padarymas prieinamos interneto vartotojams tam tikra pasirinkta tvarka, laikytinos asmens duomenų tvarkymu, jei ši informacija apima asmens duomenis (rezoliucinės dalies 1 punktas). Be to, Teisingumo Teismas priminė, kad operacijos,

apie kurias kalbama toje direktyvoje, turi būti laikomos tvarkymu, įskaitant atvejį, kai jos susijusios vien su žiniasklaidos priemonėse jau paskelbta informacija. Bendra direktyvos taikymo išimtis tokiu atveju panaikintų didžiąją jos prasmės dalį (29 ir 30 punktai).

2018 m. liepos 10 d. didžiosios kolegijos Sprendimas „Jehovan todistajat“ (C-25/17, ECLI:EU:C:2018:551)[20]

Pagrindinėje byloje Suomijos duomenų apsaugos institucija priėmė sprendimą uždrausti Jehovos liudytojų bendruomenei rinkti ar tvarkyti asmens duomenis jos nariams vykdant tikėjimo skelbimo „nuo durų iki durų“ veiklą, jeigu nesilaikoma asmens duomenų tvarkymą reglamentuojančiuose Suomijos teisės aktuose nustatytų reikalavimų. Iš tiesų vykdydami tikėjimo skelbimo „nuo durų iki durų“ veiklą šios bendruomenės nariai užsirašo informaciją lankydamiesi pas asmenis, kurių jie patys ar jų bendruomenė nepažįsta. Tokie duomenys renkami sukuriant atmintinę tam, kad juos galima būtų susirasti, jeigu būtų rengiamas vėlesnis vizitas, nors atitinkami asmenys tam nedavė sutikimo ir nebuvo apie tai informuoti. Šiuo aspektu Jehovos liudytojų bendruomenė savo nariams nustatė gaires, kaip daryti tokius užrašus, ir tokie nurodymai paskelbti bent viename iš šios bendruomenės leidinių, skirtų tikėjimui skelbti.

Teisingumo Teismas nusprendė, kad religinės bendruomenės narių atliekamo asmens duomenų rinkimo vykdant skelbimo „nuo durų iki durų“ veiklą ir vėlesnio jų tvarkymo neapima Direktyvos 95/46 taikymo srities išimtys, nes tai nėra nei asmens duomenų tvarkymas vykdant šios direktyvos 3 straipsnio 2 dalies pirmoje įtraukoje nurodytą veiklą, nei asmens duomenų tvarkymas užsiimant tik asmenine ar namų ūkio veikla, kaip tai suprantama pagal minėtos direktyvos 3 straipsnio 2 dalies antrą įtrauką (51 punktas ir rezoliucinės dalies 1 punktas).

2019 m. vasario 14 d. Sprendimas „Buivids“ (C-345/17, EU:C:2019:122)

Toje byloje Teisingumo Teismas išaiškino Direktyvos 95/46 taikymo sritį ir šios direktyvos 9 straipsnyje vartojamą sąvoką „asmens duomenų tvarkymas tik žurnalistiniais sumetimais“.

Šis sprendimas priimtas nagrinėjant prašymą priimti prejudicinį sprendimą, kurį pateikė Latvijos Aukščiausiasis Teismas, nagrinėjęs S. Buivids (toliau – ieškovas) ir Nacionalinės duomenų apsaugos institucijos ginčą dėl skundo, kuriuo prašoma pripažinti neteisėtu šios institucijos sprendimą, kad šis asmuo pažeidė nacionalinės teisės aktus asmens duomenų apsaugos srityje, kai interneto svetainėje paskelbė savo paties nufilmuotą vaizdo įrašą, kuriame užfiksuota, kaip nacionalinės policijos nuovados patalpose iš jo buvo imami parodymai administracinio nusižengimo byloje. Po to, kai du žemesnės instancijos teismai atmetė jo skundą, ieškovas pateikė Aukščiausiajam Teismui kasacinį skundą. Šiame teisme jis rėmėsi savo teise į saviraiškos laisvę ir teigė, kad aptariamame vaizdo įraše nacionalinės policijos pareigūnai, kurie yra vieši asmenys, yra viešoje vietoje, todėl jiems netaikomos Duomenų apsaugos įstatymo nuostatos.

Visų pirma dėl Direktyvos 95/46 taikymo srities Teisingumo Teismas pažymėjo, kad, pirma, į aptariamą vaizdo įrašą įrašyti policijos darbuotojų atvaizdai yra asmens duomenys, ir, antra, šių asmenų vaizdo įrašo, saugomo ieškovo naudotos vaizdo kameros atmintyje, įrašymas yra

[20] Šis sprendimas pristatytas 2018 m. metiniame pranešime, p. 87 ir 88.

asmens duomenų tvarkymas. Teisingumo Teismas pridūrė, kad vaizdo įrašo, kuriame yra asmens duomenų, paskelbimas vaizdo įrašų interneto svetainėje, kur naudotojai gali žiūrėti vaizdo įrašus ir jais dalytis, yra visiškai arba iš dalies automatizuotas šių duomenų tvarkymas. Be to, Teisingumo Teismas pabrėžė, kad minėtam įrašui ir jo paskelbimui netaikomos Direktyvos 95/46 taikymo srities išimtys, be kita ko, susijusios su asmens duomenų tvarkymu, vykdomu užsiimant veikla, kuri nepatenka į šios direktyvos taikymo sritį, ir tvarkymu, vykdomu užsiimant tik asmenine ar namų ūkio veikla. Taigi Teisingumo Teismas padarė išvadą, kad į šios direktyvos taikymo sritį patenka vaizdo įrašas, kuriame užfiksuoti policijos darbuotojai, nuovadoje imantys parodymus, ir šio įrašo paskelbimas vaizdo įrašų interneto svetainėje, kurioje vartotojai gali juos įkelti, žiūrėti ir jais dalytis (31, 32, 35, 39, 42, 43 punktai ir rezoliucinės dalies 1 punktas).

Antra, dėl sąvokos „asmens duomenų tvarkymas tik žurnalistiniais sumetimais“ apimties Teisingumo Teismas pirmiausia priminė, kad plačiai aiškinant sąvoką „žurnalistika“ Direktyvos 95/46 9 straipsnyje numatytos išimtys ir leidžiančios nukrypti nuostatos taikomos visiems asmenims, vykdantiems žurnalistikos veiklą. Taigi Teisingumo Teismas nusprendė, jog tai, kad ieškovas nėra profesionalus žurnalistas, nereiškia, kad aptariamo vaizdo įrašo įrašymas ir perdavimas negali būti laikomi „asmens duomenų tvarkymu tik žurnalistiniais sumetimais“. Be to, Teisingumo Teismas pabrėžė, kad Direktyvos 95/46 9 straipsnyje numatytos išimtys ir leidžiančios nukrypti nuostatos turi būti taikomos tik tiek, kiek jos būtinos siekiant suderinti dvi pagrindines teises, t. y. teisę į privataus gyvenimo gerbimą ir teisę į saviraiškos laisvę. Šiuo klausimu Teisingumo Teismas patikslino, kad negalima atmesti galimybės, jog aptariamo vaizdo įrašymas ir jo paskelbimas šiame vaizdo įraše užfiksuotiems policijos darbuotojams nepranešus apie šį įrašą ir jo tikslus yra pagrindinės teisės į šių asmenų privataus gyvenimo gerbimą apribojimas. Todėl jis padarė išvadą, kad aptariamo vaizdo įrašymas ir paskelbimas vaizdo įrašų interneto svetainėje gali būti asmens duomenų tvarkymas tik žurnalistiniais sumetimais, jeigu iš minėto vaizdo įrašo matyti, kad minėtu įrašymu ir paskelbimu siekiama vienintelio tikslo – skleisti visuomenei informaciją, nuomones ar idėjas, o tai turi patikrinti prašymą priimti prejudicinį sprendimą pateikęs teismas (51, 52, 55, 63, 67 punktai ir rezoliucinės dalies 2 punktas).

2021 m. birželio 21 d. didžiosios kolegijos Sprendimas „Latvijas Republikas Saeima“ (Baudos taškai) (C-439/19, EU:C:2021:504)

Fiziniam asmeniui B už vieną ar kelis kelių eismo taisyklių pažeidimus buvo skirti baudos taškai. *Ceļu satiksmes drošības direkcija* (Kelių eismo saugumo direkcija, Latvija; toliau – CSDD) šiuos baudos taškus įtraukė į nacionalinį transporto priemonių ir jų vairuotojų registrą.

Pagal Latvijos teisės nuostatas, kuriomis reglamentuojamas kelių eismas[21], informacija apie į šį registrą įtrauktus transporto priemonių vairuotojams skirtus baudos taškus prieinama visuomenei ir CSDD ją atskleidžia bet kuriam to paprašiusiam asmeniui, įskaitant ūkio subjektus siekiant pakartotinai naudoti, ir šis asmuo neprivalo konkrečiai pagrįsti savo suinteresuotumo gauti šią informaciją. Kilus abejonių dėl šių nuostatų teisėtumo, B pateikė konstitucinį skundą *Latvijas Republikas Satversmes tiesa* (Konstitucinis Teismas, Latvija), kad šis išnagrinėtų, ar šios nuostatos suderinamos su teise į privatų gyvenimą.

[21] 1997 m. spalio 1 d. *Ceļu satiksmes likums* (Kelių eismo įstatymas), (Latvijas Vēstnesis, 1997, nº 274/276) 14^1 straipsnio 2 dalis.

Konstitucinis Teismas konstatavo, kad vertindamas šią konstitucinę teisę turi atsižvelgti į BDAR. Taigi, siekdamas išsiaiškinti, ar Latvijos teisės nuostatos, reglamentuojančios kelių eismą, suderinamos su šiuo reglamentu, jis Teisingumo Teismo paprašė paaiškinti kelių BDAR nuostatų apimtį.

Savo sprendime Teisingumo Teismo didžioji kolegija nusprendė, kad asmens duomenų apie baudos taškus tvarkymas yra „asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas“[22], kuriam dėl aptariamų duomenų ypatingo jautrumo BDAR numatyta didesnė apsauga (10, 46, 74, 94 punktai ir rezoliucinės dalies 1 punktas).

Šiuo klausimu jis pirmiausia pažymėjo, kad informacija apie baudos taškus yra asmens duomenys ir CSDD atliekamas jų atskleidimas yra tvarkymas, kuris patenka į BDAR materialinę taikymo sritį. Iš tiesų ši taikymo sritis yra labai plati ir šis tvarkymas nepriskiriamas prie šio reglamento taikymo išimčių (60, 61 ir 72 punktai).

Taigi, viena vertus, šio tvarkymo neapima išimtis, susijusi su BDAR netaikymu duomenų tvarkymui vykdant veiklą, kuriai netaikoma Sąjungos teisė[23]. Laikytina, kad vienintelis šios išimties tikslas – į šio reglamento taikymo sritį neįtraukti asmens duomenų tvarkymo, kai jį atlieka valstybės institucijos, vykdydamos veiklą, kuria siekiama užtikrinti nacionalinį saugumą, arba veiklą, kuri gali būti priskirta prie tos pačios kategorijos. Visų pirma tai apima veiklą, skirtą apsaugoti esminėms valstybės funkcijoms ir pagrindiniams visuomenės interesams. Su kelių eismo saugumu susijusia veikla nesiekiama šio tikslo, taigi jos negalima priskirti prie veiklos, kuria siekiama užtikrinti nacionalinį saugumą, kategorijos (62 ir 66–68 punktai).

Kita vertus, asmens duomenų apie baudos taškus atskleidimas taip pat nėra tvarkymas, kurį apima išimtis dėl BDAR netaikymo kompetentingų institucijų atliekamam asmens duomenų tvarkymui baudžiamosios teisės srityje[24]. Teisingumo Teismas konstatavo, kad atlikdama minėtą duomenų atskleidimą CSDD negali būti laikoma „kompetentinga institucija“[25] (69–71 punktai).

Siekdamas nustatyti, ar galimybė susipažinti su asmens duomenimis apie kelių eismo taisyklių pažeidimus, kaip antai baudos taškais, yra asmens duomenų apie „nusikalstamas veikas“[26], kuriems suteikta didesnė apsauga, tvarkymas, Teisingumo Teismas, be kita ko, remdamasis BDAR geneze, konstatavo, kad ši nuostata reiškia tik baudžiamojo pobūdžio pažeidimus. Tačiau aplinkybė, kad Latvijos teisės sistemoje kelių eismo taisyklių pažeidimai laikomi administraciniais nusižengimais, neturi lemiamos reikšmės vertinant, ar šie pažeidimai patenka į sąvoką „nusikalstama veika“, nes tai yra savarankiška Sąjungos teisės sąvoka, kuri visoje Sąjungoje turi būti aiškinama savarankiškai ir vienodai. Taigi priminęs tris kriterijus, kurie yra svarbūs vertinant, ar pažeidimas yra baudžiamojo pobūdžio – teisinį jo kvalifikavimą pagal nacionalinę teisę, pažeidimo pobūdį ir suinteresuotajam asmeniui gresiančios sankcijos griežtumo laipsnį – Teisingumo Teismas nusprendė, kad aptariami kelių eismo taisyklių pažeidimai patenka į sąvoką „nusikalstama veika“, kaip ji suprantama pagal BDAR. Dėl pirmųjų dviejų kriterijų Teisingumo

---

22 BDAR 10 straipsnis.

23 BDAR 2 straipsnio 2 dalies a punktas.

24 BDAR 2 straipsnio 2 dalies a punktas.

25 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89) 3 straipsnio 7 punktas.

26 BDAR 10 straipsnis.

Teismas konstatavo, kad net jei pažeidimai pagal nacionalinę teisę nėra laikomi „baudžiamaisiais“, jie gali būti tokie atsižvelgiant į pažeidimo pobūdį ir, be kita ko, į sankcija, kuri gali būti skirtą už tokį pažeidimą, siekiamą tikslą nubausti. Nagrinėjamu atveju skiriant baudos taškus už kelių eismo taisyklių pažeidimus, kaip ir kitomis sankcijomis, kurios gali būti už juos skirtos, be kita ko, siekiama tokio tikslo nubausti. Dėl trečiojo kriterijaus Teisingumo Teismas pažymėjo, kad baudos taškai skiriami tik už tam tikro sunkumo kelių eismo taisyklių pažeidimus, taigi už juos gali būti taikomos tam tikro griežtumo sankcijos. Be to, paprastai tokie taškai skiriami papildomai, kartu su už tokį pažeidimą pritaikyta sankcija, ir šių taškų sumavimas sukelia teisinių padarinių, tam tikrais atvejais net draudimą vairuoti (77, 80, 85, 87–90 ir 93 punktai).

4. Sąvoka „asmens duomenų susistemintas rinkinys“

2018 m. liepos 10 d. didžiosios kolegijos Sprendimas „Jehovan todistajat“ (C-25/17, ECLI:EU:C:2018:551)

Šiame sprendime (taip pat žr. II.3 skyrių „Sąvoka „asmens duomenų tvarkymas“) Teisingumo Teismas patikslino Direktyvos 95/46 2 straipsnio c punkte vartojamą sąvoką „susistemintas rinkinys“.

Priminęs, kad ši direktyva taikoma asmens duomenų tvarkymui rankiniu būdu, tik jeigu tvarkomi duomenys sudaro susisteminto rinkinio dalį arba yra skirti jai sudaryti, Teisingumo Teismas pažymėjo, kad ši sąvoka apima visumą asmens duomenų, kurie surinkti vykdant tikėjimo skelbimo „nuo durų iki durų“ veiklą ir kuriuos sudaro aplankytų asmenų vardai, pavardės, adresai ir kita su jais susijusi informacija, jeigu šie duomenys susisteminti pagal nustatytus kriterijus, kurie praktiškai sudaro galimybę tokius duomenis lengvai rasti siekiant juos toliau naudoti. Kad ši sąvoka apimtų tokią duomenų visumą, nebūtina, kad joje būtų konkrečių kortelių, sąrašų ar kitų paieškos sistemų (62 punktas ir rezoliucinės dalies 2 punktas).

5. Sąvoka „asmens duomenų valdytojas“

2018 m. liepos 10 d. didžiosios kolegijos Sprendimas „Jehovan todistajat“ (C-25/17, ECLI:EU:C:2018:551)

Šioje byloje (taip pat žr. II.3 ir II.4 skyrius „Sąvoka „Asmens duomenų tvarkymas“ ir „Sąvoka „Asmens duomenų susistemintas rinkinys“) Teisingumo Teismas priėmė sprendimą dėl religinės bendruomenės atsakomybės už asmens duomenų tvarkymą, atliekamą vykdant šios bendruomenės organizuotą, koordinuojamą ir skatinamą tikėjimo skelbimo „nuo durų iki durų“ veiklą.

Teisingumo Teismas konstatavo, kad kiekvieno asmens pareiga laikytis asmens duomenų apsaugą reglamentuojančių Sąjungos teisės normų negali būti laikoma religinių bendruomenių organizacinės autonomijos ribojimu. Šiuo klausimu jis padarė išvadą, kad Direktyvos 95/46 2 straipsnio d punktas, siejamas su Chartijos 10 straipsnio 1 dalimi, turi būti aiškinamas taip, kad pagal jį religinę bendruomenę kartu su tikėjimą skelbiančiais jos nariais galima laikyti asmens duomenų, kuriuos tokie nariai renka vykdydami tikėjimo skelbimo „nuo durų iki durų“ veiklą, kurią ši bendruomenė organizuoja, koordinuoja ir skatina, valdytoja, ir nebūtina, kad tokia

bendruomenė turėtų galimybę susipažinti su šiais duomenimis, taip pat nereikia įrodyti, kad ji savo nariams nustatė rašytines gaires arba pavedimus dėl tokių duomenų tvarkymo (74, 75 punktai ir rezoliucinės dalies 3 punktas).

2018 m. birželio 5 d. didžiosios kolegijos Sprendimas „Wirtschaftsakademie Schleswig Holstein" (C-210/16, ECLI:EU:C:2018:388)[27]

Vokietijos duomenų apsaugos institucija, kaip priežiūros institucija, kaip tai suprantama pagal Direktyvos 95/46 28 straipsnį, nurodė Vokietijos mokymo bendrovei, teikiančiai mokymo paslaugas per *Facebook* esantį gerbėjų tinklalapį, deaktyvuoti šį tinklalapį. Iš tiesų, minėtos institucijos teigimu, nei ši bendrovė, nei *Facebook* nepranešė gerbėjų tinklalapio lankytojams, kad naudodamos slapukus renka jų asmens duomenis, paskui juos tvarko.

Šiomis aplinkybėmis Teisingumo Teismas paaiškino sąvoką asmens „duomenų valdytojas". Šiuo klausimu jis konstatavo, kad *Facebook* esančio gerbėjų tinklalapio administratorius, kaip antai pagrindinėje byloje aptariama bendrovė, parinkdamas nustatymus (be kita ko, pagal tikslinę auditoriją ir veiklos valdymo ir skatinimo tikslus), dalyvauja šio tinklalapio lankytojų asmens duomenų tvarkymo ir priemonių nustatymo veikloje. Todėl, Teisingumo Teismo teigimu, šis administratorius kartu su *Facebook Ireland* (JAV bendrovės *Facebook* patronuojamoji bendrovė Sąjungoje) Sąjungoje turi būti laikomas tokių duomenų valdytoju, kaip jis suprantamas pagal Direktyvos 95/46 2 straipsnio d punktą (39 punktas).

2019 m. liepos 29 d. Sprendimas „Fashion ID" (C-40/17, EU:C:2019:629)

Šioje byloje Teisingumo Teismas turėjo galimybę išplėtoti sąvoką „duomenų valdytojas", atsižvelgdamas į „plugiciel" integravimą į interneto svetainę.

Šiuo atveju Vokietijos drabužių pardavimo internete įmonė *Fashion ID* į savo interneto svetainę įterpė socialinio tinklo *Facebook* socialinį modulį „Patinka". Atrodo, kad dėl šio įterpimo, kai lankytojas apsilanko *Fashion ID* interneto svetainėje, jo asmens duomenys perduodami *Facebook Ireland*. Toks perdavimas vyksta minėtam lankytojui to nežinant ir neatsižvelgiant į tai, ar jis yra socialinio tinklo *Facebook* narys ir ar spustelėjo *Facebook* mygtuką „Patinka".

Verbraucherzentrale NRW, Vokietijos visuomeninė vartotojų teisių gynimo asociacija, priekaištauja *Fashion ID* dėl to, kad ji savo interneto svetainės lankytojų asmens duomenis perdavė *Facebook Ireland*, viena vertus, be jų sutikimo ir, kita vertus, pažeisdama informavimo reikalavimus, nustatytus asmens duomenų apsaugos nuostatose. Nagrinėdamas ginčą *Oberlandesgericht Düsseldorf* (Diuseldorfo aukštesnysis apygardos teismas, Vokietija) paprašė Teisingumo Teismo išaiškinti kelias Direktyvos 95/46 nuostatas.

Teisingumo Teismas iš pradžių konstatavo, kad Interneto svetainės administratorius, kaip antai *Fashion ID*, gali būti laikomas duomenų valdytoju, kaip tai suprantama pagal Direktyvos 95/46 2 straipsnio d punktą. Vis dėlto tokia atsakomybė jam tenka tik už tą asmens duomenų tvarkymo operaciją arba operacijų visumą, kurių tikslus ir būdus jis realiai nustatė, t. y. už nagrinėjamą

[27] Šis sprendimas pristatytas 2018 m. metiniame pranešime, p. 86 ir 87.

duomenų rinkimą ir perdavimą. Tačiau, anot Teisingumo Teismo, *prima facie* neatrodo, kad *Fashion ID* nustato vėlesnių asmens duomenų tvarkymo operacijų, kurias atlieka *Facebook Ireland* po to, kai jai perduodami minėti duomenys, tikslus ir būdus, todėl *Fashion ID* neturėtų būti laikoma atsakinga už šias operacijas, kaip tai suprantama pagal šio 2 straipsnio d punktą (76, 85 punktai ir rezoliucinės dalies 2 punktas).

Be to, Teisingumo Teismas pabrėžė, jog būtina, kad kiekvienas interneto svetainės administratorius ir socialinio modulio teikėjas, kaip antai *Facebook Ireland*, tokiomis tvarkymo operacijomis siektų teisėtų interesų, kaip tai suprantama pagal Direktyvos 95/46 7 straipsnio f punktą, kad tokios operacijos galėtų būti pagrįstos (97 punktas ir rezoliucinės dalies 3 punktas).

Galiausiai Teisingumo Teismas pažymėjo, kad Direktyvos 95/46 2 straipsnio h punkte ir 7 straipsnio a punkte nurodyto atitinkamo asmens sutikimą interneto svetainės administratorius turi gauti tik dėl tų asmens duomenų tvarkymo operacijų, kurių tikslus ir būdus jis nustato. Tokiu atveju šios direktyvos 10 straipsnyje numatyta pareiga pateikti informaciją tenka ir minėtam valdytojui, tačiau informacija, kurią jis privalo pateikti duomenų subjektui, turi būti susijusi tik su asmens duomenų tvarkymo operacija ar operacijų visuma, kurių tikslus ir būdus jis nustato (106 punktas ir rezoliucinės dalies 4 punktas).

2020 m. liepos 9 d. Sprendimas „Land Hessen“ (C-272/19, EU:C:2020:535)

Peticiją Heseno federalinės žemės (Vokietija) parlamento Peticijų komitetui pateikęs pilietis prašė leisti susipažinti su jo asmens duomenimis, kuriuos šis komitetas išsaugojo tvarkydamas peticiją. Šį prašymą jis grindė BDAR, kuriame numatyta duomenų subjekto teisė iš duomenų valdytojo gauti su juo susijusius asmens duomenis.

Heseno federalinės žemės parlamento pirmininkas atmetė šį prašymą motyvuodamas tuo, kad peticijos nagrinėjimo procedūra yra parlamentinė funkcija ir kad parlamentui netaikomas BDAR.

Verwaltungsgericht Wiesbaden (Vysbadeno administracinis teismas, Vokietija), į kurį kreipėsi šis pilietis, padarė išvadą, kad pagal Vokietijos teisę nesuteikiama teisės susipažinti su asmens duomenimis nagrinėjant tokią peticiją, kokia aptariama byloje. Vis dėlto manydamas, kad tokia teisė gali kilti iš BDAR, *Verwaltungsgericht Wiesbaden* (Vysbadeno administracinis teismas) pateikė Teisingumui Teismą šį klausimą. Be to, kadangi *Verwaltungsgericht Wiesbaden* (Vysbadeno administracinis teismas) kilo abejonių dėl jo nepriklausomumo, taigi dėl jo kaip teisminės institucijos statuso, suteikiančio teisę pateikti prejudicinius klausimus Teisingumo Teismui, jis pateikė Teisingumo Teismui klausimą ir šiuo aspektu.

Savo sprendime Teisingumo Teismas atsakė, kad kai valstybės narės federalinio vieneto parlamento peticijų komitetas vienas ar kartu su kitais subjektais nustato asmens duomenų tvarkymo tikslus ir priemones, šis komitetas turi būti laikomas „duomenų valdytoju“, kaip tai suprantama pagal BDAR[28]. Tokio komiteto atliekamas asmens duomenų tvarkymas patenka į šio reglamento ir visų pirma į nuostatos, kuria atitinkamiems asmenims suteikiama teisė susipažinti su asmens duomenimis, susijusiais su jais, taikymo sritį[29].

