EUROPOS SĄJUNGOS
TEISINGUMO TEISMAS

LT

Teminis biuletenis

Asmens duomenų apsauga

Tyrimų ir dokumentacijos direktoratas

curia.europa.eu

Įžanga

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

Ji įtvirtinta pirminėje teisėje, kaip antai, Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 8 straipsnyje ir Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 16 straipsnio 1 dalyje. Be to, ši pagrindinė teisė yra glaudžiai susijusi su Chartijos 7 straipsnyje įtvirtinta teise į privatų ir šeimos gyvenimą.

Kiek tai susiję su antrine teise, pažymėtina, kad nuo XX a. paskutinio dešimtmečio vidurio Europos bendrija priėmė įvairių dokumentų, skirtų asmens duomenų apsaugai užtikrinti. 2018 m. panaikinta Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo[1] šiuo aspektu buvo pagrindinis Sąjungos teisės aktas šioje srityje.

Vėliau buvo priimta Direktyva 2002/58/EB[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, siekdamas atsižvelgti į naujus technologijų ir prekybos pokyčius, nuo 2017 m. Sąjungos teisės aktų leidėjas pradėjo šios direktyvos peržiūrą[4], kuri trunka iki šiol[5].

2016 m. Europos Sąjunga pakeitė bendrą teisinę sistemą šioje srityje. Tam ji priėmė Reglamentą (ES) 2016/679[6] dėl asmens 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, kurios nuostatos taikomos nuo 2018 m. gegužės 6 d.

---

1 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL 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. 6 išnašą).

2 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB 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/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančia Direktyvą 2002/58/EB (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. šio biuletenio I skyriaus 1 skirsnį „Sąjungos antrinės teisės suderinamumas su teise į asmens duomenų apsaugą“).

4 2017 m. sausio 10 d. Komisija pateikė pasiūlymą pakeisti šią direktyvą Reglamentu dėl privatumo ir elektroninių ryšių.

5 2021 m. vasario 10 d. Europos Sąjungos Taryba patvirtino įgaliojimus derėtis dėl privatumo ir konfidencialumo apsaugos naudojantis elektroninių ryšių paslaugomis taisyklių peržiūros; tai leido pradėti derybas su Europos Parlamentu. Su pasiūlymu dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių) galima susipažinti spustelėjus šią nuorodą: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN

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 ir kuriuo panaikinama Direktyva 95/46/EB (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

ES institucijoms ir organams tvarkant asmens duomenis, šių duomenų apsauga nuo 2018 m. gruodžio 11 d. užtikrinama Reglamentu (ES) 2018/1725[8]. Siekiant nuoseklaus požiūrio į asmens duomenų apsaugą visoje Sąjungoje, šiuo reglamentu siekiama kiek įmanoma suderinti šios srities taisykles su BDAR nustatyta tvarka.

Galiausiai siekdamas spręsti naujų technologijų keliamus iššūkius, nuo 2020 m. Sąjungos teisės aktų leidėjas ėmėsi naujų teisėkūros priemonių[9], suderinamų su Sąjungos teisės nuostatomis dėl asmens duomenų apsaugos.

Atsižvelgiant į gausią Teisingumo Teismo jurisprudenciją asmens duomenų apsaugos klausimu, šiame teminiame biuletenyje siekiama apžvelgti atrinktus pamatinius šios srities sprendimus, taip pat sprendimus, svariai prisidėjusius plėtojant šią jurisprudenciją, ypatingą dėmesį skiriant Teisingumo Teismo didžiosios kolegijos sprendimams. Kalbant konkrečiau, šis biuletenis apima jurisprudenciją, susijusią ir su bendru asmens duomenų apsaugos reglamentavimu, suformuotą aiškinant Direktyvą 95/46 ir BDAR, ir su atskirais sektoriais, kaip antai elektroniniais ryšiais ir baudžiamąja teise. Be to, jame siekiama pristatyti atskirus sprendimus, susijusius su keliuose sektoriuose taikomais teisės aktais, pirmiausia išskiriant Chartijos lemiamą vaidmenį plėtojant šią jurisprudenciją.

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 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/EB (OL L 295, 2018, p. 39).