[28] BDAR 4 straipsnio 7 punktas.
[29] BDAR 15 straipsnis.

Teisingumo Teismas, be kita ko, konstatavo, kad Heseno federalinės žemės parlamento Peticijų komiteto veiklai netaikoma BDAR numatyta išimtis. Jis pripažino, kad tokia veikla yra viešojo pobūdžio ir priskirtina šiai federalinei žemei, nes šis komitetas netiesiogiai prisideda prie parlamento veiklos, tačiau pažymėjo, kad ši veikla taip pat yra politinio ir administracinio pobūdžio. Be to, iš Teisingumo Teismo turimos bylos medžiagos nematyti, kad ši veikla šiuo atveju atitinka kurią nors iš BDAR numatytų išimčių (71–74 punktai ir rezoliucinė dalis).

6. Asmens duomenų tvarkymo teisėtumo sąlygos, atsižvelgiant į Direktyvos 95/46 7 straipsnį

2008 m. gruodžio 16 d. didžiosios kolegijos Sprendimas „Huber“ (C-524/06, EU:C:2008:724)[30]

Bundesamt für Migration und Flüchtlinge (Federalinė migracijos ir pabėgėlių reikalų tarnyba, Vokietija) administravo centrinį užsieniečių registrą, kuriame buvo renkami tam tikri asmens duomenys apie užsieniečius, Vokietijos teritorijoje gyvenančius ilgiau nei tris mėnesius. Šis registras buvo naudojamas statistiniais tikslais ir tuo atveju, kai saugumo ir policijos tarnybos, taip pat teisminės institucijos naudojosi persekiojimo ir paieškos įgaliojimais, susijusiais su kriminalinėmis arba visuomenės saugumui pavojų keliančiomis veikomis.

1996 m. Austrijos pilietis H. Huber apsigyveno Vokietijoje tam, kad jos teritorijoje užsiimtų nepriklausomo draudimo agento veikla. Manydamas, kad dėl su juo susijusių duomenų, esančių nagrinėjamame registre, tvarkymo yra diskriminuojamas (nebuvo tokios duomenų bazės, skirtos Vokietijos piliečiams), H. Huber paprašė pašalinti šiuos duomenis.

Šiomis aplinkybėmis *Oberverwaltungsgericht für das Land Nordrhein-Westfalen* (Šiaurės Reino-Vestfalijos žemės aukštesnysis administracinis teismas, Vokietija), nagrinėdamas bylą, pateikė Teisingumo Teismui klausimą dėl atitinkamame registre vykdomo asmens duomenų tvarkymo suderinamumo su Sąjungos teise.

Visų pirma Teisingumo Teismas priminė, kad Sąjungos piliečio teisė apsigyventi kitos valstybės narės, kurios pilietis jis nėra, teritorijoje nėra besąlygiška ir jai gali būti taikomi apribojimai. Taigi tokio registro naudojimas siekiant padėti valdžios institucijoms, atsakingoms už teisės aktų, susijusių su teise apsigyventi, taikymą, iš principo yra teisėtas ir, atsižvelgiant į jo pobūdį, suderinamas su diskriminacijos dėl pilietybės draudimu, įtvirtintu EB 12 straipsnio 1 dalyje (dabar SESV 18 straipsnio pirma pastraipa). Vis dėlto tokiame registre gali būti tik ta informacija, kuri yra būtina šiam tikslui, kaip tai suprantama pagal Direktyvą dėl asmens duomenų apsaugos (54, 58 ir 59 punktai).

Kiek tai susiję su tvarkymo būtinybės sąvoka, kaip ji suprantama pagal Direktyvos 95/46 7 straipsnio e punktą, Teisingumo Teismas visų pirma priminė, kad tai yra autonomiška Sąjungos teisės sąvoka, kurią reikia aiškinti taip, kad ji visiškai atitiktų Direktyvos 95/46 tikslą, apibrėžtą jos 1 straipsnio 1 dalyje. Tada jis konstatavo, kad asmens duomenų tvarkymo sistema atitinka Sąjungos teisę, jeigu joje kaupiami tik tie duomenys, kurie šioms institucijoms yra būtini taikyti

[30] Šis sprendimas pristatytas 2018 m. metiniame pranešime, p. 45.

tiems teisės aktams, ir jeigu jos centralizuotas pobūdis leidžia veiksmingiau taikyti šiuos teisės aktus tos valstybės narės pilietybės neturinčių Sąjungos piliečių teisei apsigyventi.

Bet kuriuo atveju negalima laikyti, kad tokiame registre būtina, kaip tai suprantama pagal Direktyvos 95/46 7 straipsnio e punktą, statistikos tikslais saugoti ir tvarkyti su konkrečia pavarde ir vardu susijusius asmens duomenis (52, 66 ir 68 punktai).

Be to, dėl registre esančių duomenų naudojimo kovos su nusikalstamumu tikslais Teisingumo Teismas pažymėjo, kad šis tikslas reikalauja tirti padarytus nusikaltimus ir pažeidimus, neatsižvelgiant į juos padariusių asmenų pilietybę. Taigi kovodama su nusikalstamumu valstybė narė neturėtų skirtingai vertinti savo piliečių padėties ir jos teritorijoje gyvenančių jos pilietybės neturinčių Sąjungos piliečių padėties. Todėl skirtingas savo piliečių ir kitų Sąjungos piliečių vertinimas kovos su nusikalstamumu tikslu sistemingai tvarkant asmens duomenis, susijusius tik su atitinkamos valstybės narės pilietybės neturinčiais Sąjungos piliečiais, yra pagal EB 12 straipsnio 1 dalį draudžiama diskriminacija (78–80 punktai).

2011 m. lapkričio 24 d. Sprendimas „ASNEF ir FECEMD" (C-468/10 ir C-469/10, EU:C:2011:777)

Viena vertus, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* ir, kita vertus, *Federación de Comercio Electrónico y Marketing Directo (FECEMD)* pateikė *Tribunal Supremo* (Aukščiausiasis Teismas, Ispanija) skundą administracinėje byloje dėl Karaliaus dekreto 1720/2007, įgyvendinančio Organinį įstatymą 15/1999, kuriuo į nacionalinę teisę perkeliama Direktyva 95/46 , tam tikrų straipsnių.

Konkrečiai kalbant, ASNEF ir FECEMD manė, kad siekiant sudaryti galimybę tvarkyti asmens duomenis be atitinkamo asmens sutikimo Ispanijos teisėje buvo nustatyta papildoma sąlyga, kurios nėra Direktyvoje 95/46 ir pagal kurią reikalaujama, kad tai būtų „viešųjų rinkmenų duomenys", išvardyti Organinio įstatymo 15/1999 3 straipsnio j punkte. Šiuo aspektu jos teigė, kad šiuo įstatymu ir Karaliaus dekretu 1720/2007 apribojama Direktyvos 95/46 7 straipsnio f punkto taikymo sritis; tame punkte numatyta, kad asmens duomenys be atitinkamo asmens sutikimo gali būti tvarkomi su sąlyga, susijusia tik su teisėtais interesais, kurių siekia duomenų valdytojas arba trečioji šalis (trečiosios šalys), kuriai (kurioms) atskleidžiami duomenys.

Šiuo aspektu Teisingumo Teismas visų pirma pažymėjo, kad Direktyvos 95/46 7 straipsnyje pateiktas išsamus ir baigtinis atvejų, kai asmens duomenų tvarkymas be atitinkamo asmens sutikimo gali būti laikomas teisėtu, sąrašas. Todėl valstybės narės, remdamosi minėtos direktyvos 5 straipsniu, negali nustatyti kitų asmens duomenų tvarkymo teisėtumo principų, nei numatytieji šios direktyvos 7 straipsnyje, ar papildomais reikalavimais keisti šiame 7 straipsnyje numatytų principų apimties. Iš tiesų šiuo 5 straipsniu, kiek leidžia tos direktyvos II skyriaus, taigi, ir jame esančio 7 straipsnio, nuostatos, valstybėms narėms tik suteikiama galimybė tiksliau apibrėžti asmens duomenų tvarkymo teisėtumo sąlygas (30, 32 ir 33 punktai).

Konkrečiai kalbant, siekdamos, kaip reikalaujama pagal minėtos direktyvos 7 straipsnio f punktą, palyginti atitinkamas priešingas teises ir interesus, valstybės narės gali nustatyti pagrindinius principus. Jos taip pat gali atsižvelgti į tai, kad asmens, su kuriuo susijęs šis duomenų tvarkymas, pagrindinių teisių apribojimo sunkumas gali skirtis, nelygu, ar atitinkami duomenys jau įtraukti į viešąją rinkmeną (44 ir 46 punktai).

Vis dėlto Teisingumo Teismas konstatavo, kad jei pagal nacionalinės teisės aktus kai kurių kategorijų asmens duomenys negali būti tvarkomi, dėl šių kategorijų numatant galutinį priešingų teisių ir interesų palyginimo rezultatą, o tai neleidžia konkrečiu atveju, kuriam būdingos specifinės aplinkybės, pasiekti kitokio rezultato, tai nėra patikslinimas, kaip tai suprantama pagal Direktyvos 95/46 5 straipsnį. Todėl Teisingumo Teismas padarė išvadą, kad pagal Direktyvos 95/46 7 straipsnio f punktą draudžiama valstybei narei kategoriškai ir visais atvejais atmesti galimybę tvarkyti tam tikrų kategorijų asmens duomenis, neleidžiant palyginti konkrečios situacijos priešingų teisių ir interesų (47 ir 48 punktai).

2016 m. spalio 19 d. Sprendimas „Breyer“ (C-582/14, EU:C:2016:779)

Šiame sprendime (taip pat žr. skyrių II.2. „Sąvoka „asmens duomenys“) Teisingumo Teismas atsakė į klausimą, ar pagal Direktyvos 95/46 7 straipsnio f punktą draudžiama nacionalinės teisės nuostata, pagal kurią elektroninių paslaugų teikėjas gali rinkti ir naudoti su naudotoju susijusius asmens duomenis be jo sutikimo tik tiek, kiek tai būtina siekiant leisti tam naudotojui pasinaudoti konkrečia elektronine paslauga ir atsiskaityti už ją, ir pagal kurią tikslas užtikrinti bendrą elektroninių paslaugų veikimą negali pateisinti duomenų naudojimo pasibaigus naudojimosi paslaugomis operacijai.

Teisingumo Teismas nusprendė, kad pagal Direktyvos 95/46 7 straipsnio f punktą atitinkama teisės nuostata yra draudžiama. Iš tiesų, remiantis šia nuostata, asmens duomenų tvarkymas, kaip tai suprantama pagal tą nuostatą, yra teisėtas, jei tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (trečiosios šalys), kuriai (kurioms) atskleidžiami duomenys, su sąlyga, kad atitinkamo asmens interesai arba pagrindinės teisės ir laisvės nėra viršesni. Šiuo atveju Vokietijos teisės akte kategoriškai ir visais atvejais buvo atmesta galimybė tvarkyti tam tikrų kategorijų asmens duomenis, neleidžiant palyginti konkrečioje situacijoje nagrinėjamų priešingų teisių ir interesų. Taip ja neteisėtai buvo apribota šio principo, numatyto Direktyvos 95/46 7 straipsnio f punkte, apimtis, atmetant galimybę tikslą užtikrinti bendrą elektroninių paslaugų veikimą palyginti su naudotojų interesais ar pagrindinėmis teisėmis ir laisvėmis (62–64 punktai ir rezoliucinės dalies 2 punktas).

2017 m. gegužės 4 d. Sprendimas „Rīgas satiksme“ (C-13/16, EU:C:2017:336)

Ši byla susijusi su Latvijos nacionalinės policijos ir Rygos miesto troleibusų bendrovės *Rīgas satiksme* ginču dėl prašymo perduoti su eismo įvykį sukėlusio asmens tapatybe susijusius duomenis. Nagrinėjamu atveju per eismo įvykį taksi vairuotojas savo automobilį buvo sustabdęs kelkraštyje. Tuo metu, kai *Rīgas satiksme* troleibusas važiavo pro šį taksi, ant galinės sėdynės sėdėjęs keleivis atidarė dureles, kuriomis kliudė ir apgadino troleibusą. Siekdama pateikti civilinį ieškinį *Rīgas satiksme*, be kita ko, paprašė nacionalinės policijos perduoti su eismo įvykį sukėlusio asmens tapatybe susijusius duomenis. Policija atsisakė perduoti keleivio tapatybės numerį ir jo adresą, taip pat dokumentus, susijusius su eismo įvykyje dalyvavusių asmenų paaiškinimais, motyvuodama tuo, kad administracinės procedūros, kuriai pasibaigus skiriamos nuobaudos, dokumentai gali būti perduoti tik šios bylos šalims, o kiek tai susiję su tapatybės numeriu ir adresu – Asmens duomenų apsaugos įstatymas draudžia atskleisti tokią informaciją apie privačius asmenis.

Tokiomis aplinkybėmis *Augstākās tiesas Administratīvo lietu departaments* (Aukščiausiasis Teismas, Administracinių bylų skyrius, Latvija) nusprendė pateikti Teisingumo Teismui klausimą, ar Direktyvos 95/46 7 straipsnio f punkte yra nustatyta pareiga perduoti asmens duomenis trečiajai šaliai tam, kad ji galėtų pareikšti civilinį ieškinį dėl žalos, padarytos asmens, su kuriuo susijusi šių duomenų apsauga, atlyginimo, ir ar tai, kad šis asmuo yra nepilnametis, gali turėti įtakos aiškinant šią nuostatą.

Teisingumo Teismas nusprendė, kad Direktyvos 95/46 7 straipsnio f punktas turi būti aiškinamas kaip nenustatantis pareigos perduoti asmens duomenų trečiajai šaliai, kad ši galėtų pareikšti civilinį ieškinį dėl žalos, padarytos asmens, su kuriuo susijusi šių duomenų apsauga, atlyginimo. Tačiau pagal šią nuostatą toks perdavimas nedraudžiamas, jei atliekamas pagal nacionalinę teisę, laikantis šioje nuostatoje numatytų sąlygų (27, 34 punktai ir rezoliucinė dalis).

Šiame kontekste Teisingumo Teismas pažymėjo, kad (tai dar turi patikrinti nacionalinis teismas) tokiomis aplinkybėmis, kokios susiklostė pagrindinėje byloje, neatrodo pateisinama atsisakyti nukentėjusiajam asmeniui perduoti asmens duomenis, būtinus norint pareikšti ieškinį dėl žalos atlyginimo šią žalą sukėlusiam asmeniui arba prireikus asmenims, kurie turi tėvų valdžią, dėl to, kad šis asmuo nepilnametis (33 punktas).

2017 m. rugsėjo 27 d. Sprendimas „Puškár“ (C-73/16, EU:C:2017:725)

Pagrindinėje byloje P. Puškár pateikė skundą *Najvyšší súd Slovenskej republiky* (Slovakijos Respublikos Aukščiausiasis Teismas), prašydamas nurodyti *Finančné riaditel'stvo* (Finansų direktoratas), visoms jam pavaldžioms mokesčių tarnyboms ir *Kriminálny úrad finančnej správy* (Kovos su finansiniais nusikaltimais tarnyba) neįtraukti jo į asmenų, Finansų direktorato laikomų statytiniais, registrą, kurį rinkdamas mokesčius sudarė šis direktoratas ir kurį atnaujina jis ir Kovos su finansiniais nusikaltimais tarnyba (toliau – ginčijamas registras). Be to, jis paprašė pašalinti bet kokią su juo susijusią informaciją iš šio registro ir finansų administravimo elektroninės sistemos.

Šiomis aplinkybėmis *Najvyšší súd Slovenskej republiky (Slovakijos Respublikos Aukščiausiasis Teismas)* Teisingumo Teismo, be kita ko, klausė, ar teisė į privatų ir šeimos gyvenimą, būsto neliečiamybę ir komunikacijos slaptumą, įtvirtinta Chartijos 7 straipsnyje, ir teisė į asmens duomenų apsaugą, įtvirtinta Chartijos 8 straipsnyje, gali būti aiškinamos taip, kad valstybė narė negali be suinteresuotojo asmens sutikimo sukurti asmens duomenų registro mokesčių administravimo tikslais, todėl valdžios institucijų atliekamas asmens duomenų rinkimas siekiant kovoti su mokestiniu sukčiavimu savaime kelia pavojų.

Teisingumo Teismas padarė išvadą, kad Direktyvos 95/46 7 straipsnio e punktas nedraudžia valstybės narės institucijoms tvarkyti asmens duomenis renkant mokesčius ir kovojant su mokestiniu sukčiavimu, kaip tai daryta sudarant pagrindinėje byloje ginčijamą asmenų registrą, be atitinkamų asmenų sutikimo, su sąlyga, kad, viena vertus, šios institucijos vykdo užduotis visuomenės labui pagal nacionalinę teisę, kaip tai suprantama pagal šią nuostatą, kad šio registro sudarymas ir atitinkamų asmenų įtraukimas į jį yra tinkamas ir būtinas įgyvendinant siekiamus tikslus, kad yra pakankamai įrodymų preziumuoti, jog atitinkamų asmenų įtraukimas į šį registrą yra teisėtas, ir, kita vertus, įvykdytos visos Direktyvoje 95/46 nustatytos šio asmens duomenų tvarkymo teisėtumo sąlygos (117 punktas ir rezoliucinės dalies 3 punktas).

Šiuo aspektu Teisingumo Teismas pažymėjo, kad nacionalinis teismas turi išsiaiškinti, ar ginčijamo registro sudarymas yra būtinas atliekant pagrindinėje byloje nagrinėjamą užduotį visuomenės labui, pirmiausia atsižvelgiant į aiškų ginčijamo registro sudarymo tikslą, jame nurodytiems asmenims sukeliamas teisines pasekmes ir šio registro viešąjį arba neviešąjį pobūdį. Be to, laikydamasis proporcingumo principo nacionalinis teismas turi patikrinti, ar ginčijamo registro sudarymas ir susijusių asmenų įtraukimas į jį yra tinkami įgyvendinant siekiamus tikslus ir ar nėra kitų švelnesnių priemonių šiems tikslams pasiekti (111, 112 ir 113 punktai).

Teisingumo Teismas konstatavo, jog tai, kad asmuo įrašomas į ginčijamą registrą, gali pažeisti tam tikras jo teises. Įrašymas į šį registrą gali pakenkti jo reputacijai ir santykiams su mokesčių institucijomis. Šis įrašymas gali pažeisti ir šio asmens nekaltumo prezumpciją, įtvirtintą Chartijos 48 straipsnio 1 dalyje, ir juridinių asmenų, susietų su į ginčijamą registrą įrašytais fiziniais asmenimis, laisvę užsiimti verslu, įtvirtintą Chartijos 16 straipsnyje. Todėl tokia intervencija gali būti tinkama priemonė tik tuomet, jeigu yra pakankamų požymių įtarti, kad atitinkamas asmuo fiktyviai vadovauja su juo siejamiems juridiniams asmenims ir taip kenkia mokesčių rinkimui ir kovai su mokestiniu sukčiavimu (114 punktas).

Be to, Teisingumo Teismas laikėsi nuomonės, kad jeigu būtų Direktyvos 95/46 13 straipsnyje nustatytų priežasčių apriboti tam tikras jos 6 ir 10–12 straipsniuose įtvirtintas teises, pavyzdžiui, atitinkamo asmens teisę į informavimą, toks ribojimas turėtų būti būtinas saugant minėto 13 straipsnio 1 dalyje nurodytus interesus, t. y. svarbius ekonominius ar finansinius interesus mokesčių srityje, ir būti pateisinamas teisinėmis priemonėmis (116 punktas).

2020 m. lapkričio 11 d. Sprendimas „Orange Romania“ (C-61/19, EU:C:2020:901)

Orange România SA teikia telekomunikacijų paslaugas Rumunijos rinkoje. 2018 m. kovo 28 d. *Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP) (Nacionalinė asmens duomenų tvarkymo priežiūros institucija, Rumunija) skyrė jai baudą už jos klientų asmens tapatybės dokumentų kopijų rinkimą ir saugojimą be aiškaus jų sutikimo.

Anot ANSPDCP, laikotarpiu nuo 2018 m. kovo 1 iki 26 d. *Orange România* sudarė telekomunikacijų paslaugų sutartis, kuriose įtvirtinta sąlyga, pagal kurią klientai buvo informuoti apie jų asmens tapatybės dokumentų kopijų rinkimą ir saugojimą identifikavimo tikslais ir su tuo sutiko. Su šia sąlyga susijusį langelį duomenų valdytojas pažymėjo prieš pasirašant sutartį.

Šiomis aplinkybėmis *Tribunalul București* (Bukarešto apygardos teismas, Rumunija) paprašė Teisingumo Teismo patikslinti sąlygas, kuriomis klientų sutikimą su asmens duomenų tvarkymu galima laikyti galiojančiu.

Iš pradžių Teisingumo Teismas priminė, kad Sąjungos teisėje[31] yra numatytas atvejų, kai asmens duomenų tvarkymą galima laikyti teisėtu, sąrašas. Konkrečiai kalbant, duomenų subjekto sutikimas turi būti duotas laisva valia, konkretus, informuotas ir nedviprasmiškas[32]. Šiuo aspektu sutikimas nėra tinkamas, jeigu jis duotas tyla, iš anksto pažymėtais langeliais arba neveikimu (34, 36, 37 ir 39 punktai).

[31] Direktyvos 95/46 7 straipsnis ir BDAR 6 straipsnis.
[32] Direktyvos 95/46 2 straipsnio h punktas ir BDAR 4 straipsnio 11 punktas.

Be to, kai duomenų subjekto sutikimas grindžiamas rašytiniu pareiškimu, susijusiu ir su kitais klausimais, šis pareiškimas turi būti pateiktas suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba. Siekiant duomenų subjektui užtikrinti tikrą pasirinkimo laisvę, sutarties sąlygos neturi jo klaidinti dėl galimybės sudaryti sutartį, net jeigu jis atsisako duoti sutikimą dėl jo duomenų tvarkymo (34, 36, 37, 39 ir 41 punktai).

Teisingumo Teismas pažymėjo: kadangi *Orange România* yra duomenų valdytoja, ji turi galėti įrodyti šių duomenų tvarkymo teisėtumą, taigi tai, kad jos klientai yra davę galiojantį sutikimą. Šiuo aspektu, kadangi atrodo, jog atitinkami klientai ne patys pažymėjo langelį, susijusį su jų asmens tapatybės dokumentų kopijų rinkimu ir saugojimu, vien tai, kad šis langelis buvo pažymėtas, neleidžia nustatyti jų sutikimo. Nacionalinis teismas turi atlikti šiuo tikslu reikalingus patikrinimus (42 ir 46 punktai).

Anot Teisingumo Teismo, nacionalinis teismas taip pat turi išsiaiškinti, ar nagrinėjamos sutarties sąlygos galėjo suklaidinti atitinkamus klientus dėl galimybės sudaryti sutartį, nepaisant neduoto sutikimo tvarkyti duomenis, nesant paaiškinimų dėl šios galimybės. Be to, Teisingumo Teismas pažymi, kad tuo atveju, kai klientas neduodavo sutikimo tvarkyti savo duomenis, *Orange România* reikalaudavo, kad jis raštu pareikštų, jog neduoda sutikimo nei rinkti, nei saugoti savo asmens tapatybės dokumento kopijos. Teisingumo Teismo manymu, toks papildomas reikalavimas gali nepagrįstai paveikti laisvą pasirinkimą prieštarauti dėl tokio rinkimo ir saugojimo. Bet kuriuo atveju, kadangi ši bendrovė turi įrodyti, kad jos klientai savo aktyviais veiksmais išreiškė sutikimą dėl jų asmens duomenų tvarkymo, ji negali reikalauti, kad jie aktyviai pareikštų savo nesutikimą (49–51).

Teisingumo Teismas padarė išvadą, kad telekomunikacijų paslaugų teikimo sutartis, įtvirtinanti sąlygą, pagal kurią atitinkamas asmuo buvo informuotas ir sutiko dėl savo asmens tapatybės dokumento kopijos rinkimo ir saugojimo identifikavimo tikslais, negali įrodyti, jog šis asmuo tinkamai davė sutikimą dėl tokio rinkimo ir saugojimo, jeigu su šia sąlyga susijusį langelį duomenų valdytojas pažymėjo prieš pasirašant šią sutartį, jeigu sutarties sąlygos gali suklaidinti atitinkamą asmenį dėl galimybės sudaryti atitinkamą sutartį net ir tuo atveju, jeigu jis atsisako duoti sutikimą dėl savo duomenų tvarkymo, arba jeigu duomenų valdytojas nepagrįstai apriboja laisvą pasirinkimą prieštarauti dėl tokio rinkimo ir saugojimo, reikalaudamas, kad atitinkamas asmuo, norėdamas atsisakyti duoti sutikimą, užpildytų papildomą formuliarą, kuriame būtų patvirtintas šis atsisakymas (52punktas ir rezoliucinė dalis).

2021 m. gegužės 12 d. didžiosios kolegijos Sprendimas „Bundesrepublik Deutschland“ (Interpolo raudonasis pranešimas) (C-505/19, EU:C:2021:376)

2012 m. Jungtinių Amerikos Valstijų prašymu Tarptautinė kriminalinės policijos organizacija (toliau – Interpolas), remdamasi šios šalies valdžios institucijų išduota nutartimi dėl suėmimo, paskelbė raudonąjį pranešimą dėl Vokietijos piliečio WS, siekdama galimos jo ekstradicijos. Kai asmens, dėl kurio paskelbtas toks pranešimas, buvimo vieta nustatoma Interpolo valstybėje narėje, ši iš esmės turi jį sulaikyti, suimti arba apriboti jo judėjimą.

Vis dėlto dar iki šio raudonojo pranešimo paskelbimo Vokietijoje prieš WS buvo pradėta tyrimo procedūra, prašymą priimti prejudicinį sprendimą pateikusio teismo teigimu, dėl tų pačių veikų, dėl kurių buvo paskelbtas pranešimas. Šis tyrimas 2010 m. buvo galutinai užbaigtas, WS sumokėjus pinigų sumą pagal Vokietijos baudžiamojoje teisėje numatytą specialią susitarimo procedūrą. Vėliau *Bundeskriminalamt* (Federalinė kriminalinės policijos tarnyba, Vokietija)

Interpolui pranešė mananti, kad dėl šios ankstesnės tyrimo procedūros šiuo atveju taikytinas *ne bis in idem* principas. Šis principas, įtvirtintas tiek Konvencijos dėl Šengeno susitarimo įgyvendinimo[33] 54 straipsnyje, tiek Chartijos 50 straipsnyje, draudžia, be kita ko, dėl tos pačios nusikalstamos veikos vėl persekioti asmenį, dėl kurio buvo priimtas galutinis sprendimas.

2017 m. WS pateikė skundą prieš Vokietijos Federacinę Respubliką *Verwaltungsgericht Wiesbaden* (Vysbadeno administracinis teismas, Vokietija), prašydamas įpareigoti ją imtis reikiamų priemonių, kad raudonasis pranešimas būtų panaikintas. Šiuo klausimu WS nurodė ne tik *ne bis in idem* principo, bet ir jo teisės į laisvą judėjimą, užtikrinamos pagal SESV 21 straipsnį, pažeidimą, mat jis negali vykti į valstybę, kuri yra Šengeno susitarimo šalis, arba į valstybę narę, nes rizikuoja, kad bus suimtas. Jis taip pat manė, kad dėl šių pažeidimų raudonajame pranešime pateiktų jo asmens duomenų tvarkymas prieštarauja Direktyvai 2016/680 dėl asmens duomenų apsaugos baudžiamosiose bylose[34].

Šiomis aplinkybėmis Vysbadeno administracinis teismas nusprendė kreiptis į Teisingumo Teismą dėl *ne bis in idem* principo taikymo ir, konkrečiai kalbant, dėl galimybės suimti asmenį, dėl kurio paskelbtas raudonasis pranešimas, esant tokiai situacijai, kaip nagrinėjamoji. Be to, tuo atveju, jei tas principas būtų pripažintas taikytinu, šis teismas siekė išsiaiškinti, kokių pasekmių tai turėtų tokiame pranešime pateiktų asmens duomenų tvarkymui valstybėse narėse.

Savo didžiosios kolegijos sprendime Teisingumo Teismas, be kita ko, konstatavo, kad Direktyvos 2016/680 nuostatos, siejamos su KŠSĮ 54 straipsniu ir Chartijos 50 straipsniu, turi būti aiškinamos taip, kad jos nedraudžia tvarkyti Interpolo paskelbtame raudonajame pranešime nurodytų asmens duomenų, kol tokiu teismo sprendimu nenustatoma, kad *ne bis in idem* principas taikomas veikoms, kuriomis pagrįstas šis pranešimas, jeigu toks tvarkymas atitinka šioje direktyvoje nurodytas sąlygas (121 punktas ir rezoliucinės dalies 2 punktas).

Dėl Interpolo raudonajame pranešime nurodytų asmens duomenų Teisingumo Teismas pažymėjo, kad bet kokia su asmens duomenimis atliekama operacija, kaip antai jų įrašymas į valstybės narės ieškomų asmenų sąrašą, pripažįstama „tvarkymu“, kaip tai suprantama pagal Direktyvą 2016/680[35]. Be to, jis konstatavo, kad, pirma, šiuo tvarkymu siekiama teisėto tikslo, antra, jo negalima laikyti neteisėtu vien todėl, kad dėl veikų, kuriomis grindžiamas raudonasis pranešimas, gali būti taikomas *ne bis in idem* principas[36]. Toks valstybių narių institucijų atliekamas duomenų tvarkymas gali būti būtinas, būtent siekiant patikrinti, ar taikytinas minėtas principas (111, 114, 116, 117 ir 119 punktai).

Šiomis aplinkybėmis Teisingumo Teismas taip pat nusprendė, kad pagal Direktyvą 2016/680, siejamą su KŠSĮ 54 straipsniu ir Chartijos 50 straipsniu, nedraudžiama tvarkyti raudonajame pranešime pateiktų asmens duomenų, kol remiantis galutiniu teismo sprendimu nenustatoma,

---

33 1985 m. birželio 14 d. Konvencija dėl Šengeno susitarimo, sudaryto tarp Beniliukso ekonominės sąjungos valstybių, Vokietijos Federacinės Respublikos ir Prancūzijos Respublikos vyriausybių dėl laipsniško jų bendrų sienų kontrolės panaikinimo, įgyvendinimo (OL L 239, 2000, p. 19; 2004 m. specialusis leidimas lietuvių k., 19 sk., 2 t., p. 9; toliau – KŠSĮ).

34 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89).

35 Žr. Direktyvos 2016/680 2 straipsnio 1 dalį ir 3 straipsnio 2 punktą.

36 Žr. Direktyvos 2016/680 4 straipsnio 1 dalies b punktą ir 8 straipsnio 1 dalį.

kad nagrinėjamu atveju taikomas *ne bis in idem* principas. Vis dėlto toks tvarkymas turi atitikti šioje direktyvoje numatytas sąlygas. Atsižvelgiant į tai, jis, be kita ko, turi būti būtinas kompetentingos nacionalinės institucijos vykdomoms funkcijoms, siekiant nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslų[37] (121 punktas ir rezoliucinės dalies 2 punktas).

Kita vertus, kai *ne bis in idem* principas taikomas, Interpolo raudonajame pranešime nurodytų asmens duomenų įrašymas į valstybių narių ieškomų asmenų sąrašus nebūtinas, nes nebegali būti vykdomas aptariamo asmens baudžiamasis persekiojimas dėl minėtame pranešime nurodytų veikų, taigi jis nebegali būti suimtas dėl tų pačių veikų. Darytina išvada, kad atitinkamas asmuo turi turėti galimybę prašyti ištrinti šiuos duomenis. Jei įrašas vis dėlto paliekamas, prie jo turi būti pridedama informacija, kad atitinkamas asmuo nebegali būti persekiojamas valstybėje narėje ar susitariančiojoje valstybėje už tas pačias veikas, nes taikomas *ne bis in idem* principas (120 punktas).

2021 m. birželio 22 d. didžiosios kolegijos Sprendimas „Latvijas Republikas Saeima“ (Baudos taškai) (C-439/19, EU:C:2021:504)

Šiame sprendime (taip pat žr. II.3 skyrių „Sąvoka „Asmens duomenų tvarkymas“) Teisingumo Teismas nusprendė, kad BDAR draudžiamos teisės nuostatos, pagal kurias *Ceļu satiksmes drošības direkcija* (Kelių eismo saugumo direkcija, Latvija) (toliau – CSDD) įpareigojama suteikti galimybę visuomenei susipažinti su duomenimis apie transporto priemonių vairuotojams už kelių eismo taisyklių pažeidimus skirtus baudos taškus, nereikalaujant, kad asmuo, prašantis suteikti galimybę susipažinti, įrodytų, kad turi konkretų interesą juos gauti. Jis konstatavo, kad neįrodyta, kad, be kita ko, atsižvelgiant į Latvijos vyriausybės nurodytą kelių eismo saugumo didinimo tikslą, būtina atskleisti asmens duomenis apie už kelių eismo taisyklių pažeidimus skirtus baudos taškus. Be to, Teisingumo Teismo teigimu, tokių teisės nuostatų negali pateisinti visuomenės teisė susipažinti su oficialiais dokumentais ar teisė į informacijos laisvę (113, 120–122 punktai ir rezoliucinės dalies 2 punktas).

Šiomis aplinkybėmis Teisingumo Teismas pažymėjo, kad Latvijos teisės aktuose nurodytas kelių eismo saugumo didinimas yra Sąjungos pripažintas bendrojo intereso tikslas, taigi valstybės narės gali kelių eismo saugumą laikyti „užduotimi, vykdoma viešojo intereso labui“[38]. Vis dėlto nenustatyta, kad Latvijos asmens duomenų apie baudos taškus atskleidimo tvarka yra būtina nurodytam tikslui pasiekti. Iš tiesų, viena vertus, Latvijos teisės aktų leidėjas yra nustatęs daug veikimo būdų, kurie jam būtų leidę kitomis atitinkamų asmenų pagrindines teises mažiau ribojančiomis priemonėmis pasiekti šį tikslą. Kita vertus, reikia atsižvelgti į duomenų apie baudos taškus jautrumą ir į tai, kad dėl jų atskleidimo visuomenei gali būti stipriai suvaržytos teisės į privatų gyvenimą ir į asmens duomenų apsaugą, nes šis duomenų atskleidimas gali sukelti visuomenės nepritarimą ir dėl to atitinkamas asmuo gali būti stigmatizuojamas (109–113 punktai).

Be to, Teisingumo Teismas konstatavo, kad, atsižvelgiant į šių duomenų jautrumą ir šio pagrindinių teisių suvaržymo dydį, šios teisės yra viršesnės tiek už viešąjį interesą turėti galimybę

[37] Žr. Direktyvos 2016/680 1 straipsnio 1 dalį ir 8 straipsnio 1 dalį.

[38] BDAR 6 straipsnio 1 dalies e punkte nustatyta, kad asmens duomenų tvarkymas yra teisėtas, jeigu jis yra „būtina[s] siekiant atlikti užduotį, vykdomą viešojo intereso labui. <...>“

susipažinti su oficialiais dokumentais, kaip antai nacionalinių transporto priemonių ir jų vairuotojų registru, tiek už teisę į informacijos laisvę (120 ir 121 punktai).

Be to, dėl tų pačių priežasčių Teisingumo Teismas nusprendė, kad BDAR taip pat draudžiamos Latvijos teisės nuostatos, kiek pagal jas CSDD leidžiama duomenis apie transporto priemonių vairuotojams už kelių eismo taisyklių pažeidimus skirtus baudos taškus atskleisti ūkio subjektams, kad šie galėtų juos pakartotinai naudoti ir atskleisti visuomenei (126 punktas ir rezoliucinės dalies 3 punktas).

Galiausiai Teisingumo Teismas pažymėjo, kad pagal Sąjungos teisės viršenybės principą prašymą priimti prejudicinį sprendimą pateikusiam teismui, gavusiam skundą dėl Latvijos teisės nuostatų, kurias Teisingumo Teismas pripažino nesuderinamomis su Sąjungos teise, draudžiama nuspręsti, kad šių nuostatų teisiniai padariniai lieka galioti, kol bus paskelbtas galutinis jo sprendimas (137 punktas ir rezoliucinės dalies 4 punktas).

III. Asmens duomenų tvarkymas, kaip tai suprantama pagal Direktyvą 2002/58

2018 m. spalio 2 d. didžiosios kolegijos Sprendimas „Ministerio Fiscal" (C-207/16, ECLI:EU:C:2018:788)[39]

Šioje byloje buvo nagrinėjamas Ispanijos ikiteisminio tyrimo teismo sprendimas atmesti prašymą, pateiktą atliekant tyrimą dėl plėšimo, per kurį buvo pagrobta piniginė ir mobilusis telefonas. Konkrečiai kalbant, kriminalinė policija minėto teismo paprašė suteikti jai prieigą prie telefono numerių, kurie buvo aktyvuoti iš pavogto telefono per dvylikos dienų laikotarpį, skaičiuojamą nuo vagystės dienos, naudotojų tapatybės duomenų. Šis prašymas buvo atmestas, motyvuojant tuo, kad veiksmai, dėl kurių buvo vykdomas baudžiamosios veikos tyrimas, nelaikomi „sunkia" nusikalstama veika, t. y. pagal Ispanijos teisę nusikaltimu, už kurį skiriama ilgesnė nei penkerių metų laisvės atėmimo bausmė, nes suteikti galimybę susipažinti su tapatybės duomenimis galima tik tokios nusikalstamos veikos atveju.

Priminęs, kad valdžios institucijų prieiga prie elektroninių ryšių paslaugų teikėjų saugomų asmens duomenų vykstant baudžiamojo tyrimo procesui patenka į Direktyvos 2002/58 taikymo sritį, Teisingumo Teismas nusprendė, kad prieiga prie duomenų, kuriais siekiama nustatyti pavogtu mobiliuoju telefonu aktyvuotų SIM kortelių savininkus, kaip antai šių savininkų pavardžių, vardų ir atitinkamais atvejais adresų, yra Chartijoje įtvirtintų pagrindinių teisių į privataus gyvenimo gerbimą ir duomenų apsaugą apribojimas, net jei nėra aplinkybių, dėl kurių šį ribojimą būtų galima laikyti „rimtu", ir nesvarbu, kad atitinkama su privačiu gyvenimu susijusi informacija yra arba nėra jautri ar kad dėl šio ribojimo suinteresuotieji asmenys galbūt patyrė nepatogumų. Teisingumo Teismas pabrėžė, jog šis ribojimas vis dėlto nėra toks rimtas, kad užkardant, tiriant bei nustatant baudžiamąsias veikas ir vykdant baudžiamąjį persekiojimą už jas šią prieigą būtų galima suteikti tik siekiant kovoti su sunkiais nusikaltimais. Iš tiesų, nors

[39] Šis sprendimas pristatytas 2018 m. metiniame pranešime, p. 88 ir 89.

Direktyvoje 2002/58 išsamiai išvardyti tikslai, galintys pateisinti nacionalinės teisės aktus, kuriais reglamentuojama valdžios institucijų prieiga prie atitinkamų duomenų ir taip nukrypstama nuo elektroninių ryšių konfidencialumo principo (ši prieiga iš tikrųjų turi griežtai atitikti vieną iš tų tikslų), Teisingumo Teismas pažymi, kad, kalbant apie tikslą užkardyti, tirti bei nustatyti baudžiamąsias veikas ir vykdyti baudžiamąjį persekiojimą už jas, Direktyvos 2002/58 tekste šis tikslas nėra siaurai apibrėžtas, t. y. tik kaip kova su sunkiomis nusikalstamomis veikomis, bet toje direktyvoje nurodytos „baudžiamosios veikos“ apskritai (38, 42, 59–63 punktai ir rezoliucinė dalis).

Tokiomis aplinkybėmis Teisingumo Teismas pažymėjo, jog Sprendime *Tele2 Sverige ir Watson ir kt.*[40] pateiktas aiškinimas, kad valdžios institucijų prieigą prie elektroninių ryšių paslaugų teikėjų saugomų asmens duomenų, kurie, vertinami kartu, gali leisti padaryti tikslias išvadas dėl asmenų, kurių duomenys yra tvarkomi, privataus gyvenimo, gali pateisinti tik kova su sunkiais nusikaltimais, tačiau toks aiškinimas buvo grindžiamas tuo, kad šią prieigą reglamentuojančiais teisės aktais siekiamas tikslas turi būti susijęs su šio veiksmo lemiamo nagrinėjamų pagrindinių teisių ribojimo rimtumu. Taigi pagal proporcingumo principą rimtas ribojimas šioje srityje gali būti pateisinamas ne tik siekiu kovoti su nusikaltimais, kurie taip pat turi būti kvalifikuojami kaip „sunkūs“. Tačiau jeigu ribojimas nėra rimtas, minėta prieiga gali būti pateisinama tikslu užkardyti, tirti ir nustatyti „baudžiamąsias veikas“ apskritai ir vykdyti baudžiamąjį persekiojimą už jas (54–57 punktai).

Nagrinėtu atveju Teisingumo Teismas nusprendė, kad prieiga tik prie nagrinėtame prašyme nurodytų duomenų negali būti laikoma „rimtu“ asmenų, kurių duomenys yra tvarkomi, pagrindinių teisių ribojimu, nes tie duomenys neleidžia daryti tikslių išvadų dėl jų privataus gyvenimo. Teisingumo Teismas konstatavo, kad ribojimas, kurį lemia prieiga prie šių duomenų, gali būti pateisintas tikslu užkardyti, tirti bei nustatyti „baudžiamąsias veikas“ apskritai ir vykdyti baudžiamąjį persekiojimą už jas, ir nereikalaujama, kad šios nusikalstamos veikos būtų kvalifikuojamos kaip „sunkios“ (61 ir 62 punktai).

2020 m. spalio 6 d. didžiosios kolegijos sprendimai „Privacy International“ (C-623/17, EU:C:2020:790) ir „La Quadrature du Net ir kt.“ (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791)[41]

Jurisprudencija, susijusi su asmens duomenų apsauga ir prieiga prie jų elektroninių ryšių sektoriuje, visų pirma Sprendimas *Tele2 Sverige* ir *Watson ir kt.*, kuriame Teisingumo Teismas, be kita ko, konstatavo, kad valstybės narės negali įpareigoti elektroninių ryšių paslaugų teikėjų bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenų, sukėlė susirūpinimą kai kurioms valstybėms narėms, nuogąstaujančioms, kad iš jų buvo atimta priemonė, kurią jos laikė būtina, siekiant užtikrinti nacionalinį saugumą ir kovoti su nusikalstamumu.

Esant šiam kontekstui, *Investigatory Powers Tribunal* (Bylų dėl tyrimų įgaliojimų teismas, Jungtinė Karalystė) (*Privacy International*, C-623/17), *Conseil d'État* (Valstybės Taryba, Prancūzija) (*La Quadrature du Net ir kt.*, sujungtos bylos C-511/18 ir C-512/18) bei *Cour constitutionnelle* (Konstitucinis Teismas, Belgija) (*Ordre des barreaux francophones et germanophone ir kt.*, C-520/18) nagrinėjo bylas dėl kai kurių valstybių narių šiose srityse priimtų teisės aktų, kuriais konkrečiai

[40] 2016 m. gruodžio 21 d. Teisingumo Teismo sprendimas *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970).
[41] Šie sprendimai pristatyti 2020 m. metiniame pranešime, p. 29–32.

numatoma elektroninių ryšių paslaugų teikėjų pareiga perduoti valdžios institucijai arba bendrai ir nediferencijuotai saugoti naudotojų srauto ir vietos nustatymo duomenis, teisėtumo.

Dviejuose sprendimuose, kuriuos 2020 m. spalio 6 d. paskelbė didžioji kolegija, Teisingumo Teismas visų pirma nusprendė, kad nacionalinės teisės aktai, kuriais elektroninių ryšių paslaugų teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis arba nurodytu tikslu perduoti šiuos duomenis nacionalinėms saugumo ir žvalgybos tarnyboms, patenka į Direktyvos 2002/58 taikymo sritį (Sprendimo *Privacy International* 49 punktas ir rezoliucinės dalies 1 punktas ir Sprendimo *La Quadrature du Net ir kt.* 104 punktas).

Be to, Teisingumo Teismas priminė, kad pagal Direktyvą 2002/58[42] neleidžiama, kad pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą ir draudimo saugoti šiuos duomenis išimtis taptų taisykle. Tai reiškia, kad pagal šią direktyvą valstybėms narėms, siekiant, be kita ko, užtikrinti nacionalinį saugumą, leidžiama imtis teisėkūros priemonių, kuriomis siekiama apriboti šioje direktyvoje nurodytų teisių ir pareigų, visų pirma pareigos užtikrinti pranešimų ir su jais susijusių srauto duomenų konfidencialumą, apimtį[43], tik laikantis bendrųjų Sąjungos teisės principų, įskaitant proporcingumo principą, ir Chartijoje garantuojamų pagrindinių teisių [44] (Sprendimo *Privacy International* 59 ir 60 punktai ir Sprendimo *La Quadrature du Net ir kt.* 111 ir 113 punktai).

Esant šiam kontekstui, Teisingumo Teismas, pirma, byloje *Privacy International* nusprendė, kad pagal Direktyvą 2002/58, siejamą su Chartija, draudžiami nacionalinės teisės aktai, kuriais, siekiant užtikrinti nacionalinį saugumą, elektroninių ryšių paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai perduoti srauto ir vietos nustatymo duomenis saugumo ir žvalgybos tarnyboms. Antra, sujungtose bylose *La Quadrature du Net ir kt.* ir byloje *Ordre des barreaux francophones et germanophone ir kt.* Teisingumo Teismas konstatavo, kad pagal tą pačią direktyvą draudžiamos teisėkūros priemonės, kuriomis prevenciškai elektroninių ryšių paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis.

Iš tiesų šie įpareigojimai bendrai ir nediferencijuotai perduoti ir saugoti tokius duomenis yra ypač dideli Chartijos garantuojamų pagrindinių teisių suvaržymai, nors asmenų, kurių duomenys tvarkomi, elgesys nėra susijęs su nagrinėjamais teisės aktais siekiamu tikslu. Pagal analogiją Teisingumo Teismas aiškino BDAR 23 straipsnio 1 dalį, siejamą su Chartija, taip, kad ji draudžia nacionalinės teisės aktus, kuriais prieigos prie visuomenei skirtų ryšių paslaugų internetu teikėjai ir prieglobos paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai saugoti, be kita ko, su šiomis paslaugomis susijusius asmens duomenis (Sprendimo *Privacy International* 71, 82 punktai ir rezoliucinės dalies 2 punktas ir Sprendimo *La Quadrature du Net ir kt.* 146, 168, 174, 177, 212 punktai ir rezoliucinės dalies 1 ir 3 punktai).

Vis dėlto Teisingumo Teismas nustatė, kad tais atvejais, kai atitinkama valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra, esama arba numatoma, pagal Direktyvą 2002/58, siejamą su Chartija, nedraudžiama elektroninių ryšių paslaugų teikėjus įpareigoti bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis. Esant tokiam kontekstui, Teisingumo Teismas patikslino, kad sprendimui, kuriuo nustatytas toks įpareigojimas

---

42 Direktyvos 2002/58 15 straipsnio 1 ir 3 dalys.

43 Direktyvos 2002/58 5 straipsnio 1 dalis.

44 Konkrečiai kalbant, Chartijos 7, 8 ir 11 straipsniai ir 52 straipsnio 1 dalis.

laikotarpiu, neviršijančiu to, kas griežtai būtina, turi būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi numatytų sąlygų ir garantijų. Tokiomis pačiomis sąlygomis pagal minėtą direktyvą taip pat nedraudžiama visų elektroninių ryšių priemonių naudotojų duomenų, visų pirma srauto ir vietos nustatymo, automatizuota analizė (Sprendimo *La Quadrature du Net ir kt.* 137–139, 177–179 punktai ir rezoliucinės dalies 1 ir 2 punktai).

Teisingumo Teismas pridūrė, kad pagal Direktyvą 2002/58, siejamą su Chartija, nedraudžiamos teisėkūros priemonės, numatančios tikslinį srauto ir vietos nustatymo duomenų saugojimą, kuris, remiantis objektyviais ir nediskriminaciniais veiksniais bei atsižvelgiant į duomenų subjektų kategorijas arba geografinius kriterijus, būtų apribotas laikotarpiu, neviršijančiu to, kas griežtai būtina. Minėta direktyva taip pat nedraudžia nei teisėkūros priemonių, numatančių bendrą ir nediferencijuotą ryšio šaltinio IP adresų saugojimą laikotarpiu, neviršijančiu to, kas griežtai būtina, nei priemonių, numatančių tokį bendrą ir nediferencijuotą duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimą; šiuo atveju valstybės narės nėra įpareigotos apriboti saugojimo laikotarpio. Be to, minėta direktyva nedraudžia teisėkūros priemonės, numatančios galimybę taikyti operatyvų paslaugų teikėjų turimų duomenų saugojimą, susiklosčius situacijoms, kai, siekiant išaiškinti sunkias nusikalstamas veikas ar nacionalinio saugumo pažeidimus, tokius duomenis saugoti yra būtina ilgiau, nei įstatyme nustatyti duomenų saugojimo terminai, ir kai tokios nusikalstamos veikos ar pažeidimai jau yra konstatuoti arba kai pagrįstai įtariamas jų egzistavimas (Sprendimo *La Quadrature du Net ir kt.* 161, 163, 168 punktai ir rezoliucinės dalies 1 punktas).

Be to, Teisingumo Teismas nusprendė, kad pagal Direktyvą 2002/58, siejamą su Chartija, nedraudžiami nacionalinės teisės aktai, kurie elektroninių ryšių paslaugų teikėjus įpareigoja realiuoju laiku rinkti duomenis, visų pirma srauto ir vietos nustatymo duomenis, jeigu toks rinkimas susijęs tik su tais asmenimis, dėl kurių yra pagrįsta priežastis įtarti, kad jie vienaip ar kitaip susiję su terorizmo veikla, ir jeigu tokiam duomenų rinkimui taikoma išankstinė teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, užtikrinant, kad toks duomenų rinkimas realiuoju laiku leidžiamas neviršijant to, kas griežtai būtina. Skubos atveju kontrolė turi būti vykdoma per trumpą laiką (Sprendimo *La Quadrature du Net ir kt.* 192 punktas ir rezoliucinės dalies 2 punktas).