9 Šiuo klausimu nurodytinos, be kita ko, trys teisėkūros iniciatyvos: *i)* 2022 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/868 dėl Europos duomenų valdymo, kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1724 (Duomenų valdymo aktas) (OL L 152, 2022, p. 1) ir 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/2854 dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/2394 ir Direktyva (ES) 2020/1828 (Duomenų aktas) (OL L 2854, 2023, p. 1); *ii)* teisės aktų dėl skaitmeninių paslaugų ir rinkų rinkinys, kurį sudaro 2022 m. spalio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB, (Skaitmeninių paslaugų aktas) (OL L 277, 2022, p. 1) ir 2022 m. rugsėjo 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/1925 dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828 (Skaitmeninių rinkų aktas) (OL L 265, 2022, p. 1); ir *iii)* pirmasis pasiūlymas dėl teisėkūros procedūra priimamo akto, skirto dirbtinio intelekto reglamentavimo sistemai sukurti, kuris įgyvendintas priėmus Dirbtinio intelekto aktą (OL L, 2024/1689).

Turinys

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)

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[10] ir Nr. 259/2008[11], 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 gavėjų teisės į privatų gyvenimą apskritai, o konkrečiai – teisės į jų asmens duomenų apsaugą apribojimas.

Kad tokį apribojimą būtų galima pateisinti, jis turi būti numatytas įstatymuose, nekeisti šių teisių esmės ir, remiantis proporcingumo principu, turi būti būtinas ir iš tikrųjų atitikti Sąjungos pripažįstamus bendrojo intereso tikslus, o naudojimosi šiomis teisėmis išimtys ir apribojimai neturi viršyti to, kas būtina. Tokiomis aplinkybėmis Teisingumo Teismas

[10] 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).

[11] 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).

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.

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. Vis dėlto Teisingumo Teismas nekvestionavo tokios paramos gavėjų sąrašų paskelbimo, kurį nacionalinės valdžios institucijos atliko laikotarpiu iki to sprendimo paskelbimo dienos, poveikio.

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)

Šis sprendimas priimtas išnagrinėjus prašymus įvertinti Direktyvos 2006/24/EB dėl duomenų saugojimo 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 saugojimu, 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 2006/24 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.

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 reikalaujamas duomenų saugojimas 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 saugojimas, siekiant juos galimai perduoti kompetentingoms nacionalinėms institucijoms, iš tikrųjų atitinka bendrojo intereso tikslą, t. y. kovą su dideliu nusikalstamumu, o galiausiai – visuomenės saugumą.

Vis dėlto Teisingumo Teismas laikėsi nuomonės, kad priimdamas direktyvą dėl duomenų saugojimo Sąjungos teisės aktų leidėjas peržengė ribas, kurios nustatomos pagal proporcingumo principą. Todėl šią direktyvą jis pripažino negaliojančia, nes konstatavo, kad joje nustatytas plataus masto ir ypač didelis pagrindinių teisių apribojimas nebuvo pakankamai reglamentuotas, siekiant užtikrinti, kad šis apribojimas neviršytų to, kas griežtai būtina. Direktyva 2006/24 buvo 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. Be to, šioje direktyvoje nebuvo numatyta 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, nei materialinių ir procedūrinių tokios galimybės ar tokio naudojimo sąlygų. Galiausiai, kiek tai susiję su duomenų saugojimo laikotarpiu, toje direktyvoje buvo nustatytas ne mažiau kaip šešių mėnesių laikotarpis ir nebuvo daroma jokio skirtumo tarp duomenų kategorijų, atsižvelgiant į atitinkamus asmenis ar galimą duomenų naudingumą siekiamo tikslo atžvilgiu.

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

Taigi minėtoje direktyvoje nebuvo visapusiškai užtikrinta nepriklausomos institucijos atliekama apsaugos ir saugumo reikalavimų laikymosi kontrolė, kaip to aiškiai reikalaujama Chartijoje.

2022 m. birželio 21 d. didžiosios kolegijos Sprendimas „Ligue des droits humains“ (C-817/19, EU:C:2022:491)

PNR duomenys (*Passenger Name Record*) yra oro vežėjų rezervavimo ir išvykimo kontrolės sistemose saugoma informacija apie rezervacijas. PNR direktyvoje[12] šie vežėjai įpareigojami kiekvieno keleivio, kuris keliauja ES išorės skrydžiu tarp trečiosios šalies ir Europos Sąjungos, duomenis perduoti atitinkamo skrydžio paskirties ar išvykimo valstybės narės informacijos apie keleivius skyriui (toliau – IKS), siekiant kovoti su terorizmu ir sunkiais nusikaltimais. Iš tiesų IKS iš anksto vertina taip perduotus PNR duomenis[13], paskui juos saugo, kad atitinkamos valstybės narės ar kitos valstybės narės kompetentingos institucijos galėtų atlikti galimą vėlesnį vertinimą. Valstybės narės gali nuspręsti šią direktyvą taikyti ir ES vidaus skrydžiams[14].