Galiausiai Teisingumo Teismas nagrinėjo klausimą dėl nesuderinamais su Sąjungos teise pripažintų nacionalinės teisės aktų galiojimo laiko atžvilgiu. Šiuo klausimu jis nusprendė, kad nacionalinis teismas negali taikyti nacionalinės teisės nuostatos, suteikiančios jam teisę apriboti laiko atžvilgiu poveikį aktų, kuriuos jis turi pripažinti negaliojančiais ir pagal kuriuos elektroninių ryšių paslaugų teikėjai įpareigojami taikyti bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, pripažintą nesuderinamu su Direktyva 2002/58, siejama su Chartija.

Atsižvelgiant į tai, siekdamas prašymą priimti prejudicinį sprendimą pateikusiam teismui pateikti naudingą atsakymą Teisingumo Teismas priminė, kad pagal šiuo metu galiojančią Sąjungos teisę informacijos ir įrodymų, gautų prieštaraujant Sąjungos teisei saugant duomenis, priimtinumo ir vertinimo baudžiamajame procese, pradėtame dėl sunkiomis nusikalstamomis veikomis įtariamų asmenų, klausimas sprendžiamas remiantis tik nacionaline teise. Vis dėlto Teisingumo Teismas patikslino, kad remiantis Direktyva 2002/58, aiškinama atsižvelgiant į veiksmingumo principą, vykstant baudžiamajam procesui, nacionalinis teismas turi atmesti įrodymus, gautus atliekant su Sąjungos teise nesuderinamą bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų

saugojimą, jeigu asmenys, įtariami padarę nusikalstamas veikas, negali veiksmingai pareikšti nuomonės dėl šių įrodymų (Sprendimo *La Quadrature du Net ir kt.* 222, 228 punktai ir rezoliucinės dalies 4 punktas).

2021 m. kovo 2 d. didžiosios kolegijos Sprendimas „Prokuratuur“ (Prieigos prie elektroninių pranešimų duomenų sąlygos) (C-746/18, EU:C:2021:152)

Estijoje H. K. buvo iškelta baudžiamoji byla dėl vagysčių, pasinaudojimo trečiojo asmens banko kortele ir smurto prieš teismo procese dalyvaujančius asmenis. Pirmosios instancijos teismas nuteisė H. K. už šias nusikalstamas veikas dvejų metų laisvės atėmimo bausme. Šis nuosprendis vėliau patvirtintas apeliacinėje instancijoje. Protokolai, kuriais remiantis konstatuotos šios nusikalstamos veikos, buvo parengti, be kita ko, pasinaudojus asmens duomenimis, surinktais teikiant elektroninių ryšių paslaugas. *Riigikohus* (Aukščiausiasis Teismas, Estija), kuriam H. K. pateikė kasacinį skundą, kilo abejonių, ar su Sąjungos teise[45] yra suderinamos sąlygos, kuriomis ikiteisminio tyrimo institucijos gavo prieigą prie šių duomenų.

Šios abejonės susijusios, pirma, su klausimu, ar laikotarpio, per kurį ikiteisminio tyrimo institucijos turėjo prieigą prie duomenų, trukmė yra kriterijus, leidžiantis įvertinti atitinkamų asmenų pagrindinių teisių suvaržymo, kurį lemia tokia prieiga, dydį. Kadangi šis laikotarpis buvo labai trumpas arba surinktų duomenų kiekis labai nedidelis, prašymą priimti prejudicinį sprendimą pateikusiam teismui kilo klausimas, ar kovos su nusikalstamumu apskritai, o ne vien kovos su sunkiais nusikaltimais, tikslas gali pateisinti tokį suvaržymą. Antra, prašymą priimti prejudicinį sprendimą pateikęs teismas abejojo, ar galima Estijos prokuratūrą, atsižvelgiant į įvairius pagal Estijos teisės aktus jai priskirtus uždavinius, laikyti „nepriklausoma“ administracine institucija, kaip tai suprantama pagal Sprendimą *Tele2 Sverige ir Watson ir kt.*[46], galinčia leisti ikiteisminio tyrimo institucijos prieigą prie atitinkamų duomenų.

Teisingumo Teismo didžiosios kolegijos sprendime konstatuota, kad pagal Direktyvą 2002/58, siejamą su Chartija, draudžiamos nacionalinės teisės normos, leidžiančios valdžios institucijų prieigą prie srauto duomenų ar vietos nustatymo duomenų, galinčių suteikti informacijos apie elektroninių ryšių priemonės naudotojo pranešimus arba jo naudojamų galinių įrenginių vietą ir leisti padaryti tikslias išvadas apie jo privatų gyvenimą nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo už jas tikslais, neribojant šios prieigos taikymo vien procedūroms, kuriomis siekiama kovoti su sunkiais nusikaltimais arba užkirsti kelią didelėms grėsmėms visuomenės saugumui. Teisingumo Teismas nurodė, kad laikotarpis, už kurį prašoma leisti susipažinti su šiais duomenimis, ir šiuo laikotarpiu turimų duomenų kiekis ar pobūdis šiuo atžvilgiu neturi reikšmės. Be to, Teisingumo Teismas nusprendė, kad pagal šią direktyvą, siejamą su Chartija, draudžiamos nacionalinės teisės normos, suteikiančios prokuratūrai įgaliojimus leisti valdžios institucijos prieigą prie srauto duomenų ir vietos nustatymo duomenų ikiteisminio tyrimo tikslais (45, 59 punktai ir rezoliucinės dalies 1 ir 2 punktai).

Kiek tai susiję su nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo už jas tikslu, kurio siekiama nagrinėjamomis teisės normomis, remdamasis proporcingumo principu Teisingumo Teismas nusprendė, kad tik kovos su sunkiais nusikaltimais arba didelių grėsmių visuomenės saugumui prevencijos tikslai gali pateisinti valdžios institucijų

[45] Konkrečiau kalbant, su Direktyvos 2002/58 15 straipsnio 1 dalimi, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi.

[46] 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970, 120 punktas).

prieigą prie visų srauto ar vietos nustatymo duomenų, galinčių leisti daryti tikslias išvadas apie atitinkamų asmenų privatų gyvenimą, o kiti veiksniai, susiję su prašymo leisti susipažinti su duomenimis proporcingumu, kaip antai laikotarpio, už kurį prašoma leisti susipažinti su tokiais duomenimis, trukmė, negali lemti, kad nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo už jas apskritai tikslas pateisintų tokią prieigą (33 ir 35 punktai).

Dėl prokuratūrai suteiktos kompetencijos leisti valdžios institucijos prieigą prie srauto duomenų ir vietos nustatymo duomenų vadovaujant ikiteisminiam tyrimui Teisingumo Teismas priminė, kad nacionalinėje teisėje turi būti nustatytos sąlygos, kurioms esant elektroninių ryšių paslaugų teikėjai turi suteikti kompetentingoms nacionalinėms institucijoms prieigą prie duomenų, kuriais disponuoja. Vis dėlto, kad tokios teisės normos atitiktų proporcingumo reikalavimą, jose turi būti numatytos aiškios ir tikslios taisyklės, reglamentuojančios nagrinėjamos priemonės apimtį ir taikymą bei nustatančios minimalius reikalavimus, kad asmenys, kurių asmens duomenys tvarkomi, turėtų pakankamai garantijų, leidžiančių veiksmingai apsaugoti šiuos duomenis nuo piktnaudžiavimo pavojų. Tokios teisės normos turi būti teisiškai privalomos pagal nacionalinę teisę ir jose turi būti nurodyta, kokiomis aplinkybėmis ir materialinėmis bei procedūrinėmis sąlygomis gali būti imtasi tokių duomenų tvarkymą numatančios priemonės, taip užtikrinant, kad teisių suvaržymas neviršytų to, kas griežtai būtina (48 punktas).

Teisingumo Teismas nurodė, kad siekiant praktiškai užtikrinti visišką tokių sąlygų laikymąsi būtina, kad, prieš suteikiant kompetentingoms nacionalinėms institucijoms prieigą prie saugomų duomenų, teismas arba nepriklausomas administracinis subjektas atliktų išankstinę kontrolę ir savo sprendimą priimtų gavęs motyvuotą šių institucijų prašymą, pateiktą, be kita ko, vykdant prevencijos, atskleidimo arba baudžiamojo persekiojimo procedūras. Tinkamai pagrįstos skubos atveju kontrolė turi būti įvykdyta per trumpą laiką (51 punktas).

Šiuo klausimu Teisingumo Teismas pažymėjo, kad atliekant išankstinę kontrolę, be kita ko, reikalaujama, kad teismas ar subjektas, kuriam pavesta ją atlikti, turėtų visus įgaliojimus ir suteiktų visas garantijas, būtinas užtikrinti įvairių nagrinėjamų interesų ir teisių suderinimui. Konkrečiau kalbant apie ikiteisminį tyrimą, pažymėtina, kad tokiai kontrolei vykdyti reikia, kad šis teismas arba subjektas galėtų užtikrinti teisingą pusiausvyrą tarp interesų, susijusių su tyrimo poreikiais kovojant su nusikalstamumu, ir asmenų, prie kurių duomenų suteikiama prieiga, pagrindinių teisių į privataus gyvenimo gerbimą ir asmens duomenų apsaugą. Kai šią kontrolę vykdo ne teismas, o nepriklausomas administracinis subjektas, jis turi turėti statusą, leidžiantį jam vykdyti savo funkcijas objektyviai ir nešališkai, ir šiuo tikslu jis turi būti apsaugotas nuo bet kokios išorinės įtakos (52 ir 53 punktai).

Kaip nurodė Teisingumo Teismas, iš to matyti, kad nepriklausomumo reikalavimas, kurį turi atitikti institucija, atsakinga už išankstinę kontrolę, reiškia, kad ši institucija turi turėti trečiojo asmens statusą institucijos, prašančios leisti susipažinti su duomenimis, atžvilgiu, kad pirmoji institucija galėtų objektyviai ir nešališkai vykdyti šią kontrolę be jokios išorinės įtakos. Konkrečiai baudžiamosios teisės srityje nepriklausomumo reikalavimas reiškia, kad už šią išankstinę kontrolę atsakinga institucija, pirma, nedalyvauja vykdant nagrinėjamą ikiteisminį tyrimą ir, antra, turi būti nešališka baudžiamojo proceso šalims. Taip nėra prokuratūros, kuri, kaip Estijos prokuratūra, vadovauja ikiteisminiam tyrimui ir prireikus palaiko valstybinį kaltinimą, atveju. Vadinasi, prokuratūra negali atlikti minėtos išankstinės kontrolės (54, 55 ir 57 punktai).

IV. Asmens duomenų perdavimas į trečiąsias šalis

2003 m. lapkričio 6 d. didžiosios kolegijos Sprendimas „Lindqvist“ (C-101/01, EU:C:2003:596)[47]

Šioje byloje (taip pat žr. skyrių II.3. „Sąvoka „asmens duomenų tvarkymas“) prašymą priimti prejudicinį sprendimą pateikęs teismas visų pirma norėjo išsiaiškinti, ar B. Lindqvist perdavė duomenis į trečiąją šalį, kaip tai suprantama pagal minėtą direktyvą.

Teisingumo Teismas nusprendė, kad „duomenų perdavimas į trečiąsias šalis“, kaip tai suprantama pagal Direktyvos 95/46 25 straipsnį, nevyksta, kai vienoje valstybėje narėje esantis asmuo interneto puslapyje, saugomame interneto svetainės, kurioje yra šis puslapis, prieglobą teikiančio toje pačioje ar kitoje valstybėje narėje įsisteigusio fizinio ar juridinio asmens, įrašo asmens duomenis ir taip juos padaro prieinamus visiems prie interneto prisijungusiems asmenims, įskaitant esančius trečiosiose šalyse (71 punktas ir rezoliucinės dalies 4 punktas).

Atsižvelgiant į, viena vertus, interneto technologijų pažangą rengiant Direktyvą 95/46 ir, kita vertus, į tai, kad jos IV skyriuje, kuriame yra minėtas 25 straipsnis, užtikrinantis, kad valstybės narės kontroliuotų asmens duomenų perdavimą į trečiąsias šalis ir draudžiama atlikti tokį perdavimą, kai jos neužtikrina adekvataus apsaugos lygio, nėra interneto naudojimo kriterijų, negalima preziumuoti, kad Bendrijos teisės aktų leidėjas į sąvoką „duomenų perdavimas į trečiąsias šalis“ ketino įtraukti tokį duomenų įrašymą į interneto puslapį, net jeigu jie dėl to tampa prieinami trečiųjų šalių asmenims, turintiems prieigai prie tokių duomenų reikalingas technines priemones (63, 64 ir 68 punktai).

2015 m. spalio 6 d. didžiosios kolegijos Sprendimas „Schrems“ (C-362/14, EU:C:2015:650)[48]

Austrijos pilietis ir socialinio tinklo *Facebook* vartotojas M. Schrems pateikė skundą *Data Protection Commissioner* (Duomenų apsaugos komisaras, Airija) dėl to, kad *Facebook Ireland* perdavinėjo į Jungtines Amerikos Valstijas (JAV) šių vartotojų asmens duomenis ir juos saugojo toje šalyje esančiuose serveriuose, kur jie buvo tvarkomi. Anot M. Schrems, JAV teisė ir praktika nesuteikia pakankamos apsaugos nuo valdžios institucijų vykdomo į šią šalį perduotų duomenų sekimo. Duomenų apsaugos komisaras atsisakė tirti šį skundą, be kita ko, motyvuodamas tuo, kad Sprendime 2000/520[49] Komisija konstatavo, jog pagal „saugaus uosto“ (anglų k. „safe harbour“)[50] sistemą JAV užtikrina adekvatų perduotų asmens duomenų apsaugos lygį.

Būtent tokiomis aplinkybėmis *High Court* (Aukštasis teismas, Airija) Teisingumo Teismui pateikė prašymą išaiškinti Direktyvos 95/46 25 straipsnio 6 dalį, pagal kurią Komisija gali konstatuoti, kad trečioji šalis užtikrina adekvatų perduotų duomenų apsaugos lygį, taip pat iš esmės prašymą patvirtinti Sprendimo 2000/520, kurį Komisija priėmė remdamasi Direktyvos 95/46 25 straipsnio 6 dalimi, galiojimą.

---

47 Šis sprendimas pristatytas 2003 m. metiniame pranešime, p. 67.

48 Šis sprendimas pristatytas 2015 m. metiniame pranešime, p. 53.

49 2000 m. liepos 26 d. Komisijos sprendimas 2000/520 dėl Europos Parlamento ir Tarybos direktyvos 95/46 dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“ (OL L 215, 2000, p. 7).

50 „Saugaus uosto“ sistema apima tam tikrus su asmens duomenų apsauga susijusius principus, kuriuos JAV įmonės gali savanoriškai taikyti.

Teisingumo Teismas visą Komisijos sprendimą pripažino negaliojančiu, visų pirma pabrėždamas, kad jam priimti pirmiausia reikėjo, kad Komisija tinkamai motyvuodama konstatuotų, jog atitinkama trečioji šalis iš tikrųjų užtikrina iš esmės tokį patį pagrindinių teisių apsaugos lygį, koks garantuojamas Sąjungos teisės sistemoje. Kadangi Sprendime 2000/520 Komisija to nepadarė, to sprendimo 1 straipsniu pažeidžiami reikalavimai, nustatyti Direktyvos 95/46 25 straipsnio 6 dalyje, siejamoje su Chartija, todėl jis negalioja. „Saugaus uosto“ principai taikomi tik įsipareigojusioms JAV organizacijoms, gaunančioms asmens duomenis iš Sąjungos, ir nereikalaujama, kad JAV valdžios institucijos būtų įpareigotos laikytis šių principų. Be to, Sprendimas 2000/520 leidžia nustatyti asmenų, kurių asmens duomenys yra arba gali būti perduoti iš Sąjungos į JAV, pagrindinių teisių apribojimus, tačiau jame nėra išvados dėl to, ar JAV esama valstybinio pobūdžio taisyklių, skirtų nustatyti, kiek šios teisės gali būti apribotos, ir nėra konstatuota, kad esama veiksmingos teisinės apsaugos nuo tokio pobūdžio apribojimų (82, 87–89, 96–98 punktai ir rezoliucinės dalies 2 punktas).

Be to, Teisingumo Teismas pripažino negaliojančiu Sprendimo 2000/520 3 straipsnį, kiek juo iš nacionalinių kontrolės institucijų atimami įgaliojimai, kuriuos jos turi pagal Direktyvos 95/46 28 straipsnį tuo atveju, kai asmuo nurodo aplinkybes, galinčias sukelti abejonių dėl Komisijos sprendimo, kuriame konstatuota, jog trečioji šalis užtikrina adekvatų apsaugos lygį, suderinamumo su privataus gyvenimo ir asmens pagrindinių laisvių ir teisių apsauga (102–104 punktai). Teisingumo Teismas padarė išvadą, kad Sprendimo 2000/520 1 ir 3 straipsnių negaliojimas turi įtakos viso šio sprendimo galiojimui (105 ir 106 punktai).

Kiek tai susiję su tokio apribojimo pateisinimo negalimumu, Teisingumo Teismas visų pirma pažymėjo, kad Sąjungos teisės aktuose, kuriais apribojamos pagrindinės teisės, užtikrinamos pagal Chartijos 7 ir 8 straipsnius, turi būti numatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojama priemonės apimtis ir taikymas ir nustatomi minimalūs reikalavimai, kad asmenims, kurių duomenims tai turi įtakos, būtų suteikta pakankamai garantijų, leidžiančių veiksmingai apsaugoti jų asmens duomenis nuo piktnaudžiavimo pavojų, taip pat bet kokios neteisėtos prieigos prie šių duomenų ir neteisėto jų naudojimo. Būtinybė turėti tokias garantijas yra dar svarbesnė tais atvejais, kai asmens duomenys tvarkomi automatiniu būdu ir kyla didelis neteisėtos prieigos prie šių duomenų pavojus (91 punktas).

Be to, pagrindinės teisės į privatų gyvenimą apsauga Sąjungos lygiu reikalauja, kad nukrypti nuo asmens duomenų apsaugos leidžiančios nuostatos ir jos apribojimai neviršytų to, kas yra griežtai būtina (92 punktas). Taigi, tuo, kas yra griežtai būtina, nėra ribojami teisės aktai, kurie apskritai leidžia saugoti visų asmenų, kurių duomenys buvo perduoti iš Sąjungos, visus tuos duomenis, jų nediferencijuojant, nenustatant jokių apribojimų arba išimčių pagal siekiamą tikslą ir nenumatant objektyvių kriterijų, leidžiančių nubrėžti ribas valstybės institucijų prieigai prie duomenų ir jų vėlesniam naudojimui konkrečiais, griežtai ribojamais ir galinčiais pateisinti apribojimą, taikomą tiek prieigai prie šių duomenų, tiek jų naudojimui, tikslais (93 punktas). Konkrečiai kalbant, teisės aktai, leidžiantys valstybės institucijoms apskritai susipažinti su elektroninės komunikacijos turiniu, kelia pavojų pagrindinės teisės į privatų gyvenimą esmei. Be to, teisės aktais, nenumatančiais asmeniui jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad jis gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos ištaisyti ar pašalinti, nepaisoma Chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės (94 ir 95 punktai).

2017 m. liepos 26 d. didžiosios kolegijos Nuomonė 1/15 (ES ir Kanados susitarimas dėl PNR) (EU:C:2017:592)

2017 m. liepos 26 d. Teisingumo Teismas pirmą kartą priėmė sprendimą dėl tarptautinio susitarimo projekto suderinamumo su Europos Sąjungos pagrindinių teisių chartija, konkrečiai – su nuostatomis, susijusiomis su privataus gyvenimo gerbimu ir asmens duomenų apsauga.

Europos Sąjunga ir Kanada vedė derybas dėl susitarimo dėl oro keleivių duomenų perdavimo ir tvarkymo (susitarimas dėl PNR (*Passenger Name Record*)); jis buvo pasirašytas 2014 m. Europos Sąjungos Tarybai paprašius Europos Parlamento jį patvirtinti, šis nusprendė pateikti Teisingumo Teismo klausimą, ar numatytas sudaryti susitarimas atitinka Sąjungos teisę.

Numatytas sudaryti susitarimas leidžia sistemingą ir nuolatinį visų keleivių PNR duomenų perdavimą Kanados valdžios institucijai tam, kad jie būtų naudojami ir saugomi, taip pat galimą jų tolesnį perdavimą kitoms institucijoms ir kitoms trečiosioms šalims, siekiant kovoti su terorizmu ir sunkiais tarpvalstybiniais nusikaltimais. Numatytame sudaryti susitarime, be kita ko, nurodytas penkerių metų duomenų saugojimo laikotarpis ir nustatyti konkretūs PNR duomenų saugumo ir vientisumo reikalavimai, kaip antai reikalavimas nedelsiant užmaskuoti neskelbtinus duomenis, taip pat jame numatyta teisė susipažinti su duomenimis, juos ištaisyti ir pašalinti bei galimybė pateikti administracinį skundą ar ieškinį.

PNR duomenys, apie kuriuos kalbama numatytame sudaryti susitarime, be oro keleivių pavardžių ir vardų bei jų koordinačių, apima informaciją, kurios reikia rezervacijai, kaip antai numatytas kelionės datas, maršrutą, informaciją, susijusią su bilietais ir tuo pačiu rezervacijos numeriu užregistruotų asmenų grupe, informaciją apie mokėjimo priemones ar sąskaitas, informaciją apie bagažą, taip pat bendras pastabas apie keleivius.

Savo nuomonėje Teisingumo Teismas priėjo prie išvados, kad PNR susitarimas negali būti sudarytas toks, koks jis suformuluotas, nes tam tikros jo nuostatos nesuderinamos su Sąjungos pripažįstamomis pagrindinėmis teisėmis.

Visų pirma Teisingumo Teismas konstatavo, kad tiek PNR duomenų perdavimas iš Sąjungos kompetentingai Kanados institucijai, tiek reglamentavimas, dėl kurio Sąjunga vedė derybas su Kanada, susijęs su šių duomenų saugojimo sąlygomis, jų naudojimu ir galimu vėlesniu perdavimu kitoms Kanados institucijoms, Europolui, Eurojustui, valstybių narių teisminėms institucijoms arba policijai ar kitų trečiųjų šalių institucijoms, riboja pagal Chartijos 7 straipsnį užtikrinamą teisę. Šie veiksmai riboja ir Chartijos 8 straipsnyje įtvirtintą pagrindinę teisę į asmens duomenų apsaugą, nes reiškia asmens duomenų tvarkymą (125 ir 126 punktai).

Be to, jis pabrėžia, kad net jeigu kai kurie PNR duomenys, vertinami atskirai, neatrodo kaip galintys atskleisti svarbią su atitinkamų asmenų privačiu gyvenimu susijusią informaciją, vis dėlto, vertinami kartu, jie gali atskleisti, be kita ko, visą kelionės maršrutą, kelionių įpročius, ryšius, egzistuojančius tarp dviejų ar daugiau asmenų, taip pat informaciją apie oro keleivių finansinę padėtį, jų mitybos įpročius ar sveikatos būklę, net galėtų atskleisti apie šiuos keleivius neskelbtinų duomenų, kurių apibrėžtis pateikta numatyto sudaryti susitarimo 2 straipsnio e punkte (informacija apie rasinę ar etninę kilmę, politines pažiūras, religinius įsitikinimus ir t. t.) (128 punktas).

Šiuo aspektu Teisingumo Teismas laikėsi nuomonės, kad nors nagrinėjamus apribojimus galima pateisinti bendrojo intereso tikslo siekimu (visuomenės saugumo garantija kovojant su terorizmu ir sunkiais tarpvalstybiniais nusikaltimais), tam tikros šio susitarimo nuostatos nėra apribotos tuo, kas griežtai būtina, ir jose nenustatyta aiškių ir tikslių taisyklių.

Konkrečiai kalbant, Teisingumo Teismas pažymėjo, jog atsižvelgiant į pavojų, kad duomenų tvarkymas gali pažeisti nediskriminavimo principą, neskelbtinų duomenų perdavimas Kanadai reikalauja tikslaus ir itin svaraus pateisinimo, kuris būtų grindžiamas kitais motyvais nei visuomenės apsauga nuo terorizmo ir sunkių tarpvalstybinių nusikaltimų. Šiuo atveju tokio pateisinimo nėra. Tuo remdamasis Teisingumo Teismas padarė išvadą, kad susitarimo dėl neskelbtinų duomenų perdavimo Kanadai ir dėl šių duomenų tvarkymo ir saugojimo nuostatos yra nesuderinamos su pagrindinėmis teisėmis (165 ir 232 punktai).

Antra, Teisingumo Teismas laikėsi nuomonės, kad, oro keleiviams išvykus iš Kanados, numatytame sudaryti susitarime nurodytas visų oro keleivių PNR duomenų kaupimas neapsiriboja tuo, kas griežtai būtina. Kiek tai susiję su oro keleiviais, dėl kurių nebuvo nustatytos terorizmo ar sunkių tarpvalstybinių nusikaltimų rizikos nuo jų atvykimo į Kanadą iki išvykimo iš jos, neatrodo, kad jiems išvykus tarp jų PNR duomenų ir numatytu sudaryti susitarimu siekiamo tikslo būtų ryšys (bent jau netiesioginis), kuris pateisintų šių duomenų saugojimą. Kita vertus, oro keleivių, dėl kurių buvo objektyvių įrodymų, leidžiančių manyti, kad jie netgi po to, kai išvyko iš Kanados, galėjo kelti riziką kovojant su terorizmu ir sunkiais tarpvalstybiniais nusikaltimais, PNR duomenis leidžiama saugoti ir jiems išvykus iš šios šalies, netgi penkerių metų laikotarpį (205–207 ir 209 punktai).

Trečia, Teisingumo Teismas konstatavo, kad Europos Sąjungos pagrindinių teisių chartijos 7 straipsnyje įtvirtinta teisė į privatų gyvenimą reiškia, jog atitinkamas asmuo turi turėti galimybę įsitikinti, kad jo asmens duomenys tvarkomi tiksliai ir teisėtai. Tam, kad toks asmuo galėtų atlikti reikiamus patikrinimus, jam turi būti suteikta teisė gauti savo asmens duomenis, kurie yra tvarkomi.

Šiuo aspektu jis pabrėžė, jog numatytame sudaryti susitarime svarbu, kad oro keleiviai būtų informuoti apie su jais susijusių keleivio duomenų perdavimą į atitinkamą trečiąją šalį ir apie šių duomenų naudojimą, ir tai būtų padaryta nuo momento, kai tokios informacijos suteikimas negali pakenkti numatytame sudaryti susitarime nurodytų valdžios institucijų atliekamiems tyrimams. Iš tiesų tokios informacijos reikia, kad oro keleiviai galėtų pasinaudoti teise prašyti leisti susipažinti su duomenimis apie save ir prireikus juos ištaisyti, taip pat pagal Chartijos 47 straipsnio pirmą pastraipą teise į veiksmingą gynybą teisme.

Taigi, atvejais, kai yra objektyvių įrodymų, pateisinančių keleivių duomenų naudojimą siekiant kovoti su terorizmu ir sunkiais tarpvalstybiniais nusikaltimais ir lemiančių poreikį gauti išankstinį teisminės institucijos arba nepriklausomo administracinio subjekto leidimą, oro keleivius reikia informuoti individualiai. Tas pats taikytina tuo atveju, kai su oro keleiviais susiję duomenys perduodami kitoms valdžios institucijoms arba privatiems asmenims. Vis dėlto toks informacijos suteikimas galimas tik nuo momento, kai tai negali pakenkti numatytame sudaryti susitarime nurodytų valdžios institucijų atliekamiems tyrimams (219, 220, 223 ir 224 punktai).

2020 m. liepos 16 d. didžiosios kolegijos Sprendimas „Facebook Ireland ir Schrems" (C-311/18, ECLI:EU:C:2015:559)[51]

BDAR nurodyta, kad iš principo galima perduoti tokius duomenis į trečiąją šalį, tik jei atitinkama trečioji šalis užtikrina tinkamą šių duomenų apsaugos lygį. Pagal šį reglamentą Komisija gali konstatuoti, kad trečioji šalis savo nacionalinės teisės aktais arba tarptautiniais įsipareigojimais užtikrina tinkamą apsaugos lygį[52]. Nesant tokio sprendimo dėl tinkamumo, tokį perdavimą galima atlikti, tik jei Sąjungoje įsteigtas asmens duomenų eksportuotojas numato tinkamas apsaugos priemones, kurios, be kita ko, gali kilti iš Komisijos priimtų standartinių duomenų apsaugos sąlygų, ir jei duomenų subjektai turi įgyvendinamas teises ir veiksmingas teisių gynimo priemones[53]. Be to, BDAR aiškiai nustatytos sąlygos, kuriomis galima atlikti tokį perdavimą nesant sprendimo dėl tinkamumo arba tinkamų apsaugos priemonių[54].

Maximillian Schrems yra Austrijoje gyvenantis šios šalies pilietis; nuo 2008 m. jis yra *Facebook* vartotojas. M. Schrems, kaip ir kitų Sąjungoje teritorijoje gyvenančių vartotojų, asmens duomenis (visus arba jų dalį) *Facebook Ireland* perduoda į Jungtinių Amerikos Valstijų teritorijoje esančius *Facebook Inc.* priklausančius serverius ir jie ten tvarkomi. M. Schrems pateikė Airijos priežiūros institucijai skundą, jame iš esmės prašė uždrausti šį duomenų perdavimą. Jis tvirtino, kad Jungtinių Amerikos Valstijų teisė ir praktika neužtikrina pakankamos apsaugos nuo valdžios institucijų prieigos prie į šią šalį perduodamų duomenų. Šis skundas buvo atmestas, be kita ko, motyvuojant tuo, kad Sprendime 2000/520[55] Komisija konstatavo, jog Jungtinės Valstijos užtikrina tinkamą duomenų apsaugos lygį. Gavęs *High Court* (Aukštasis Teismas, Airija) prejudicinį klausimą, 2015 m. spalio 6 d. sprendimu Teisingumo Teismas pripažino šį Komisijos sprendimą negaliojančiu (toliau – Sprendimas *Schrems*)[56] (52 ir 53 punktai).

Paskelbus Sprendimą *Schrems* ir vėliau Airijos teismui panaikinus sprendimą, kuriuo buvo atmestas M. Schrems skundas, Airijos priežiūros institucija paprašė jo performuluoti savo skundą atsižvelgiant į tai, kad Teisingumo Teismas pripažino negaliojančiu Sprendimą 2000/520. Performuluotame skunde M. Schrems teigė, kad Jungtinės Amerikos Valstijos neužtikrina pakankamos į šią šalį perduodamų asmens duomenų apsaugos. Jis prašė sustabdyti jo asmens duomenų perdavimą iš Sąjungos į Jungtines Amerikos Valstijas, kurį *Facebook Ireland* dabar atlieka, remdamasi Sprendimo 2010/87 priede pateiktomis standartinėmis apsaugos sąlygomis, arba uždrausti tokį perdavimą ateityje[57]. Manydama, kad M. Schrems skundo išnagrinėjimas, be kita ko, priklauso nuo Sprendimo 2010/87 galiojimo, priežiūros institucija inicijavo procesą *High Court* (Aukštasis Teismas), kad šis Teisingumo Teismui pateiktų prašymą priimti prejudicinį

[51] Šis sprendimas pristatytas 2020 m. metiniame pranešime, p. 26–29.
[52] BDAR 45 straipsnis.
[53] BDAR 46 straipsnio 1 ir 2 dalys.
[54] BDAR 49 straipsnis.
[55] 2000 m. liepos 26 d. Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46 dėl saugaus uosto privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų Dažnai užduodamų klausimų (OL L 215, 2000, p. 7; 2004 m. specialusis leidimas lietuvių k., 16 sk., 1 t., p. 119).
[56] 2015 m. spalio 6 d. Sprendimas *Schrems*, C-362/14, EU:C:2015:650 (taip pat žr. CP Nr. 117/15).
[57] 2010 m. vasario 5 d. Komisijos sprendimas dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46 nuostatas (OL L 39, 2010, p. 5), iš dalies pakeistas 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimu (ES) 2016/2297 (OL L 344, 2016, p. 100).

sprendimą. Pradėjus šią procedūrą, Komisija priėmė Sprendimą (ES) 2016/1250 dėl ES ir JAV duomenų apsaugos skydo užtikrinamos apsaugos tinkamumo[58] (54, 55 ir 57 punktai).

Prašymu priimti prejudicinį sprendimą šį prašymą pateikęs teismas Teisingumo Teismui pateikė klausimus dėl BDAR taikytinumo asmens duomenų perdavimui remiantis Sprendime 2010/87 pateiktomis standartinėmis apsaugos sąlygomis, dėl šiuo reglamentu reikalaujamo apsaugos lygio, kai atliekamas toks perdavimas, ir dėl šiomis aplinkybėmis priežiūros institucijoms tenkančių pareigų. Be to, *High Court* (Aukštasis Teismas) iškėlė klausimą tiek dėl Sprendimo 2010/87, tiek dėl Sprendimo 2016/1250 galiojimo.

Teisingumo Teismas konstatuoja, kad išnagrinėjus Sprendimą 2010/87 atsižvelgiant į Europos Sąjungos pagrindinių teisių chartiją (toliau – Chartija) nenustatyta nieko, kas galėtų paveikti jo galiojimą. Tačiau jis pripažino Sprendimą 2016/1250 negaliojančiu (rezoliucinės dalies 4 ir 5 punktai).

Visų pirma Teisingumo Teismas laikėsi nuomonės, kad Sąjungos teisė, be kita ko, BDAR, taikoma asmens duomenų perdavimui, kurį komerciniais tikslais atlieka valstybėje narėje įsteigtas ūkio subjektas kitam trečiojoje šalyje įsteigtam ūkio subjektui, net jei atliekant šį perdavimą arba po jo atitinkamos trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais. Jis pažymi, jog tai, kad trečiosios šalies institucijos atlieka tokį duomenų tvarkymą, nereiškia, kad jis nepatenka į BDAR taikymo sritį (86, 88, 89 punktai ir rezoliucinės dalies 1 punktas).

Dėl reikalaujamo apsaugos lygio atliekant tokį perdavimą Teisingumo Teismas nusprendė, kad šiuo tikslu BDAR nuostatose numatyti reikalavimai, susiję su tinkamomis apsaugos priemonėmis, įgyvendinamomis teisėmis ir veiksmingomis teisių gynimo priemonėmis, turi būti aiškinami taip, kad asmenų, kurių asmens duomenys perduodami į trečiąją šalį remiantis standartinėmis duomenų apsaugos sąlygomis, apsaugos lygis turi būti iš esmės lygiavertis tam, kuris garantuojamas Sąjungoje šiuo reglamentu, siejamu su Chartija. Šiomis aplinkybėmis jis pažymėjo, kad vertinant šį apsaugos lygį turi būti atsižvelgta ir į Sąjungoje įsteigto duomenų eksportuotojo ir atitinkamoje trečiojoje šalyje įsteigto perduodamų duomenų gavėjo sudarytų sutarčių sąlygas, ir, kiek tai susiję su galima šios trečiosios šalies valdžios institucijų prieiga prie taip perduotų asmens duomenų, į atitinkamus šios šalies teisinės sistemos aspektus (105 punktas ir rezoliucinės dalies 2 punktas).

Dėl vykstant tokiam perdavimui priežiūros institucijoms tenkančių pareigų Teisingumo Teismas nusprendė, kad, nebent Komisija yra teisėtai priėmusi sprendimą dėl tinkamumo, šios institucijos, be kita ko, privalo sustabdyti arba uždrausti duomenų perdavimą į trečiąją šalį, jei atsižvelgdamos į visas konkrečias šio perdavimo aplinkybes mano, kad šioje trečiojoje šalyje standartinių duomenų apsaugos sąlygų nesilaikoma arba jų negalima laikytis ir kad kitomis priemonėmis negalima užtikrinti pagal Sąjungos teisę reikalaujamos perduodamų duomenų apsaugos, jeigu Sąjungoje įsteigtas eksportuotojas pats nesustabdė arba nenutraukė tokio perdavimo (121 punktas ir rezoliucinės dalies 3 punktas).

[58] 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46 (OL L 207, 2016, p. 1).

Teisingumo Teismas taip pat išnagrinėjo Sprendimo 2010/87 galiojimą. Teisingumo Teismo teigimu, šio sprendimo galiojimo nepaneigia vien tai, kad jame pateiktos standartinės duomenų apsaugos sąlygos dėl savo sutartinio pobūdžio nėra privalomos trečiųjų šalių, į kurias gali būti perduodami asmens duomenys, valdžios institucijoms. Tačiau jis pažymėjo, kad minėto sprendimo galiojimas priklauso nuo to, ar jame yra įtvirtinti veiksmingi mechanizmai, leidžiantys praktiškai užtikrinti, kad būtų laikomasi Sąjungos teisėje reikalaujamo apsaugos lygio ir kad asmens duomenų perdavimas, grindžiamas tokiomis sąlygomis, būtų sustabdytas arba uždraustas pažeidus šias sąlygas ar nesant galimybės jų laikytis. Teisingumo Teismas konstatavo, kad Sprendime 2010/87 nustatyti tokie mechanizmai. Šiuo klausimu jis, be kita ko, pabrėžė, kad šiuo sprendimu duomenų eksportuotojui ir perduodamų duomenų gavėjui nustatyta pareiga iš anksto patikrinti, ar atitinkamoje trečiojoje šalyje laikomasi šio apsaugos lygio, ir kad pagal šį sprendimą šis gavėjas privalo informuoti duomenų eksportuotoją, jei negali laikytis standartinių apsaugos sąlygų, o šis eksportuotojas tuomet turi sustabdyti duomenų perdavimą ir (arba) nutraukti su duomenų gavėju sudarytą sutartį (132, 136, 137, 142, 148 punktai ir rezoliucinės dalies 4 punktas).

Galiausiai Teisingumo Teismas išnagrinėjo Sprendimo 2016/1250 galiojimą, atsižvelgdamas į reikalavimus, kylančius iš BDAR, siejamo su Chartijos nuostatomis, garantuojančiomis teisę į privatų ir šeimos gyvenimą, asmens duomenų apsaugą ir teisę į veiksmingą teisminę gynybą. Šiuo klausimu Teisingumo Teismas pažymėjo, kad tame sprendime, kaip ir Sprendime 2000/520, įtvirtinta reikalavimų, susijusių su nacionaliniu saugumu, viešuoju interesu ir JAV teisės aktų laikymusi, viršenybė, taigi remiantis ja galima nustatyti asmenų, kurių asmens duomenys perduodami į šią trečiąją šalį, pagrindinių teisių suvaržymus. Teisingumo Teismo teigimu, asmens duomenų apsaugos apribojimai, kurių kyla iš Jungtinių Amerikos Valstijų nacionalinės teisės aktų, susijusių su JAV valdžios institucijų prieiga prie tokių duomenų, perduodamų iš Sąjungos į šią trečiąją šalį, ir šių institucijų atliekamu jų naudojimu, ir kuriuos Komisija įvertino Sprendime 2016/1250, nėra sureglamentuoti taip, kad atitiktų reikalavimus, iš esmės lygiaverčius Sąjungos teisėje nustatytiems pagal proporcingumo principą, nes šiais teisės aktais grindžiamos stebėjimo programos neapsiriboja tuo, kas griežtai būtina. Remdamasis tame sprendime pateiktomis išvadomis Teisingumo Teismas pažymėjo, jog, kalbant apie tam tikras stebėjimo programas, iš minėtų teisės aktų jokiu būdu nematyti, kad juose yra įtvirtintų įgaliojimų įgyvendinti šias programas apribojimų ar garantijų ne JAV asmenims, kuriems gali būti taikomos šios programos. Teisingumo Teismas pridūrė, kad nors tuose teisės aktuose numatyti reikalavimai, kurių turi laikytis JAV valdžios institucijos, kai įgyvendina atitinkamas stebėjimo programas, pagal juos duomenų subjektams nesuteikiamos įgyvendinamos teisės, kuriomis jie galėtų remtis teismuose prieš JAV valdžios institucijas (164, 165, 180–182, 184 ir 185 punktai).

Dėl teisminės apsaugos reikalavimo Teisingumo Teismas nusprendė, kad, priešingai, nei Sprendime 2016/1250 konstatavo Komisija, tame sprendime nurodytu ombudsmeno mechanizmu šiems asmenims nesuteikiama teisių gynimo priemonė institucijoje, suteikiančioje garantijas, iš esmės lygiavertes reikalaujamoms Sąjungos teisėje, kuria galėtų būti užtikrintas tiek pagal šį mechanizmą numatyto ombudsmeno nepriklausomumas, tiek normų, kuriomis tas ombudsmenas būtų įgaliotas priimti JAV žvalgybos tarnyboms privalomus sprendimus, egzistavimas. Remdamasis visais šiais motyvais Teisingumo Teismas pripažino Sprendimą 2016/1250 negaliojančiu (195–197, 201 punktai ir rezoliucinės dalies 5 punktas).

V. Asmens duomenų apsauga internete

1. Teisė prieštarauti asmens duomenų tvarkymui („Teisė būti pamirštam“)

2014 m. gegužės 13 d. didžiosios kolegijos Sprendimas „Google Spain ir Google“ (C-131/12, EU:C:2014:317)

Šiame sprendime (taip pat žr. II.3 skyrių „Sąvoka „asmens duomenų tvarkymas“) Teisingumo Teismas patikslino Direktyvoje 95/46 numatytos teisės susipažinti su asmens duomenimis ir teisės prieštarauti dėl jų tvarkymo internete apimtį.

Taigi, priimdamas sprendimą dėl interneto paieškos variklio eksploatuotojo atsakomybės masto Teisingumo Teismas iš esmės nurodė, kad, siekiant užtikrinti Direktyvos 95/46 12 straipsnio b punkte ir 14 straipsnio pirmos pastraipos a punkte numatytą teisę susipažinti su informacija ir teisę prieštarauti, ir jeigu iš tiesų įvykdytos juose numatytos sąlygos, šis eksploatuotojas privalo iš rezultatų sąrašo, rodomo atlikus paiešką pagal asmens asmenvardį, pašalinti nuorodas į trečiųjų asmenų paskelbtus tinklalapius, kuriuose yra informacijos apie šį asmenį. Teisingumo Teismas pažymėjo, kad tokia pareiga gali kilti ir tais atvejais, kai šis asmenvardis arba ši informacija nėra prieš tai ištrinti arba tuo pačiu metu ištrinami iš šių tinklalapių, net jei atitinkami duomenys šiuose tinklalapiuose paskelbti teisėtai (88 punktas ir rezoliucinės dalies 3 punktas).

Be to, paklaustas, ar pagal šią direktyvą atitinkamas asmuo gali prašyti iš tokio rezultatų sąrašo pašalinti nuorodas į tinklalapius, motyvuodamas tuo, kad nori, jog su juo susijusi informacija po tam tikro laiko būtų „pamiršta“, Teisingumo Teismas visų pirma pažymėjo, kad net iš pradžių teisėtas tikslių duomenų tvarkymas, praėjus tam tikram laikui, gali nebeatitikti šios direktyvos, jei tie duomenys nebereikalingi tais tikslais, dėl kurių buvo surinkti arba tvarkomi; be kita ko, taip yra tuo atveju, kai duomenys atrodo neadekvatūs, nereikšmingi ar nebereikšmingi arba pertekliniai atsižvelgiant į tikslus arba praėjusį laiką (93 punktas). Todėl jei atitinkamo asmens prašymu konstatuojama, kad šių nuorodų įtraukimas į rezultatų sąrašą tuo etapu yra nesuderinamas su minėta direktyva, atitinkama šio sąrašo informacija ir nuorodos turi būti ištrintos (94 punktas). Tokiomis aplinkybėmis konstatavimas, kad atitinkamas asmuo turi teisę į tai, kad su juo susijusi informacija rezultatų sąraše nebebūtų siejama su jo asmenvardžiu, nereiškia, jog įtraukus tam tikrą informaciją į rezultatų sąrašą atitinkamam asmeniui yra padaryta žalos (96 punktas ir rezoliucinės dalies 4 punktas).

Galiausiai Teisingumo Teismas pažymėjo: kadangi atitinkamas asmuo, atsižvelgiant į Chartijos 7 ir 8 straipsniuose jam suteiktas pagrindines teises, gali prašyti, kad atitinkama informacija nebebūtų pateikiama plačiajai visuomenei įtraukiant ją į tokį rezultatų sąrašą, šios teisės iš principo yra viršesnės ne tik už paieškos variklio eksploatuotojo ekonominį interesą, bet ir už visuomenės interesą surasti tą informaciją vykdant paiešką pagal šio subjekto asmenvardį. Tačiau taip nebūtų tuo atveju, jei dėl konkrečių aplinkybių, kaip antai šio subjekto padėties viešajame gyvenime, paaiškėtų, kad šių pagrindinių teisių apribojimą pateisina viršesnis visuomenės interesas dėl įtraukimo į atitinkamus sąrašus turėti prieigą prie tam tikros informacijos (97 punktas ir rezoliucinės dalies 4 punktas).

2. Asmens duomenų tvarkymas ir teisė į intelektinę nuosavybę

2008 m. sausio 29 d. didžiosios kolegijos Sprendimas „Promusicae“ (C-275/06, EU:C:2008:54)[59]

Ispanijos pelno nesiekianti asociacija *Promusicae*, jungianti muzikos ir audiovizualinių įrašų gamintojus ir leidėjus, kreipėsi į Ispanijos teismus su prašymu nurodyti *Telefónica de España SAU* (komercinė bendrovė, be kita ko, teikianti prieigos prie interneto paslaugas) atskleisti tam tikrų asmenų, kuriems ji teikė prieigos prie interneto paslaugą ir kurių IP adresas, taip pat prisijungimo data ir laikas buvo žinomi, tapatybę ir fizinį adresą. Anot *Promusicae*, šie asmenys naudojosi rinkmenų pasikeitimo programa, vadinamąja „peer to peer“ arba P2P (skaidri dalijimosi turiniu priemonė, kuri yra nepriklausoma, decentralizuota ir naudoja pažangias paieškos ir atsisiuntimo funkcijas), ir leido prieigą prie jų asmeninio kompiuterio laisvai prieinamų duomenų rinkmenoje esančių fonogramų, kurių turtinės panaudojimo teisės priklausė *Promusicae* nariams. Taigi ji paprašė suteikti šią informaciją tam, kad galėtų pradėti civilinius procesus prieš suinteresuotuosius asmenis.

Tokiomis aplinkybėmis *Juzgado de lo Mercantil no 5 de Madrid* (Madrido komercinis teismas Nr. 5, Ispanija) pateikė Teisingumo Teismui klausimą, ar Sąjungos teisės aktai įpareigoja valstybes nares numatyti pareigą pateikti asmens duomenis vykstant civiliniam procesui tam, kad būtų užtikrinta veiksminga autorių teisių apsauga.

Anot Teisingumo Teismo, šiame prašyme priimti prejudicinį sprendimą keltas klausimas dėl būtinybės suderinti reikalavimus, susijusius su įvairių pagrindinių teisių apsauga, t. y. teisės į privataus gyvenimo gerbimą ir teisių į nuosavybės apsaugą bei į veiksmingas teisinės gynybos priemones.

Šiuo aspektu Teisingumo Teismas padarė išvadą, kad, esant tokiai situacijai, kokia nagrinėta pagrindinėje byloje, Direktyva 2000/31 dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva)[60], Direktyva 2001/29 dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo[61], Direktyva 2004/48 dėl intelektinės nuosavybės teisių gynimo[62] ir Direktyva 2002/58 neįpareigoja valstybių narių, užtikrinant veiksmingą autorių teisių apsaugą, numatyti pareigą pateikti asmens duomenis vykstant civiliniam procesui. Vis dėlto Sąjungos teisė reikalauja, kad perkeldamos šias direktyvas šios valstybės užtikrintų, kad bus vadovaujamasi tokiu jų aiškinimu, kuris leistų garantuoti teisingą skirtingų Bendrijos teisės sistemos saugomų pagrindinių teisių pusiausvyrą. Be to, įgyvendindamos minėtas direktyvas perkeliančias priemones valstybių narių valdžios institucijos ir teismai privalo ne tik aiškinti savo nacionalinę teisę taip, kad ši atitiktų šias direktyvas, bet ir nesivadovauti tokiu jų aiškinimu, kuris pažeistų minėtas pagrindines teises arba kitus bendruosius Bendrijos teisės principus, kaip antai proporcingumo principą (70 punktas ir rezoliucinė dalis).

---

59 Šis sprendimas pristatytas 2008 m. metiniame pranešime, p. 46.

60 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31 dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva) (OL L 178, 2000, p. 1; 2004 m. specialusis leidimas lietuvių k., 13 sk., 25 t., p. 399).

61 2001 m. gegužės 22 d. Europos Parlamento ir Tarybos direktyva 2001/29 dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo (OL L 167, 2001, p. 10; 2004 m. specialusis leidimas lietuvių k., 17 sk., 1 t., p. 230).

62 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos direktyva 2004/48 dėl intelektinės nuosavybės teisių gynimo (OL L 157, 2004, p. 45; 2004 m. specialusis leidimas lietuvių k., 17 sk., 2 t., p. 32).

2011 m. lapkričio 24 d. Sprendimas „Scarlet Extended“ (C-70/10, EU:C:2011:771)[63]

Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) konstatavo, kad interneto prieigos paslaugų teikėjos *Scarlet Extended SA* (toliau – *Scarlet*) paslaugomis besinaudojantys interneto vartotojai be leidimo ir nemokėdami mokesčių internete siuntėsi jos kataloge esančius kūrinius, pasinaudodami „peer-to-peer“ tinklais. SABAM kreipėsi į nacionalinį teismą, o šis pirmojoje instancijoje įpareigojo *Scarlet* nutraukti šiuos autorių teisių pažeidimus, užkertant kelią savo klientams pasinaudojant „peer-to-peer“ programine įranga bet kokia forma siųsti ar gauti elektronines rinkmenas su muzikos kūriniais iš SABAM repertuaro.