Ligue des droits humains kreipėsi į *Cour constitutionnelle* (Konstitucinis Teismas, Belgija) su skundu dėl įstatymo, kuriuo į Belgijos teisę perkeliama tiek PNR direktyva, tiek API direktyva[15], panaikinimo. Pareiškėjos teigimu, šis įstatymas pažeidžia teisę į privatų gyvenimą ir asmens duomenų apsaugą. Ji kritikuoja, pirma, labai platų PNR duomenų pobūdį ir, antra, bendrą šių duomenų rinkimo, perdavimo ir tvarkymo pobūdį. Anot jos, įstatymas taip pat kelia grėsmę laisvam asmenų judėjimui, nes juo netiesiogiai atkuriama sienų kontrolė, PNR sistemą išplečiant ES vidaus skrydžiams ir vežimui kitomis transporto priemonėmis Sąjungoje.

Šiomis aplinkybėmis Belgijos Konstitucinis Teismas pateikė Teisingumo Teismui prašymą priimti prejudicinį sprendimą dėl klausimų, susijusių, be kita ko, su PNR direktyvos galiojimu.

Didžiosios kolegijos sprendimu Teisingumo Teismas patvirtino PNR direktyvos galiojimą tiek, kiek ji gali būti aiškinama pagal Chartiją.

Šiuo klausimu Teisingumo Teismas konstatavo: Teisingumo Teismo pateiktas PNR direktyvos nuostatų aiškinimas remiantis Chartijos 7, 8 ir 21 straipsniuose bei 52 straipsnio 1 dalyje[16] įtvirtintomis pagrindinėmis teisėmis užtikrina šios direktyvos atitiktį šiems straipsniams, todėl nagrinėjant pateiktus klausimus nenustatyta jokių aplinkybių, galinčių turėti įtakos šios direktyvos galiojimui.

---

12 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais (OL L 119, 2016, p. 132; toliau – PNR direktyva).

13 Šio išankstinio vertinimo tikslas – nustatyti asmenis, kuriuos kompetentingos institucijos turi toliau tirti, atsižvelgiant į tai, kad šie asmenys gali būti susiję su teroristiniais arba sunkiais nusikaltimais. Toks vertinimas atliekamas sistemingai ir automatizuotomis priemonėmis lyginant PNR duomenis su duomenimis duomenų bazėse, „atitinkančiose <...> tikslus“, arba juos tvarkant pagal PNR direktyvos 6 straipsnio 2 dalies a punkte ir 3 dalyje iš anksto nustatytus kriterijus.

14 Pasinaudodamos PNR direktyvos 2 straipsnyje numatyta galimybe.

15 2004 m. balandžio 29 d. Tarybos direktyva 2004/82/EB dėl vežėjų įpareigojimo perduoti keleivių duomenis (OL L 261, 2004, p. 24; toliau – API direktyva). Šia direktyva reglamentuojamas oro vežėjų atliekamas išankstinės informacijos apie keleivius (kaip antai, naudojamo kelionės dokumento numeris ir tipas, taip pat pilietybė) perdavimas kompetentingoms nacionalinėms valdžios institucijoms siekiant gerinti sienų kontrolę ir kovoti su nelegalia imigracija.

16 Pagal šią nuostatą bet koks šios Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės. Be to, šių teisių ir laisvių apribojimai galimi tik tuo atveju, kai jie būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

Visų pirma jis priminė, kad Sąjungos teisės aktas turi būti aiškinamas taip, kad, kiek įmanoma, nekiltų abejonių dėl jo galiojimo ir kad jis atitiktų visą pirminę teisę, ypač Chartijos nuostatas, todėl valstybės narės turi užtikrinti, kad jos nesirems tokiu teisės akto aiškinimu, kuris prieštarauja Sąjungos teisinėje tvarkoje įtvirtintoms saugomoms pagrindinėms teisėms arba kitiems Sąjungos pripažintiems bendriesiems principams. Dėl PNR direktyvos Teisingumo Teismas nurodė, kad iš daugelio jos konstatuojamųjų dalių ir nuostatų matyti, kad jomis reikalaujama tokio Sąjungos teisinę tvarką atitinkančio aiškinimo, pabrėžiant, kad Sąjungos teisės aktų leidėjas, nurodydamas aukštą duomenų apsaugos lygį, didelę reikšmę teikia visapusiškai Chartijoje įtvirtintų pagrindinių teisių pagarbai.

Teisingumo Teismas konstatavo, kad PNR direktyvoje nustatyti tam tikro dydžio Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymai, ypač kiek ja siekiama nustatyti nuolatinio, netikslinio ir sistemingo stebėjimo sistemą, apimančią visų oro transporto paslaugomis besinaudojančių asmenų asmens duomenų automatizuotą vertinimą. Jis priminė, kad galimybė valstybėms narėms pateisinti tokį suvaržymą turi būti vertinama atsižvelgiant į jo dydį ir patikrinant, ar siekiamo bendrojo intereso tikslo svarba yra proporcinga šio suvaržymo dydžiui.