Gavęs *Scarlet* skundą, *cour d'appel de Bruxelles* (Briuselio apeliacinis teismas, Belgija) atidėjo sprendimo priėmimą ir pateikė Teisingumo Teismui prejudicinį klausimą, ar toks įpareigojimas yra suderinamas su Sąjungos teise.

Teisingumo Teismas nusprendė, kad direktyvas 95/46, 2000/31, 2001/29, 2002/58 ir 2004/48, aiškinamas kartu ir atsižvelgiant į iš taikytinų pagrindinių teisių apsaugos kylančius reikalavimus, reikia aiškinti taip, kad jomis draudžiama įpareigoti *Scarlet* įdiegti filtravimo sistemą (visiems naudojantis jos paslaugomis gaunamiems ir siunčiamiems elektroniniams pranešimams, per, be kita ko, „peer-to-peer“ programinę įrangą, visų jos klientų atžvilgiu, prevenciškai, tik jos sąskaita, neterminuotai), leidžiančią nustatyti tokio tiekėjo tinklu siunčiamas muzikos, kinematografijos ar audiovizualinių kūrinių, kurių intelektinės nuosavybės teisės tariamai priklauso ieškovui, elektronines rinkmenas, kad būtų galima užblokuoti tokių rinkmenų, kuriomis keičiantis pažeidžiamos autorių teisės, persiuntimą (54 punktas ir rezoliucinė dalis).

Anot Teisingumo Teismo, toks įpareigojimas pažeidžia Direktyvos 2000/31 15 straipsnio 1 dalyje įtvirtintą draudimą tokiam paslaugų teikėjui nustatyti bendrą priežiūros pareigą ir reikalavimą užtikrinti tinkamą pusiausvyrą tarp, viena vertus, intelektinės nuosavybės teisės ir, kita vertus, laisvės užsiimti verslu, teisės į asmens duomenų apsaugą ir laivės gauti ir skleisti informaciją (40, 49 punktai).

Šiomis aplinkybėmis Teisingumo Teismas pažymėjo, kad, pirma, įpareigojimas įdiegti ginčijamą filtravimo sistemą reikštų, kad reikia sistemingai analizuoti visų pranešimų turinį ir rinkti informaciją apie vartotojų, kurie siunčia neleistino turinio pranešimus tinklu, IP adresus ir juos nustatyti, nors šie adresai yra saugomų asmens duomenų dalis, nes leidžia tiksliai nustatyti tokius vartotojus (51 punktas). Antra, kyla pavojus, kad šis įpareigojimas pažeis informacijos laisvę, nes yra rizika, kad naudojantis šia sistema nebus galimybės tinkamai atskirti neleistino ir leistino turinio pranešimų, taigi ją naudojant galėtų būtų blokuojami leistino turinio pranešimai. Iš tiesų neginčijama, kad atsakymas į klausimą dėl siuntimo teisėtumo priklauso ir nuo autorių teisėms taikomų teisės aktuose numatytų išimčių, kurios valstybėse narėse skiriasi. Be to, kai kuriose valstybėse narėse tam tikri kūriniai gali būti viešai prieinami arba patalpinti internete, jų autoriams leidus jais naudotis nemokamai (52 punktas).

Taigi Teisingumo Teismas konstatavo, kad nustatęs *Scarlet* įpareigojimą įdiegti ginčijamą filtravimo sistemą atitinkamas nacionalinis teismas nesilaikytų reikalavimo užtikrinti tinkamą pusiausvyrą tarp, viena vertus, intelektinės nuosavybės teisės ir, kita vertus, laisvės užsiimti verslu, teisės į asmens duomenų apsaugą ir laivės gauti ir skleisti informaciją (53 punktas).

[63] Šis sprendimas pristatytas 2011 m. metiniame pranešime, p. 37.

2012 m. balandžio 19 d. Sprendimas „Bonnier Audio ir kt.“ (C-461/10, EU:C:2012:219)

Högsta domstolen (Aukščiausiasis Teismas, Švedija), nagrinėdamas *Bonnier Audio AB*, *Earbooks AB*, *Norstedts Förlagsgrupp AB, Piratförlaget AB* ir *Storyside AB* (toliau – *Bonnier Audio ir kt.*) ginčą su *Perfect Communication Sweden AB* (toliau – *ePhone*) dėl pastarosios prieštaravimo, pareikšto dėl *Bonnier Audio* ir kt. prašymo įpareigoti atskleisti duomenis, pateikė Teisingumo Teismui prašymą priimti prejudicinį sprendimą dėl direktyvų 2002/58 ir 2004/48 išaiškinimo.

Šioje byloje *Bonnier Audio ir kt*. buvo leidybos bendrovės, be kita ko, turinčios išimtines 27 kūrinių atgaminimo, leidybos ir viešojo platinimo įgarsintų knygų forma teises. Jos manė, kad buvo pažeistos išimtinės jų teisės, nes šie 27 kūriniai be jų sutikimo buvo viešai išplatinti per FTP („file transfer protocol“) serverį, leidžiantį keistis rinkmenomis ir perduoti duomenis iš vieno prie interneto prijungto kompiuterio į kitą. Todėl jos kreipėsi į Švedijos teismus su prašymu įpareigoti atskleisti asmens, naudojančio IP adresą, iš kurio, kaip preziumuojama, buvo siunčiamos atitinkamos rinkmenos, asmenvardį ir adresą.

Šiomis aplinkybėmis gavęs kasacinį skundą *Högsta domstolen* pateikė Teisingumo Teismui klausimą, ar Sąjungos teisė draudžia taikyti remiantis Direktyvos 2004/48 8 straipsniu priimtą nacionalinės teisės nuostatą, pagal kurią, siekiant identifikuoti interneto abonentą, civiliniame procese leidžiama įpareigoti interneto prieigos paslaugų teikėją atskleisti autorių teisių savininkui ar jo atstovui abonento, turinčio IP adresą, kuriuo naudojantis buvo tariamai pažeistos minėtos teisės, tapatybę. Buvo preziumuojama, pirma, kad prašymą nustatyti įpareigojimą pateikęs asmuo pateikė faktinių įrodymų, kad buvo pažeistos autorių teisės, ir, antra, kad prašoma priemonė yra proporcinga.

Teisingumo Teismas visų pirma priminė, kad Direktyvos 2004/48 8 straipsnio 3 dalis, siejama su Direktyvos 2002/58 15 straipsnio 1 dalimi, valstybėms narėms nedraudžia įtvirtinti pareigos perduoti asmens duomenis privatiems asmenims, kad civilines bylas nagrinėjančiuose teismuose būtų galima iškelti bylą už autorių teisių pažeidimus, tačiau pagal ją valstybės narės neįpareigojamos numatyti tokios pareigos. Vis dėlto valstybių narių valdžios institucijos ir teismai privalo ne tik aiškinti savo nacionalinę teisę taip, kad ji atitiktų šias direktyvas, bet ir nesivadovauti tokiu jų aiškinimu, kuris pažeistų minėtas pagrindines teises arba kitus bendruosius Sąjungos teisės principus, kaip antai proporcingumo principą (55 ir 56 punktai).

Šiuo aspektu jis konstatavo, kad pagal atitinkamą nacionalinės teisės aktą, be kita ko, reikalaujama, jog tam, kad būtų galima nustatyti įpareigojimą atskleisti aptariamus duomenis, turi egzistuoti faktiniai pažeistos intelektinės nuosavybės teisės į kūrinį įrodymai, prašoma informacija turi palengvinti autorių teisių pažeidimo ar tokių teisių suvaržymo tyrimą, o šį įpareigojimą pagrindžiančios priežastys turi nusverti nepatogumus ar kitą žalą, kurią toks įpareigojimas gali sukelti adresatui arba bet kuriam priešingam interesui (58 punktas).

Taigi Teisingumo Teismas priėjo prie išvados, kad direktyvomis 2002/58 ir 2004/48 nedraudžiamas nacionalinės teisės aktas, kaip antai nagrinėtas pagrindinėje byloje, kiek juo nacionaliniam teismui, į kurį galintis pareikšti ieškinį asmuo kreipiasi su prašymu įpareigoti atskleisti asmens duomenis, suteikiama galimybė atsižvelgiant į kiekvieno atvejo aplinkybes ir tinkamai laikantis iš proporcingumo principo kylančių reikalavimų pasverti turimus priešingus interesus (61 punktas ir rezoliucinė dalis).

2021 m. birželio 17 d. Sprendimas „M.I.C.M.“ (C-597/19, EU:C:2021:492)

Įmonė *Mircom International Content Management & Consulting (M.I.C.M.) Limited* (toliau – *Mircom*) *Ondernemingsrechtbank Antwerpen* (Antverpeno komercinių bylų teismas, Belgija, toliau – prašymą priimti prejudicinį sprendimą pateikęs teismas) pateikė interneto prieigos teikėjai *Telenet BVBA* prašymą suteikti informacijos. Šiuo prašymu siekiama, kad būtų priimtas sprendimas, įpareigojantis *Telenet* pateikti savo klientų tapatybės duomenis, remiantis IP adresais, kuriuos įmonei *Mircom* surinko specializuota įmonė. *Telenet* klientų interneto ryšys buvo naudojamas *BitTorrent* protokolo pagalba lygiarangių (*peer-to-peer*) tinkle dalijantis filmais iš *Mircom* katologo. *Telenet* nesutinka su *Mircom* prašymu.

Šiomis aplinkybėmis prašymą priimti prejudicinį sprendimą pateikęs teismas pirmiausia Teisingumo Teismo klausė, ar failo, kuriame yra saugomas kūrinys, dalių pasidalijimas minėtame tinkle yra viešas paskelbimas pagal Sąjungos teisę. Be to, jis siekė sužinoti, ar intelektinės nuosavybės teisių turėtojas, kaip antai *Mircom*, kuris šių teisių nenaudoja, tačiau iš tariamų pažeidėjų reikalauja atlyginti žalą, gali pasinaudoti Sąjungos teisėje numatytomis priemonėmis, procedūromis ir gynybos būdais, kad užtikrintų šių teisių apsaugą, pavyzdžiui, paprašydamas suteikti informaciją. Galiausiai prašymą priimti prejudicinį sprendimą pateikęs teismas paprašė Teisingumo Teismo išaiškinti, ar būdas, kuriuo *Mircom* rinko klientų IP adresus, ir duomenų atskleidimas, kurio ji prašo iš *Telenet*, yra teisėti.

Teisingumo Teismas nusprendė, kad pagal Sąjungos teisę[64] iš principo nedraudžiama nei intelektinės nuosavybės teisių turėtojui ar trečiajam asmeniui, veikiančiam jo vardu, sistemingai įrašyti lygiarangių (*peer-to-peer*) tinklų naudotojų IP adresus, kurių interneto ryšys tariamai buvo naudojamas teises pažeidžiančioje veikloje (išankstinis asmens duomenų tvarkymas), nei atskleisti naudotojų pavardes ir pašto adresus šiam teisių turėtojui ar trečiajam asmeniui, kad jie galėtų pareikšti ieškinį dėl žalos atlyginimo (vėlesnis asmens duomenų tvarkymas). Vis dėlto tokios iniciatyvos ir prašymai turi būti pagrįsti, proporcingi, jais neturi būti piktnaudžiaujama ir jie turi būti numatyti nacionalinėje teisėkūros priemonėje, kuria ribojama iš Sąjungos teisės kylančių teisių ir pareigų apimtis. Teisingumo Teismas pažymėjo, kad Sąjungos teisėje tokiai įmonei, kaip *Telenet*, nėra nustatyta pareigos atskleisti privatiems asmenims asmens duomenis tam, kad civiliniuose teismuose būtų galima pradėti teismo procesą dėl autorių teisių pažeidimų. Vis dėlto Sąjungos teisė leidžia valstybėms narėms nustatyti tokią pareigą (97, 125–127 punktai ir rezoliucinės dalies 3 punktas).

3. Asmens duomenų pašalinimas

2019 m. rugsėjo 24 d. didžiosios kolegijos Sprendimas „GC ir kt.“ (Nuorodų į jautrius duomenis pašalinimas) (C-136/17, ECLI:EU:C:2019:773)[65]

Šiame sprendime Teisingumo Teismas, posėdžiaudamas didžiojoje kolegijoje, patikslino paieškos sistemos eksploatuotojo pareigas, susijusias su prašymu pašalinti nuorodas, turinčias jautrių duomenų.

---

64 BDAR 6 straipsnio 1 dalies f punktas ir Direktyvos 2002/58 15 straipsnio 1 dalis.

65 Šis sprendimas pristatytas 2019 m. metiniame pranešime, p. 117 ir 118.

Google netenkino keturių asmenų prašymų iš rezultatų sąrašo, paieškos sistemoje rodomo atlikus paiešką pagal jų asmenvardžius, pašalinti įvairias nuorodas į trečiųjų asmenų skelbiamus tinklalapius, be kita ko, į spaudos straipsnius. Gavusi šių keturių asmenų skundus *Commission nationale de l'informatique et des libertés* (Nacionalinė informatikos ir laisvių komisija, CNIL, Prancūzija) atsisakė nurodyti *Google* pašalinti prašomas nuorodas. Bylą nagrinėjanti *Conseil d'État* (Valstybės Taryba, Prancūzija) kreipėsi į Teisingumo Teismą su prašymu patikslinti pagal Direktyvą 95/46 paieškos sistemos eksploatuotojui tenkančias pareigas nagrinėjant prašymą pašalinti nuorodas.

Pirma, Teisingumo Teismas priminė, kad, išskyrus tam tikras išimtis ir nukrypti leidžiančias nuostatas, draudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti sveikatos duomenis ir duomenis apie lytinį gyvenimą[66]. Kiek tai susiję su duomenų apie nusikalstamas veikas, apkaltinamuosius nuosprendžius arba kardomąsias priemones tvarkymu, tokius duomenis iš principo galima tvarkyti tik prižiūrint valdžios institucijai arba jeigu nacionalinėje teisėje yra numatytos tinkamos ir specialios apsaugos priemonės[67] (39 ir 40 punktai).

Teisingumo Teismas nusprendė, kad draudimas ar apribojimai, susiję su šių specialių kategorijų asmens duomenų tvarkymu, taikomi paieškos sistemos eksploatuotojui, kaip ir visiems kitiems asmens duomenų valdytojams. Šiais draudimais ir apribojimais siekiama užtikrinti didesnę apsaugą nuo tokių duomenų tvarkymo, kuris dėl ypatingo minėtų duomenų jautrumo gali itin stipriai suvaržyti pagrindines teises į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą (42–44 punktai).

Vis dėlto paieškos sistemos eksploatuotojas yra atsakingas ne dėl to, kad asmens duomenys nurodyti trečiųjų asmenų paskelbtame tinklalapyje, o dėl nuorodos į šį puslapį teikimo. Tokiomis aplinkybėmis jautrių duomenų tvarkymo draudimas ir apribojimai šiam eksploatuotojui taikomi tik dėl nuorodos teikimo, todėl įgyvendinami pagal duomenų subjekto pateiktą prašymą atliekant patikrinimą, prižiūrimą kompetentingų nacionalinių institucijų (46 ir 47 punktai).

Antra, Teisingumo Teismas laikėsi nuomonės, kad tais atvejais, kai eksploatuotojas gauna prašymą panaikinti nuorodas, susijusias su jautriais duomenimis, jis iš esmės privalo, išskyrus tam tikras išimtis, tokį prašymą patenkinti. Dėl šių išimčių pasakytina, kad eksploatuotojas gali, be kita ko, netenkinti tokio prašymo, kai konstatuoja, jog nuorodos nukreipia į duomenų subjekto akivaizdžiai paviešintus duomenis[68], jeigu tokių nuorodų teikimas atitinka kitas asmens duomenų tvarkymo teisėtumo sąlygas, nebent šis asmuo dėl priežasčių, susijusių su jo konkrečia padėtimi, turi teisę prieštarauti minėtam nuorodų teikimui[69] (65 ir 69 punktai).

Bet kuriuo atveju, gavęs prašymą pašalinti nuorodą, paieškos sistemos eksploatuotojas turi patikrinti, ar nuorodos į tinklalapį, kuriame paskelbti jautrūs duomenys, įtraukimas į rezultatų sąrašą, rodomą atlikus paiešką pagal to asmens asmenvardį, yra neišvengiamai būtinas siekiant apsaugoti internautų, potencialiai suinteresuotų atlikus tokią paiešką gauti prieigą prie šio tinklalapio, informacijos laisvę. Šiuo klausimu Teisingumo Teismas pabrėžė, kad nors teisė į

66 Direktyvos 95/46 8 straipsnio 1 dalis ir Reglamento 2016/679 9 straipsnio 1 dalis.
67 Direktyvos 95/46 8 straipsnio 5 dalis ir Reglamento 2016/679 10 straipsnis.
68 Direktyvos 95/46 8 straipsnio 2 dalies e punktas ir Reglamento 2016/679 9 straipsnio 2 dalies e punktas.
69 Direktyvos 95/46 14 straipsnio pirmos pastraipos a punktas ir Reglamento 2016/679 21 straipsnio 1 dalis.

privataus gyvenimo gerbimą ir teisė į asmens duomenų apsaugą paprastai yra viršesnės už internautų informacijos laisvę, vis dėlto ši pusiausvyra tam tikrais atvejais gali priklausyti nuo atitinkamos informacijos pobūdžio ir jos jautrumo, galinčio turėti įtakos duomenų subjekto privačiam gyvenimui, taip pat nuo visuomenės intereso susipažinti su šia informacija, kuris gali skirtis, nelygu šio asmens vaidmuo viešajame gyvenime (66 ir 68 punktai).

Trečia, Teisingumo Teismas nusprendė, kad gavęs prašymą pašalinti nuorodą į duomenis apie baudžiamąjį teismo procesą prieš duomenų subjektą, susijusius su ankstesniu šio proceso etapu ir nebeatitinkančius tikrosios padėties, paieškos sistemos eksploatuotojas, atsižvelgdamas į visas konkretaus atvejo aplinkybes, privalo įvertinti, ar minėtas asmuo turi teisę reikalauti, kad atitinkama informacija šiuo metu nebebūtų siejama su jo asmenvardžiu rezultatų sąraše, rodomame atlikus paiešką pagal jo asmenvardį. Tačiau net jeigu taip nėra dėl to, kad atitinkamos nuorodos įtraukimas yra neišvengiamai būtinas siekiant suderinti teisę į duomenų subjekto privataus gyvenimo gerbimą ir teisę į asmens duomenų apsaugą su potencialiai suinteresuotų internautų informacijos laisve, eksploatuotojas privalo ne vėliau kaip gavęs prašymą pašalinti nuorodą pakeisti rezultatų sąrašą taip, kad pagal jį sudarytas bendras vaizdas internautui parodytų aktualią teisminę padėtį, o tam reikia, be kita ko, kad nuorodos į tinklalapius su informacija tuo klausimu atsirastų pirmoje šio sąrašo vietoje (77 ir 78 punktai).

2019 m. rugsėjo 24 d. didžiosios kolegijos Sprendimas „Google“ (Nuorodų pašalinimo teritorinė taikymo sritis) (C-507/17, ECLI:EU:C:2019:772)[70]

Commission nationale de l'informatique et des libertés (Nacionalinė informatikos ir laisvių komisija, CNIL, Prancūzija) *Google* oficialiai įspėjo, kad tenkindama prašymą pašalinti nuorodas ši bendrovė iš rezultatų sąrašo, rodomo atlikus paiešką pagal duomenų subjekto asmenvardį, turi ištrinti nuorodas į tinklalapius, kuriuose pateikiami su šiuo asmeniu susiję asmens duomenys, iš visų savo paieškos sistemos domeno vardo plėtinių. *Google* atsisakius atsižvelgti į šį oficialų įspėjimą, CNIL skyrė šiai bendrovei 100 000 EUR baudą. *Conseil d'État* (Valstybės Taryba), į kurią kreipėsi *Google*, Teisingumo Teismo paprašė patikslinti paieškos sistemos eksploatuotojo pareigos pagal Direktyvą 95/46 įgyvendinti teisę reikalauti pašalinti nuorodas teritorinę apimtį.

Visų pirma Teisingumo Teismas priminė, kad pagal Sąjungos teisę fiziniai asmenys gali remtis savo teise reikalauti pašalinti nuorodas prieš paieškos sistemos eksploatuotoją, turintį vieną ar kelis padalinius Sąjungos teritorijoje, nepaisant to, ar asmens duomenys tvarkomi (konkrečiu atveju teikiamos nuorodos į tinklalapius, kuriuose yra su asmeniu, besiremiančiu tokia teise, susijusių asmens duomenų) Sąjungoje, ar už jos ribų[71].

Kiek tai susiję su teisės reikalauti pašalinti nuorodas apimtimi, Teisingumo Teismas nusprendė, kad paieškos sistemos eksploatuotojas turi pašalinti nuorodas ne iš visų savo sistemos versijų, o tik iš tų, kurios apima visas valstybes nares. Šiuo klausimu jis nurodė, kad nors universalus nuorodų pašalinimas, atsižvelgiant į interneto ir paieškos sistemų charakteristikas, galėtų visiškai atitikti Sąjungos teisės aktų leidėjo tikslą užtikrinti aukštą asmens duomenų apsaugos lygį visoje Sąjungoje, iš Sąjungos teisės[72] visiškai nematyti, kad siekdamas įgyvendinti šį tikslą teisės aktų

[70] Šis sprendimas pristatytas 2019 m. metiniame pranešime, p. 118 ir 119.
[71] Direktyvos 95/46 4 straipsnio 1 dalies a punktas ir Reglamento 2016/679 3 straipsnio 1 dalis.
[72] Direktyvos 95/46 12 straipsnio b punktas ir 14 straipsnio pirmos pastraipos a punktas ir Reglamento 2016/679 17 straipsnio 1 dalis.

leidėjas būtų suteikęs teisei reikalauti pašalinti nuorodas apimtį, kuri išeitų už valstybių narių teritorijos ribų. Konkrečiai kalbant, nors Sąjungos teisėje nustatytas valstybių narių priežiūros institucijų bendradarbiavimo mechanizmas, leidžiantis priimti bendrą sprendimą, kuris būtų grindžiamas teisės į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą bei įvairių valstybių narių visuomenės intereso turėti prieigą prie informacijos pusiausvyra, šiuo metu tokio mechanizmo, kiek tai susiję su nuorodų pašalinimo už Sąjungos ribų apimtimi, nenumatyta (62 ir 73 punktai).

Pagal šiuo metų galiojančią Sąjungos teisę paieškos sistemos eksploatuotojas turi pašalinti prašyme nurodytas nuorodas ne tik iš vienos paieškos sistemos versijos, kuri apima asmens, dėl kurio atliekamas toks pašalinimas, gyvenamosios vietos valstybę narę, bet ir iš paieškos sistemos versijų, kurios apima valstybes nares, būtent tam, kad būtų užtikrintas vienodas ir aukštas apsaugos lygis visoje Sąjungoje. Be to, jei reikia, toks eksploatuotojas turi imtis pakankamai veiksmingų priemonių, kad Sąjungos interneto vartotojams būtų užkirstas kelias arba bent jau jie būtų labai atgrasyti turėti prieigą atitinkamais atvejais iš paieškos sistemos versijos, kuri apima trečiąją valstybę, prie nuorodų, kurias prašoma pašalinti, o nacionalinis teismas turi patikrinti, ar eksploatuotojo nustatytos priemonės tenkina šį reikalavimą (70 punktas).

Galiausiai Teisingumo Teismas pabrėžė, kad nors pagal Sąjungos teisę nereikalaujama, kad paieškos sistemos eksploatuotojas pašalintų nuorodas iš visų savo paieškos sistemos versijų, tai nėra draudžiama. Taigi, valstybės narės priežiūros arba teisminė institucija išlaiko kompetenciją, atsižvelgdama į nacionalinius pagrindinių teisių apsaugos standartus, nustatyti pusiausvyrą tarp, viena vertus, duomenų subjekto teisės į privataus gyvenimo gerbimą ir į jo asmens duomenų apsaugą ir, kita vertus, teisės į informacijos laisvę, ir tai atlikdama prireikus nurodyti tokios paieškos sistemos eksploatuotojui pašalinti nuorodas iš visų tokios sistemos versijų (65 ir 72 punktai).

4. Interneto svetainės naudotojo sutikimas saugoti informaciją arba suteikti prieigą prie informacijos naudojant slapukus

2019 m. spalio 1 d. didžiosios kolegijos Sprendimas „Planet49" (C-673/17, ECLI:EU:C:2019:801)[73]

Tame sprendime Teisingumo Teismas nusprendė, kad sutikimas saugoti informaciją arba suteikti prieigą prie jos naudojant slapukus, įrengtus interneto svetainės naudotojo galiniame įrenginyje, nėra tinkamai duotas, kai leidimą lemia iš anksto pažymėtas langelis, neatsižvelgiant į tai, ar nagrinėjama informacija yra asmens duomenys, ar ne. Be to, Teisingumo Teismas pažymėjo, kad paslaugų teikėjas interneto svetainės naudotojui turi nurodyti slapukų veikimo trukmę ir informuoti apie galimybę (arba ne) tretiesiems asmenims turėti prieigą prie šių slapukų.

Ginčas pagrindinėje byloje susijęs su *Planet49* organizuota loterija interneto svetainėje www.dein-macbook.de. Kad galėtų joje dalyvauti, interneto vartotojai turėjo nurodyti savo pavardę ir adresą interneto puslapyje, kuriame buvo žymimieji langeliai. Langelis, pagal kurį leidžiama įdiegti slapukus, buvo pažymėtas iš anksto. Gavęs Vokietijos vartotojų asociacijų federacijos skundą *Bundesgerichtshof* (Aukščiausiasis Federalinis Teismas, Vokietija) suabejojo dėl naudotojų sutikimo, gauto panaudojant iš anksto pažymėtą langelį, galiojimo ir dėl paslaugos teikėjui tenkančios pareigos suteikti informaciją apimties.

Prašymas priimti prejudicinį sprendimą iš esmės buvo susijęs su Direktyvoje 2002/58[74], siejamoje su Direktyva 95/46[75] ir BDAR[76], vartojamos sąvokos „sutikimas" aiškinimu.

Pirma, Teisingumo Teismas pažymėjo, kad Direktyvos 95/46 2 straipsnio h punkte, į kurį daroma nuoroda Direktyvos 2002/58 2 straipsnio f punkte, sutikimas apibrėžiamas kaip reiškiantis „bet kurį savanoriškai ir žinomai duotą konkretų duomenų subjekto pareiškimą [valios pareiškimą], kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję [jo asmens] duomenys". Jis nurodė, kad reikalavimas dėl duomenų subjekto valios „pareiškimo" akivaizdžiai reiškia aktyvius, o ne pasyvius veiksmus. Reikia pažymėti, kad sutikimas, duotas pasitelkiant iš anksto pažymėtą žymimąjį langelį, neapima aktyvių interneto svetainės naudotojo veiksmų. Be to, Direktyvos 2002/58 5 straipsnio 3 dalies, kurioje po pakeitimų, padarytų Direktyva 2009/136, numatyta, kad naudotojas turi būti davęs „sutikimą" įdiegti slapukus, genezė rodo, kad nuo šiol naudotojo sutikimas negali būti preziumuojamas ir turi kilti iš aktyvaus jo elgesio. Galiausiai nuo šiol aktyvus sutikimas yra numatytas BDAR[77], kurio 4 straipsnio 11 punkte reikalaujamas valios pareiškimas, be kita ko, „vienareikšmiais veiksmais", o jo 32 konstatuojamojoje dalyje aiškiai nurodyta, kad sutikimu negali būti laikoma „tyla, iš anksto pažymėti langeliai arba neveikimas" (49, 52, 56 ir 62 punktai).

Taigi Teisingumo Teismas nusprendė, kad nėra duotas galiojantis sutikimas, kai išsaugoti informaciją arba prieiti prie informacijos, saugomos interneto svetainės naudotojo galiniame įrenginyje, leidžiama pagal iš anksto pažymėtą žymimąjį langelį, kurio žymėjimą naudotojas turi

---

73 Šis sprendimas pristatytas 2019 m. metiniame pranešime, p. 120 ir 121.

74 Direktyvos 2002/58, iš dalies pakeistos 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136 (OL L 337, 2009, p. 11), 2 straipsnio f punktas ir 5 straipsnio 3 dalis.

75 Direktyvos 95/46 2 straipsnio h punktas.

76 Reglamento 2016/679 6 straipsnio 1 dalies a punktas.

77 Ten pat.

pašalinti, jei nori atsisakyti duoti sutikimą. Jis pridūrė, jog tai, kad naudotojas aktyvuoja dalyvavimo nurodytoje loterijoje mygtuką, negali pakakti, kad būtų galima manyti, kad jis davė galiojantį sutikimą įdiegti slapukus (63 punktas).

Antra, Teisingumo Teismas konstatavo, kad Direktyvos 2002/58 5 straipsnio 3 dalimi naudotoją siekiama apsaugoti nuo bet kokio kišimosi į jo privatų gyvenimą, neatsižvelgiant į tai, ar šis kišimasis susijęs su asmens duomenimis, ar ne. Vadinasi, sutikimo sąvoka neturi būti aiškinama skirtingai, atsižvelgiant į tai, ar interneto svetainės naudotojo galiniame įrenginyje saugoma arba naudojama informacija yra (arba nėra) asmens duomenys (69 ir 71 punktai).

Trečia, Teisingumo Teismas pažymėjo, kad pagal Direktyvos 2002/58 5 straipsnio 3 dalį reikalaujama, kad naudotojas būtų davęs sutikimą, pateikus jam aiškią ir išsamią informaciją, visų pirma apie tvarkymo tikslus. Aiški ir išsami informacija turi leisti naudotojui lengvai nustatyti savo duodamo sutikimo pasekmes ir užtikrinti, kad šis sutikimas būtų duotas žinant visas aplinkybes. Šiuo klausimu Teisingumo Teismas nusprendė, kad slapukų veikimo trukmė ir galimybė (arba ne) tretiesiems asmenims turėti prieigą prie šių slapukų, yra dalis aiškios ir detalios informacijos, kurią paslaugų teikėjas turi pateikti interneto svetainės naudotojui (73–75 ir 81 punktai).

VI. Nacionalinės priežiūros institucijos

1. Nepriklausomumo reikalavimo apimtis

2010 m. kovo 9 d. didžiosios kolegijos Sprendimas „Komisija / Vokietija“ (C-518/07, ECLI:EU:C:2010:125)[78]

Savo ieškiniu Komisija Teisingumo Teismo prašė konstatuoti, kad taikydama priežiūros institucijų, kompetentingų prižiūrėti asmens duomenų tvarkymą ne viešajame sektoriuje įvairiose žemėse (*Länder*), valstybės kontrolę ir dėl to neteisingai perkėlusi reikalavimą, pagal kurį institucijos, įpareigotos užtikrinti šių duomenų apsaugą, turi būti „visiškai nepriklausomos“, Vokietijos Federacinė Respublika neįvykdė įsipareigojimų pagal Direktyvos 95/46 28 straipsnio 1 dalies antrą pastraipą.

Vokietijos Federacinė Respublika savo ruožtu teigė, kad pagal Direktyvos 95/46 28 straipsnio 1 dalies antrą pastraipą reikalaujama, kad priežiūros institucijos vykdytų funkcijas nepriklausomai, t. y. kad šios institucijos būtų nepriklausomos nuo jų kontroliuojamo ne viešojo sektoriaus ir kad joms nebūtų daroma išorinė įtaka. Jos nuomone, Vokietijos žemėse (*Länder*) vykdoma valstybės kontrolė buvo ne tokia išorinė įtaka, o administracijos vidaus priežiūros mechanizmas, įgyvendinamas institucijų, susijusių su tuo pačiu kaip ir priežiūros institucijos administraciniu aparatu ir, kaip ir pastarosios, privalančių įgyvendinti Direktyvos 95/46 tikslus.

Teisingumo Teismas nusprendė, kad nacionalinių priežiūros institucijų nepriklausomumo garantija, numatyta Direktyvoje 95/46, siekiama užtikrinti veiksmingą ir patikimą nuostatų,

[78] Šis sprendimas pristatytas 2010 m. metiniame pranešime, p. 34.

susijusių su fizinių asmenų apsauga tvarkant asmens duomenis, laikymosi kontrolę ir ji turi būti aiškinama atsižvelgiant į šį tikslą. Ji buvo numatyta ne tam, kad šioms institucijoms ir jų tarnautojams būtų suteiktas ypatingas statusas, o tam, kad būtų sustiprinta su jų sprendimais susijusių asmenų ir organizacijų apsauga, todėl vykdydamos savo funkcijas priežiūros institucijos turi veikti objektyviai ir nešališkai (25 punktas).

Teisingumo Teismas manė, kad šios priežiūros institucijos, įpareigotos prižiūrėti, kaip ne viešajame sektoriuje tvarkomi asmens duomenys, turi veikti nepriklausomai, t. y. vykdyti savo funkcijas be išorinės įtakos. Šis nepriklausomumas reiškia ne tik tai, kad jų prižiūrimos organizacijos nedaro joms jokios įtakos, bet ir tai, kad nėra jokių nurodymų ir kitos išorinės – tiesioginės ar netiesioginės – įtakos, galinčios sutrukdyti minėtoms institucijoms vykdyti jų užduotį, t. y. nustatyti teisingą pusiausvyrą tarp teisės į privatų gyvenimą apsaugos ir laisvo asmens duomenų judėjimo. Vien to, jog kontrolės institucijos gali daryti politinę įtaką kompetentingų priežiūros institucijų sprendimams, pakanka, kad būtų pakenkta tų funkcijų nepriklausomam vykdymui. Viena vertus, kontrolės institucijų sprendimų priėmimo praktika gali lemti priežiūros institucijų „išankstinį paklusnumą“. Kita vertus, šių priežiūros institucijų prisiimtas teisės į privataus gyvenimą saugotojų vaidmuo reikalauja, kad nei jų sprendimai, taigi, nei jos pačios, nebūtų šališki. Todėl, anot Teisingumo Teismo, nacionalinių priežiūros institucijų atžvilgiu vykdoma valstybės kontrolė nėra suderinama su nepriklausomumo reikalavimu (30, 36, 37 punktai ir rezoliucinė dalis).

2012 m. spalio 16 d. didžiosios kolegijos Sprendimas „Komisija / Austrija“ (C-614/10, EU:C:2012:631)

Savo ieškiniu Komisija Teisingumo Teismo prašė konstatuoti, jog nepriėmusi visų nuostatų, kurių reikia, kad Austrijoje galiojančiais teisės aktais būtų tenkinamas asmens duomenų apsaugos priežiūrai įsteigtos *Datenschutzkommission* (Duomenų apsaugos komisija) nepriklausomumo kriterijus, Austrija neįvykdė įsipareigojimų pagal Direktyvos 95/46 28 straipsnio 1 dalies antrą pastraipą.

Teisingumo Teismas konstatavo, jog Austrija neįvykdė įsipareigojimų, iš esmės laikydamasis nuomonės, kad Direktyvoje 95/46 nustatyto priežiūros institucijos nepriklausomumo kriterijaus neįvykdo valstybė narė, kuri priima teisės aktus, pagal kuriuos šios institucijos valdantysis narys yra valstybės tarnautojas, kuriam taikoma tarnybinė priežiūra, jo biuras integruotas į nacionalinės vyriausybės tarnybas, o valstybės vyriausybės vadovas turi besąlyginę teisę gauti informaciją apie visus šios institucijos valdymo aspektus (66 punktas ir rezoliucinė dalis).

Teisingumo Teismas visų pirma priminė, kad Direktyvos 95/46 28 straipsnio 1 dalies antroje pastraipoje vartojami žodžiai „visiškai nepriklausomai“ reiškia, kad priežiūros institucijos turi turėti tiek nepriklausomybės, kad galėtų vykdyti joms pavestas užduotis be išorinės įtakos. Šiuo aspektu vien to, kad tokia institucija turi funkcinį nepriklausomumą, nes jos nariai yra nepriklausomi ir vykdydami pareigas nėra varžomi jokių nurodymų, nepakanka, kad priežiūros institucija būtų apsaugota nuo bet kokios išorės įtakos. Reikalaujamu nepriklausomumu siekiama užkirsti kelią ne tik tiesioginei įtakai, daromai teikiant nurodymus, bet ir bet kokios formos netiesioginei įtakai, kuri gali pakreipti priežiūros institucijos sprendimus kuria nors linkme. Be to, dėl priežiūros institucijoms tenkančio teisės į privataus gyvenimą saugotojų vaidmens jų sprendimai, taigi, ir pačios institucijos, neturi kelti jokių įtarimų dėl šališkumo (41–43 ir 52 punktai).

Teisingumo Teismas pažymėjo, kad nebūtina numatyti atskiros nacionalinei priežiūros institucijai skirtos biudžeto eilutės, kaip tai padaryta Reglamento (EB) Nr. 45/2001 43 straipsnio 3 dalyje, kad būtų įvykdytas Direktyvos 95/46 minėtoje nuostatoje numatytas nepriklausomumo kriterijus. Iš tiesų valstybės narės neprivalo savo nacionalinėje teisėje numatyti Reglamento (EB) Nr. 45/2001 V skyriaus nuostatoms analogiškų nuostatų, kad užtikrintų visišką jų priežiūros institucijos (-ų) nepriklausomumą, taigi gali numatyti, kad, biudžeto teisės požiūriu, priežiūros institucija priklauso atitinkamam ministerijos padaliniui. Tačiau reikiamų žmogiškųjų ir materialinių išteklių suteikimas tokiai institucijai neturi užkirsti kelio vykdyti jai pavestas užduotis „visiškai nepriklausomai“, kaip tai suprantama pagal Direktyvos 95/46 28 straipsnio 1 dalies antrą pastraipą (58 punktas).

2014 m. balandžio 8 d. didžiosios kolegijos Sprendimas „Komisija / Vengrija“ (C-288/12, EU:C:2014:237)[79]

Šioje byloje Komisija Teisingumo Teismo prašė konstatuoti, kad pirma laiko nutraukusi asmens duomenų apsaugos priežiūros institucijos kadenciją Vengrija neįvykdė įsipareigojimų pagal Direktyvą 95/46.

Teisingumo Teismas nusprendė, kad įsipareigojimų pagal Direktyvą 95/46 neįvykdo ta valstybė narė, kuri pirma laiko nutraukia asmens duomenų apsaugos priežiūros institucijos veiklos laikotarpį (62 punktas ir rezoliucinės dalies 1 punktas).

Anot Teisingumo Teismo, nepriklausomumas, kurį turi turėti priežiūros institucijos, kompetentingos kontroliuoti šių duomenų tvarkymą, be kita ko, reiškia, kad šios institucijos turi būti apsaugotos nuo bet kokios 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 (51 punktas).

Be to, Teisingumo Teismas priminė: kadangi vien tokio funkcinio nepriklausomumo nepakanka, kad priežiūros institucijos būtų apsaugotos nuo bet kokios išorinės įtakos, vien to, jog valstybės kontrolės institucijos gali daryti politinę įtaką priežiūros institucijų sprendimams, pakanka, kad būtų pakenkta nepriklausomam tų funkcijų vykdymui. Jei visoms valstybėms narėms būtų leidžiama nutraukti priežiūros institucijos kadenciją nepasibaigus iš pradžių numatytam terminui, nepaisant taikytinuose teisės aktuose šiuo atžvilgiu iš anksto nustatytų garantijų, tokio pirmalaikio nutraukimo pavojus, kuris šios institucijos atžvilgiu egzistuotų visą jos kadencijos laikotarpį, galėtų lemti jos tam tikros formos paklusnumą politinei valdžiai, nesuderinamą su minėtu nepriklausomumo reikalavimu. Be to, esant tokiai situacijai, priežiūros institucija negalėtų būti laikoma galinčia bet kokiomis aplinkybėmis veikti ir nekelti jokių įtarimų dėl šališkumo (52–55 punktai).

2. Taikytinos teisės ir kompetentingos priežiūros institucijos nustatymas

[79] Šis sprendimas pristatytas 2014 m. metiniame pranešime, p. 62.

2015 m. spalio 1 d. Sprendimas „Weltimmo“ (C-230/14, EU:C:2015:639)[80]

Nemzeti Adatvédelmi és Információszabadság Hatóság (Nacionalinė institucija, atsakinga už duomenų apsaugą ir informacijos laisvę, Vengrija) skyrė baudą Slovakijoje įregistruotai bendrovei *Weltimmo*, eksploatuojančiai interneto tinklalapius, kuriuose talpinami skelbimai apie Vengrijoje esantį nekilnojamąjį turtą, motyvuodama tuo, kad ši bendrovė nepašalino šiuose tinklalapiuose skelbimus talpinančių asmenų asmens duomenų, nepaisant to, kad jie to prašė, ir perdavė šiuos duomenis skolų išieškojimo įmonėms tam, kad būtų apmokėtos sąskaitos, pagal kurias dar nėra sumokėta. Anot Vengrijos priežiūros institucijos, taip bendrovė *Weltimmo* pažeidė Vengrijos teisės aktą, kuriuo į vidaus teisę perkelta Direktyva 95/46.

Gavęs kasacinį skundą, *Kúria* (Aukščiausiasis Teismas, Vengrija) išreiškė abejonių dėl taikytinos teisės nustatymo ir dėl įgaliojimų, kuriuos Vengrijos priežiūros institucija turi pagal Direktyvos 95/46 4 straipsnio 1 dalį ir 28 straipsnį. Todėl jis pateikė Teisingumo Teismui kelis prejudicinius klausimus.

Dėl taikytinos nacionalinės teisės Teisingumo Teismas nusprendė, kad pagal Direktyvos 95/46 4 straipsnio 1 dalies a punktą leidžiama taikyti kitos nei ta, kur asmens duomenų valdytojas registruotas, valstybės narės teisės aktus dėl asmens duomenų apsaugos, jeigu šis valdytojas per nuolatinį padalinį tos valstybės narės teritorijoje veiksmingai ir realiai vykdo bent minimalią veiklą, kurios pagrindu atliekamas šis tvarkymas. Siekiant nustatyti, ar taip yra, prašymą priimti prejudicinį sprendimą pateikęs teismas, gali, be kita ko, atsižvelgti į tai, kad, pirma, duomenų valdytojo veikla, kurią vykdydamas jis tvarkė duomenis, yra eksploatuoti tos valstybės narės teritorijoje esančio nekilnojamojo turto skelbimų interneto tinklapius, kurie parengti tos valstybės kalba, todėl ji iš esmės ar net visiškai skirta minėtai valstybei narei. Antra, prašymą priimti prejudicinį sprendimą pateikęs teismas gali atsižvelgti į tai, kad šis duomenų valdytojas turi atstovą minėtoje valstybėje narėje, įgaliotą išieškoti iš šios veiklos kilusias skolas ir atstovauti jam per administracinį ir teismo procesus dėl atitinkamų duomenų tvarkymo. Tačiau Teisingumo Teismas pažymėjo, kad su šiuo duomenų tvarkymu susijusių asmenų pilietybė neturi reikšmės (41 punktas ir rezoliucinės dalies 1 punktas).

Kiek tai susiję su skundus nagrinėjančios priežiūros institucijos kompetencija ir įgaliojimais pagal Direktyvos 95/46 28 straipsnio 4 dalį, Teisingumo Teismas konstatavo, kad ši institucija gali nagrinėti šiuos skundus, nesvarbu, kokia teisė taikytina, taigi, netgi neišsiaiškinusi, kokia nacionalinė teisė turi būti taikoma tvarkant atitinkamus duomenis (54 punktas). Vis dėlto padariusi išvadą, kad taikytina kitos valstybės narės teisė, ji negali skirti sankcijų už savo valstybės narės teritorijos ribų. Esant tokiai situacijai, ji, vykdydama šios direktyvos 28 straipsnio 6 dalyje numatytą bendradarbiavimo pareigą, privalo prašyti šios kitos valstybės narės priežiūros institucijos konstatuoti šios teisės pažeidimą ir taikyti sankcijas, jeigu pagal ją galima tai daryti, remdamasi jai perduota informacija (57, 60 punktai ir rezoliucinės dalies 2 punktas).

3. Nacionalinių priežiūros institucijų įgaliojimai

[80] Šis sprendimas pristatytas 2015 m. metiniame pranešime, p. 55.

2015 m. spalio 6 d. didžiosios kolegijos Sprendimas „Schrems“ (C-362/14, EU:C:2015:650)

Šioje byloje (taip pat žr. IV skyrių „Asmens duomenų perdavimas į trečiąsias šalis“) Teisingumo Teismas, be kita ko, nusprendė, kad nacionalinės priežiūros institucijos turi kompetenciją vykdyti asmens duomenų perdavimo į trečiąsias šalis kontrolę.

Šiuo aspektu Teisingumo Teismas visų pirma konstatavo, kad nacionalinės priežiūros institucijos turi nemažai įgaliojimų ir šie įgaliojimai, kurių negalutinis sąrašas pateiktas Direktyvos 95/46 28 straipsnio 3 dalyje, yra būtinos priemonės, kad jos galėtų atlikti savo užduotis. Taigi minėtos institucijos, be kita ko, turi tyrimo įgaliojimus, pavyzdžiui, įgaliojimus rinkti bet kokią jų priežiūros funkcijai vykdyti būtiną informaciją, įgaliojimus imtis tokių veiksmingų intervencijos priemonių, koks yra laikinas ar galutinis draudimas tvarkyti duomenis, arba įgaliojimus kreiptis į teismą (43 punktas).

Dėl įgaliojimų vykdyti asmens duomenų perdavimo į trečiąsias šalis kontrolę Teisingumo Teismas nusprendė, kad iš Direktyvos 96/45 28 straipsnio 1 ir 6 dalių matyti, jog nacionalinių priežiūros institucijų įgaliojimai yra susiję su asmens duomenų tvarkymu tų institucijų valstybės narės teritorijoje, todėl remiantis šiuo 28 straipsniu jos neturi įgaliojimų, kai tokie duomenys tvarkomi trečiosios šalies teritorijoje (44 punktas).

Vis dėlto asmens duomenų perdavimo iš valstybės narės į trečiąją šalį operacija savaime yra asmens duomenų tvarkymas, atliekamas valstybės narės teritorijoje. Todėl, kadangi pagal Chartijos 8 straipsnio 3 dalį ir Direktyvos 95/46 28 straipsnį nacionalinės priežiūros institucijos įgaliotos kontroliuoti, kaip laikomasi Sąjungos taisyklių dėl fizinių asmenų apsaugos tvarkant asmens duomenis, kiekviena iš jų turi kompetenciją patikrinti, ar asmens duomenų perdavimas iš valstybės narės, kuriai ji priklauso, į trečiąją šalį atitinka šioje direktyvoje nustatytus reikalavimus (45 ir 47 punktai).

2018 m. birželio 5 d. didžiosios kolegijos Sprendimas „Wirtschaftsakademie Schleswig-Holstein“ (C-210/16, ECLI:EU:C:2018:388)

Šiame sprendime (taip pat žr. II.5 skyrių „Asmens duomenų valdytojas“), be kita ko, susijusiame su Direktyvos 95/46 4 ir 28 straipsnių išaiškinimu, Teisingumo Teismas pateikė poziciją dėl priežiūros institucijų įgaliojimų imtis veiksmų apimties, atsižvelgiant į asmens duomenų tvarkymą dalyvaujant keliems subjektams.

Taigi Teisingumo Teismas nusprendė, kad tuo atveju, kai įmonė, įsteigta už Sąjungos ribų (kaip antai JAV bendrovė *Facebook*), turi kelis padalinius skirtingose valstybėse narėse, valstybės narės priežiūros institucija gali naudotis jai pagal šios direktyvos 28 straipsnio 3 dalį suteiktais įgaliojimais dėl tos valstybės narės teritorijoje įsteigto šios įmonės padalinio (nagrinėtu atveju *Facebook Germany*), net jei, remiantis užduočių paskirstymu grupės viduje, pirma, šis padalinys yra atsakingas tik už reklamai skirtos vietos pardavimą ir kitą rinkodaros veiklą tos valstybės narės teritorijoje ir, antra, išimtinė atsakomybė už asmens duomenų rinkimą ir tvarkymą visoje Europos Sąjungos teritorijoje tenka kitoje valstybėje narėje įsteigtam padaliniui (nagrinėtu atveju *Facebook Ireland*) (64 punktas ir rezoliucinės dalies 2 punktas).

Teisingumo Teismas taip pat pažymėjo, kad kai vienos valstybės narės priežiūros institucija ketina dėl šios valstybės narės teritorijoje įsteigto subjekto įgyvendinti įgaliojimus imtis

priemonių, kurie nurodyti Direktyvos 95/46 28 straipsnio 3 dalyje, dėl asmens duomenų apsaugos taisyklių pažeidimų, kuriuos padarė už šių duomenų tvarkymą atsakingas trečiasis asmuo, turintis registruotą buveinę kitoje valstybėje narėje (nagrinėtu atveju *Facebook Ireland*), ši priežiūros institucija turi kompetenciją, nepriklausomai nuo kitos valstybės narės (Airijos) priežiūros institucijos, vertinti tokio duomenų tvarkymo teisėtumą ir gali įgyvendinti savo įgaliojimus imtis veiksmų dėl jos teritorijoje įsteigto subjekto, prieš tai nepaprašiusi tos kitos valstybės narės priežiūros institucijos imtis veiksmų (74 punktas ir rezoliucinės dalies 3 punktas).

2021 m. birželio 15 d. didžiosios kolegijos Sprendimas „Facebook Ireland ir kt.“ (C-645/19, EU:C:2021:483)

2015 m. rugsėjo 11 d. *Commission belge de la protection de la vie privée* (Belgijos privataus gyvenimo apsaugos komisija, toliau – PGAK) pirmininkas *Nederlandstalige rechtbank van eerste aanleg Brussel* (nyderlandų kalba bylas nagrinėjantis Briuselio pirmosios instancijos teismas, Belgija) pareiškė ieškinį *Facebook Ireland*, *Facebook Inc.* ir *Facebook Belgium*, siekdamas, kad būtų nutraukti *Facebook* tariamai daromi duomenų apsaugos teisės aktų pažeidimai. Šie pažeidimai pasireiškė visų pirma tuo, kad buvo renkama ir naudojama informacija apie Belgijos internautų, turinčių *Facebook* paskyrą ir jos neturinčių, naršymo elgesį, pasitelkiant įvairias technologijas, kaip antai slapukus, socialinius papildinius [81] ar pikselius.

2018 m. vasario 16 d. šis teismas pripažino savo jurisdikciją nagrinėti šį ieškinį ir iš esmės nusprendė, kad socialinis tinklas *Facebook* nepakankamai informavo Belgijos internautus apie atitinkamos informacijos rinkimą ir naudojimą. Be to, internautų sutikimas dėl minėtos informacijos rinkimo ir tvarkymo buvo pripažintas negaliojančiu.

2018 m. kovo 2 d. *Facebook Ireland*, *Facebook Inc.* ir *Facebook Belgium* apskundė šį sprendimą prašymą priimti prejudicinį sprendimą pateikusiame teisme – *Hof van beroep te Brussel* (Briuselio apeliacinis teismas, Belgija). Tame teisme vykstančiame procese *Autorité belge de protection des données* (Belgijos duomenų apsaugos institucija, toliau – DAI) dalyvavo kaip PGAK pirmininko teisių ir pareigų perėmėja. Prašymą priimti prejudicinį sprendimą pateikęs teismas pripažino savo jurisdikciją priimti sprendimą tik dėl *Facebook Belgium* pateikto apeliacinio skundo.

Prašymą priimti prejudicinį sprendimą pateikusiam teismui kilo abejonių dėl BDAR[82] numatyto vieno langelio mechanizmo taikymo poveikio DAI kompetencijai, konkrečiau kalbant, jis siekė išsiaiškinti, ar, kiek tai susiję su aplinkybėmis, susiklosčiusiomis po BDAR įsigaliojimo, t. y. po 2018 m. gegužės 25 d., DAI gali imtis veiksmų prieš *Facebook Belgium*, nors *Facebook Ireland* buvo pripažintas atitinkamų duomenų valdytoju. Vadovaujantis BDAR numatytu vieno langelio principu, nuo tos datos kompetenciją pareikšti ieškinį dėl veiksmų nutraukimo turi tik Airijos duomenų apsaugos komisaras, kuriam taikoma Airijos teismų kontrolė (36 ir 37 punktai).

Didžiosios kolegijos priimtame sprendime Teisingumo Teismas patikslino nacionalinių priežiūros institucijų įgaliojimus pagal BDAR. Jis, be kita ko, nusprendė, kad pagal šį reglamentą valstybės narės priežiūros institucijai tam tikromis sąlygomis leidžiama naudotis savo įgaliojimais dėl

---

81 Pavyzdžiui, mygtukus „Patinka“ arba „Bendrinti“.

82 BDAR 56 straipsnio 1 dalyje numatyta: „Nedarant poveikio 55 straipsniui, duomenų valdytojo arba duomenų tvarkytojo pagrindinės buveinės arba vienintelės buveinės priežiūros institucija turi kompetenciją veikti kaip vadovaujanti priežiūros institucija, kai tas duomenų valdytojas arba duomenų tvarkytojas vykdo tarpvalstybinį duomenų tvarkymą. <...>“

tariamų BDAR pažeidimų kreiptis į tos valstybės teismą ir pradėti teismo procesą dėl tarpvalstybinio duomenų tvarkymo[83], nors šio tvarkymo atveju ji nėra vadovaujanti institucija (rezoliucinės dalies 1 punktas).

Pirma, Teisingumo Teismas patikslino sąlygas, kuriomis nacionalinė priežiūros institucija, neturinti vadovaujančios institucijos statuso, tarpvalstybinio duomenų tvarkymo atveju privalo naudotis įgaliojimais dėl tariamų BDAR pažeidimų – kreiptis į valstybės narės teismą ir tam tikrais atvejais pradėti teismo procesą, kad būtų užtikrintas šio reglamento taikymas. Taigi, pirma, pagal BDAR šiai priežiūros institucijai turi būti suteikta kompetencija priimti sprendimą, kuriuo konstatuojama, kad toks duomenų tvarkymas pažeidžia šiame reglamente nustatytas taisykles, ir, antra, šiuo įgaliojimu turi būti naudojamasi laikantis minėtame reglamente numatytų bendradarbiavimo ir nuoseklumo užtikrinimo procedūrų[84] (75 punktas ir rezoliucinės dalies 1 punktas).

Tarpvalstybinio duomenų tvarkymo atveju BDAR numatytas vieno langelio mechanizmas[85], grindžiamas kompetencijos paskirstymu „vadovaujančiai priežiūros institucijai“ ir kitoms susijusioms nacionalinėms priežiūros institucijoms. Pagal šį mechanizmą reikalaujama, kad institucijos glaudžiai, lojaliai ir veiksmingai bendradarbiautų, siekdamos užtikrinti nuoseklią ir vienodą asmens duomenų apsaugos taisyklių apsaugą ir taip išlaikyti jo veiksmingumą. BDAR šiuo klausimu įtvirtinta principinė vadovaujančios priežiūros institucijos kompetencija priimti sprendimą, kuriuo konstatuojama, kad tarpvalstybinis duomenų tvarkymas pažeidžia šiame reglamente nustatytas taisykles[86], o kitų nacionalinių priežiūros institucijų kompetencija priimti tokį sprendimą, net ir laikiną, yra išimtis[87]. Vis dėlto vadovaujanti priežiūros institucija, naudodamasi kompetencija, negali nepalaikyti būtino dialogo ir lojalaus bei veiksmingo bendradarbiavimo su kitomis atitinkamomis priežiūros institucijomis. Todėl, vykstant šiam bendradarbiavimui, vadovaujanti priežiūros institucija negali neatsižvelgti į kitų susijusių priežiūros institucijų pozicijas, o dėl bet kokio tinkamo ir pagrįsto vienos iš šių institucijų pateikto prieštaravimo bent jau laikinai gali būti blokuojamas vadovaujančios priežiūros institucijos sprendimo projekto priėmimas (50–53, 5–59 ir 63–65 punktai).

Be to, kaip patikslino Teisingumo Teismas, aplinkybė, kad valstybės narės priežiūros institucija, kuri nėra vadovaujanti priežiūros institucija, tarpvalstybinio duomenų tvarkymo atveju gali pasinaudoti įgaliojimu dėl tariamų BDAR pažeidimų – kreiptis į tos valstybės teismą ir pradėti teismo procesą, tik laikydamasi sprendimų priėmimo kompetencijos paskirstymo vadovaujančiai priežiūros institucijai ir kitoms priežiūros institucijoms taisyklių[88], yra suderinama su Chartijos 7, 8 ir 47 straipsniais, kuriuose asmenims atitinkamai užtikrinama teisė į asmens duomenų apsaugą ir teisė į veiksmingą teisinę gynybą (67 punktas).

Antra, Teisingumo Teismas nusprendė, kad tarpvalstybinio duomenų tvarkymo atveju valstybės narės priežiūros institucijai, kuri nėra vadovaujanti priežiūros institucija, siekiant pasinaudoti

83 Kaip tai suprantama pagal BDAR 4 straipsnio 23 punktą.
84 Numatytos BDAR 56 ir 60 straipsniuose.
85 BDAR 56 straipsnio 1 dalis.
86 BDAR 60 straipsnio 7 dalis.
87 BDAR 56 straipsnio 2 dalyje ir 66 straipsnyje įtvirtintos vadovaujančios priežiūros institucijos principinės kompetencijos priimti sprendimus išimtys.
88 Numatytos 55 ir 56 straipsniuose, siejamuose su BDAR 60 straipsniu.

įgaliojimu pareikšti ieškinį[89] nereikalaujama, kad tarpvalstybinį asmens duomenų tvarkymą vykdantis duomenų valdytojas ar duomenų tvarkytojas, kuriam pareiškiamas šis ieškinys, šios valstybės narės teritorijoje turėtų pagrindinę buveinę arba kitą buveinę. Vis dėlto naudojimasis šiuo įgaliojimu turi patekti į BDAR teritorinę taikymo sritį[90], o tai reiškia, kad tarpvalstybinį duomenų tvarkymą vykdantis duomenų valdytojas arba duomenų tvarkytojas turi turėti buveinę Sąjungos teritorijoje (80, 83, 84 punktai ir rezoliucinės dalies 2 punktas).

Trečia, Teisingumo Teismas pripažino, kad tarpvalstybinio duomenų tvarkymo atveju valstybės narės priežiūros institucija, kuri nėra vadovaujanti priežiūros institucija, gali pasinaudoti įgaliojimu dėl tariamų BDAR pažeidimų – kreiptis į tos valstybės teismą ir tam tikrais atvejais pradėti teismo procesą tiek prieš duomenų valdytojo pagrindinę buveinę, esančią šios institucijos valstybėje narėje, tiek prieš kitą šio duomenų valdytojo buveinę, jeigu ieškinys reiškiamas dėl duomenų tvarkymo, atliekamo šiai buveinei vykdant veiklą, o minėta institucija turi kompetenciją pasinaudoti šiuo įgaliojimu.

Vis dėlto Teisingumo Teismas patikslino, jog šiuo įgaliojimu galima naudotis su sąlyga, kad BDAR taikomas. Nagrinėjamu atveju, kadangi Belgijoje esančios *Facebook* grupės buveinės veikla neatsiejamai susijusi su pagrindinėje byloje nagrinėjamu asmens duomenų tvarkymu, už kurį Sąjungos teritorijoje yra atsakinga *Facebook Ireland*, toks tvarkymas laikomas atliekamu „duomenų valdytojo [buveinei vykdant] savo veiklą“, todėl visiškai patenka į BDAR taikymo sritį (94–96 punktai ir rezoliucinės dalies 3 punktas).

Ketvirta, Teisingumo Teismas nusprendė, kad tuomet, kai valstybės narės priežiūros institucija, kuri nėra „vadovaujanti priežiūros institucija“, pareiškė ieškinį dėl tarpvalstybinio asmens duomenų tvarkymo iki BDAR įsigaliojimo momento, ieškinys Sąjungos teisės požiūriu gali būti toliau nagrinėjamas remiantis Direktyvos 95/46, kuri tebetaikoma joje įtvirtintų taisyklių pažeidimams, padarytiems iki šios direktyvos panaikinimo, nuostatomis. Be to, tokį ieškinį minėta institucija gali pareikšti dėl pažeidimų, padarytų įsigaliojus BDAR, jeigu yra susiklosčiusi viena iš situacijų, kai šis reglamentas išimties tvarka suteikia tai institucijai kompetenciją priimti sprendimą, kuriuo konstatuojama, kad nagrinėjamas duomenų tvarkymas pažeidžia šio reglamento normas ir laikomasi pačiame reglamente numatytų bendradarbiavimo procedūrų (105 punktas ir rezoliucinės dalies 4 punktas).

Galiausiai, penkta, Teisingumo Teismas pripažino tiesioginį BDAR nuostatos, pagal kurią kiekviena valstybė narė įstatymuose numato, kad jos priežiūros institucija yra įgaliota atkreipti teisminių institucijų dėmesį į visus šio reglamento pažeidimus ir tinkamais atvejais pradėti teismo procesą, veikimą. Todėl tokia institucija gali remtis šia nuostata, siekdama pareikšti ieškinį arba toliau tęsti procesą prieš asmenis, net jeigu ji konkrečiai nebuvo perkelta į atitinkamos valstybės narės teisę (113 punktas ir rezoliucinės dalies 5 punktas).

VII. Sąjungos teisės aktų taikymas teritoriniu aspektu

[89] Pagal BDAR 58 straipsnio 5 dalį.

[90] BDAR 3 straipsnio 1 dalyje numatyta, kad šis reglamentas taikomas asmens duomenų tvarkymui, „kai asmens duomenis <...> tvarko duomenų valdytojo arba duomenų tvarkytojo buveinė [Sąjungoje], vykdydama savo veiklą, neatsižvelgiant į tai, ar duomenys tvarkomi Sąjungoje, ar ne“.

2014 m. gegužės 13 d. didžiosios kolegijos Sprendimas „Google Spain ir Google“ (C-131/12, EU:C:2014:317)

Šiame sprendime (taip pat žr. II.3. skyrių „Sąvoka „asmens duomenų tvarkymas“ ir V.1. skyrių „Teisė prieštarauti dėl asmens duomenų tvarkymo“ („Teisė būti pamirštam“)) Teisingumo Teismas sprendė dėl Direktyvos 95/46 teritorinės taikymo srities.

Taigi, Teisingumo Teismas nusprendė, kad asmens duomenys yra tvarkomi duomenų valdytojo padaliniui vykdant veiklą valstybės narės teritorijoje, kaip tai suprantama pagal Direktyvą 95/46, jei paieškos variklio eksploatuotojas, kurio buveinė yra trečiojoje šalyje, įsteigia valstybėje narėje savo filialą arba patronuojamąją bendrovę, kurių veikla orientuojama į šios valstybės gyventojus, kad reklamuotų ir parduotų šio variklio rodomiems reklaminiams pranešimams skirtas vietas (55, 60 punktai ir rezoliucinės dalies 2 punktas).

Tokiomis aplinkybėmis paieškos variklio eksploatuotojo veikla ir atitinkamoje valstybėje narėje esančio jo padalinio veikla yra skirtingos, tačiau neatsiejamai susijusios, nes su reklaminiams pranešimams skirtomis vietomis susijusi veikla yra priemonė, kuria siekiama padaryti atitinkamą paieškos variklį ekonomiškai pelningą, o šis variklis savo ruožtu yra šią veiklą leidžianti vykdyti priemonė (56 punktas).

VIII. Visuomenės teisė susipažinti su Europos Sąjungos institucijų dokumentais ir asmens duomenų apsauga

2010 m. birželio 29 d. didžiosios kolegijos Sprendimas „Komisija / Bavarian Lager“ (C-28/08 P, EU:C:2010:378)

Bendrovė *Bavarian Lager*, kuri buvo įsteigta siekiant importuoti vokišką alų, skirtą Jungtinės Karalystės gėrimų pardavimo vartoti vietoje įstaigoms, negalėjo parduoti savo produkto, nes daug Jungtinės Karalystės verslininkų, eksploatuojančių gėrimų pardavimo vartoti vietoje įstaigas, buvo susaistyti išimtinių pirkimo sutarčių, kurios juos įpareigojo pirkti alų tik iš tam tikrų alaus daryklų.

Remiantis Jungtinės Karalystės teisės aktais, susijusiais su alaus tiekimu (toliau – GBP), Britanijos alaus daryklos privalėjo barų valdytojams suteikti galimybę pirkti alų, pagamintą kitoje alaus darykloje, su sąlyga, kad jis laikomas statinėse. Didžiosios dalies ne Jungtinėje Karalystėje pagaminto alaus nebuvo galima laikyti „statinėse laikomu alumi“, kaip tai suprantama pagal GBP, taigi jis nepateko į šių teisės aktų taikymo sritį. Manydama, kad minėti teisės aktai yra kiekybiniam importo apribojimui lygiavertį poveikį turinti priemonė, *Bavarian Lager* pateikė skundą Komisijai.

Vykstant Komisijos prieš Jungtinę Karalystę inicijuotai procedūrai dėl įsipareigojimų neįvykdymo, Bendrijos ir Jungtinės Karalystės institucijų atstovai, taip pat Vidaus rinkos alaus daryklų konfederacijos (VRADK) atstovai dalyvavo 1996 m. spalio 11 d. susitikime. Jungtinės Karalystės institucijoms pranešus Komisijai apie nagrinėjamų teisės aktų pakeitimą siekiant leisti parduoti buteliuose laikomą alų (kaip skirtingos kilmės alų) lygiai kaip statinėse laikomą alų, Komisija informavo *Bavarian Lager* apie procedūros dėl įsipareigojimų nevykdymo sustabdymą.

Bavarian Lager paprašius pateikti jai visą 1996 m. spalio mėn. susitikimo protokolą nurodant visus dalyvius, Komisija 2004 m. kovo 18 d. sprendimu šį prašymą atmetė, remdamasi, be kita ko, šių asmenų privataus gyvenimo apsauga, užtikrinama pagal Reglamentą Nr. 45/2001.

Bavarian Lager pateikė ieškinį Bendrajam Teismui, prašydama panaikinti šį Komisijos sprendimą. 2007 m. lapkričio 8 d. sprendimu Bendrasis Teismas panaikino Komisijos sprendimą, be kita ko, laikydamasis nuomonės, kad vien suinteresuotųjų asmenų vardų ir pavardžių įtraukimas į subjekto, kuriam jos atstovavo, vardu susitikime dalyvavusių asmenų sąrašą nekenkia ir nekelia pavojaus šių asmenų privačiam gyvenimui. Komisija, palaikoma Jungtinės Karalystės ir Tarybos, pateikė Teisingumo Teismui apeliacinį skundą dėl šio Bendrojo Teismo sprendimo.

Teisingumo Teismas pirmiausia pažymėjo, kad kai pagal Reglamentą Nr. 1049/2001 dėl galimybės susipažinti su dokumentais[91] pateiktu prašymu siekiama susipažinti su dokumentais, kuriuose yra asmens duomenų, taikomos visos Reglamento Nr. 45/2001 nuostatos, įskaitant nuostatą, pagal kurią asmens duomenų gavėjui nustatoma pareiga įrodyti būtinybę juos atskleisti, ir nuostatą, pagal kurią atitinkamam asmeniui suteikiama teisė bet kada dėl viršesnių teisėtų priežasčių, susijusių su konkrečia jo padėtimi, nesutikti, kad būtų tvarkomi su juo susiję duomenys (63 punktas).

Teisingumo Teismas konstatavo, kad susitikimo, vykusio per procedūrą dėl įsipareigojimų neįvykdymo, dalyvių sąraše, pateiktame to susitikimo protokole, yra asmens duomenų, kaip tai suprantama pagal Reglamento Nr. 45/2001 2 straipsnio a punktą, nes galėjo būti nustatyta šiame susitikime dalyvavusių asmenų tapatybė (70 punktas).

Galiausiai jis padarė išvadą, kad reikalaudama, jog dėl asmenų, kurie nedavė aiškaus sutikimo atskleisti tame protokole esančius jų asmens duomenis, būtų įrodyta tų duomenų perdavimo būtinybė, Komisija taikė minėto reglamento 8 straipsnio b punkto nuostatas (77 punktas).

Iš tiesų tuo atveju, kai pagal Reglamentą Nr. 1049/2001 pateiktame prašyme leisti susipažinti su minėtu protokolu nėra jokių aiškių ir pagrįstų įrodymų ir jokių įtikinamų argumentų, kurie patvirtintų šių asmens duomenų perdavimo būtinybę, Komisija negali palyginti atitinkamų šalių skirtingų interesų. Ji taip pat negali patikrinti, ar yra priežasčių manyti, kad šiuo perdavimu galėtų būti pažeisti atitinkamų asmenų teisėti interesai, kaip reikalaujama pagal Reglamento Nr. 45/2001 8 straipsnio b punktą (78 punktas)[92].

2015 m. liepos 16 d. Sprendimas „ClientEarth ir PAN Europe / EFSA“ (C-615/13 P, EU:C:2015:489)

Europos maisto saugos tarnyba (EFSA) sudarė darbo grupę, siekdama parengti Reglamento (EB) Nr. 1107/2009[93] 8 straipsnio 5 dalies įgyvendinimo gaires; pagal tą nuostatą asmuo, prašantis išduoti leidimą pateikti į rinką augalų apsaugos produktą, prie dokumentų rinkinio turi pridėti prieinamą specialistų recenzuotą mokslo literatūrą, kaip nustatė EFSA, susijusią su veikliąja

[91] 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001, p. 43; 2004 m. specialusis leidimas lietuvių k., 1 sk., 3 t., p. 331).

[92] Šis sprendimas pristatytas 2010 m. metiniame pranešime, p. 14.

[93] 2009 m. spalio 21 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1107/2009 dėl augalų apsaugos produktų pateikimo į rinką ir panaikinantis Tarybos direktyvas 79/117/EEB ir 91/414/EEB (OL L 309, 2009, p. 1).

medžiaga ir jos metabolitais, darančiais šalutinį poveikį sveikatai, aplinkai ir atsitiktinai paveiktoms rūšims.

Pateikus gairių projektą visuomenei susipažinti, *ClientEarth* ir *Pesticide Action Network Europe* (*PAN Europe*) pateikė dėl jo pastabas. Šiomis aplinkybėmis jos kartu kreipėsi į EFSA su prašymu leisti susipažinti su tam tikrais dokumentais, susijusiais su gairių projekto rengimu, įskaitant išorės ekspertų pastabas.

EFSA leido *ClientEarth* ir *PAN Europe* susipažinti, be kita ko, su išorės ekspertų atskiromis pastabomis dėl gairių projekto. Tačiau ji nurodė, kad remdamasi Reglamento Nr. 1049/2001 4 straipsnio 1 dalies b punktu ir Sąjungos teisės aktais dėl asmens duomenų apsaugos, be kita ko, Reglamentu Nr. 45/2001, įslaptino šių ekspertų pavardes. Šiuo klausimu ji teigė, kad ekspertų pavardžių atskleidimas būtų laikomas asmens duomenų perdavimu, kaip tai suprantama pagal Reglamento Nr. 45/2001 8 straipsnį, ir kad nagrinėjamu atveju nebuvo tenkinamos šiame straipsnyje nustatytos tokių duomenų perdavimo sąlygos.

Taigi *ClientEarth ir PAN Europe* Bendrajam Teismui pateikė ieškinį, prašydamos panaikinti minėtą EFSA sprendimą. Bendrajam Teismui atmetus ieškinį, *ClientEarth* ir *PAN Europe* pateikė Teisingumo Teismui apeliacinį skundą dėl šio Bendrojo Teismo sprendimo[94].

Pirma, Teisingumo Teismas pažymėjo: kadangi prašoma informacija leistų vieną ar kitą konkretų ekspertą sieti su tam tikra pastaba, ji susijusi su fiziniais asmenimis, kurių tapatybė žinoma, todėl tai yra asmens duomenys, kaip jie suprantami pagal Reglamento Nr. 45/2001 2 straipsnio a punktą. Kadangi „asmens duomenų“, kaip jie suprantami pagal Reglamento Nr. 45/2001 2 straipsnio a punktą, sąvoka ir „duomenų, susijusių su privačiu gyvenimu“ sąvoka neturi būti painiojamos, Teisingumo Teismas padarė išvadą, kad *ClientEarth* ir *PAN Europe* teiginys, jog ginčijama informacija nesiejama su atitinkamų ekspertų privačiu gyvenimu, yra nepagrįstas (29 ir 32 punktai).

Antra, Teisingumo Teismas išnagrinėjo *ClientEarth* ir de *PAN Europe* argumentą, grindžiamą tuo, kad egzistavo tam tikras nepasitikėjimas EFSA, dažnai kaltinta šališkumu pasitelkiant ekspertus, turinčius tam tikrų asmeninių interesų, kuriuos lemia jų ryšiai su pramonės atstovais, taip pat tuo, kad buvo būtinybė užtikrinti šios institucijos sprendimų priėmimo proceso skaidrumą. Šis argumentas buvo grindžiamas tyrimu, kurį atlikus konstatuota, kad dauguma EFSA darbo grupei priklausiusių ekspertų palaikė ryšius su pramonės lobistų grupėmis. Šiuo aspektu Teisingumo Teismas nusprendė, kad ginčijamą informaciją buvo būtina gauti siekiant konkrečiai patikrinti kiekvieno šių ekspertų nešališkumą vykdant savo mokslo užduotį EFSA naudai. Todėl Teisingumo Teismas panaikino Bendrojo Teismo sprendimą, konstatuodamas, kad Bendrasis Teismas neteisingai nusprendė, jog minėto *ClientEarth* ir *PAN Europe* argumento neužteko ginčijamos informacijos perdavimo būtinybei įrodyti (57–59 punktai).

Trečia, vertindamas ginčijamo EFSA sprendimo teisėtumą Teisingumo Teismas nagrinėjo, ar yra pagrindo manyti, kad dėl duomenų perdavimo galėtų nukentėti atitinkamų asmenų teisėti interesai. Šiuo aspektu jis konstatavo, kad EFSA teiginys, jog ginčijamos informacijos atskleidimas galėjo kelti grėsmę minėtų ekspertų privačiam gyvenimui ir neliečiamumui, yra bendro pobūdžio svarstymas, kuris kaip nors kitaip nagrinėjamu atveju nebuvo pagrįstas. Priešingai, Teisingumo

[94] 2013 m. rugsėjo 13 d. Bendrojo Teismo sprendimas *ClientEarth ir PAN Europe / EFSA* (T-214/11, EU:T:2013:483).

Teismas konstatavo, kad pats toks atskleidimas būtų leidęs išsklaidyti atitinkamus įtarimus dėl šališkumo arba suteikęs galimai susijusiems ekspertams galimybę ginčyti, prireikus pasinaudojant turimomis teisių gynimo priemonėmis, šių su šališkumu susijusių teiginių pagrįstumą. Atsižvelgdamas į tai Teisingumo Teismas panaikino ir EFSA sprendimą (69 ir 73 punktai).

* * *

Šioje informacijos suvestinėje pristatyti sprendimai yra nurodyti jurisprudencijos katalogo skyriuose 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07., 4.11.11.01.