Teisingumo Teismas padarė išvadą, kad šioje direktyvoje numatytas PNR duomenų perdavimas, tvarkymas ir saugojimas gali būti laikomi apribotais tuo, kas griežtai būtina kovos su teroristiniais nusikaltimais ir sunkiais nusikaltimais tikslais, su sąlyga, kad šioje direktyvoje numatyti įgaliojimai aiškinami siaurai. Šiuo klausimu paskelbtame sprendime visų pirma patikslinta, kad:

- Pagal PNR direktyvą nustatyta sistema turėtų apimti tik aiškiai identifikuojamą informaciją, pateiktą jos I priedo punktuose ir susijusią su įvykdytu skrydžiu ir atitinkamu keleiviu, o tai reiškia, kad kai kurios tame priede nurodytos kategorijos apima tik konkrečiai jose nurodytą informaciją[17].

- Pagal PNR direktyvą nustatyta sistema turėtų būti taikoma tik tokiems teroristiniams ir sunkiems nusikaltimams, kurie objektyviai (bent netiesiogiai) susiję su keleivių vežimu oru. Ši sistema negali būti taikoma tokiems šio tipo nusikaltimams, kurie, nors ir atitinka šioje direktyvoje nustatytą kriterijų dėl sunkumo ribos ir yra nurodyti direktyvos II priede, vis dėlto, atsižvelgiant į nacionalinės baudžiamosios teisenos sistemos ypatumus, yra priskiriami prie įprastų nusikaltimų.

- Bet koks PNR direktyvos taikymo išplėtimas visiems ES vidaus skrydžiams ar jų daliai, jeigu valstybė narė nuspręstų pasinaudoti tokia direktyvoje numatyta galimybe, turi apsiriboti tuo, kas griežtai būtina. Tokiam taikymo srities išplėtimui

[17] Pavyzdžiui „Informacija apie mokėjimo būdus“ (priedo 6 punktas) turi apimti tik informaciją, susijusią su mokėjimo už lėktuvo bilietą būdais ir sąskaitos už jį išrašymu, ir visiškai neapima kitos tiesiogiai su skrydžiu nesusijusios informacijos, o „Bendros pastabos“ (12 punktas) gali apimti tik šiame punkte aiškiai išvardytą informaciją, susijusią su nepilnamečiais keleiviais.

turi būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas yra privalomas, kontrolė. Šiuo klausimu Teisingumo Teismas patikslino:

- tik tuo atveju, kai atitinkama valstybė narė nustato pakankamai konkrečias aplinkybes, leidžiančias manyti, kad jai kyla tikra, esama arba numanoma terorizmo grėsmė, šios direktyvos taikymas visiems ES vidaus skrydžiams į tą valstybę narę arba iš jos ribotu laikotarpiu, kuris yra griežtai būtinas, tačiau kuris gali būti pratęstas, neviršija to, kas griežtai būtina[18].

- Nesant tokios terorizmo grėsmės, minėta direktyva neturėtų būti taikoma visiems ES vidaus skrydžiams, o turėtų apsiriboti tik ES vidaus skrydžiais, susijusiais su tam tikrais oro maršrutais ar kelionių schemomis arba tam tikrais oro uostais, dėl kurių, atitinkamos valstybės narės nuomone, yra požymių, pateisinančių tokį taikymą. Griežta būtinybė taikyti šį reikalavimą taip atrinktiems ES vidaus skrydžiams turi būti reguliariai peržiūrima, atsižvelgiant į sąlygų, dėl kurių jie buvo atrinkti, pokyčius.

- Atlikdamas išankstinį PNR duomenų vertinimą (jo tikslas – nustatyti asmenis, kuriuos prieš atvykstant ar išvykstant reikia papildomai patikrinti; toks vertinimas iš pradžių atliekamas automatizuotu būdu) IKS, pirma, gali palyginti šiuos duomenis tik su duomenimis, esančiais duomenų bazėse, susijusiose su asmenimis ar daiktais, kurie yra ieškomi arba dėl kurių buvo paskelbti perspėjimai[19]. Šios duomenų bazės turi būti nediskriminacinės ir kompetentingos institucijos jas turi naudoti kovai su teroristiniais nusikaltimais ir sunkiais nusikaltimais, kurie yra objektyviai (bent netiesiogiai) susiję su keleivių vežimu oru. Antra, dėl išankstinio vertinimo pagal iš anksto nustatytus kriterijus IKS neturėtų naudoti dirbtinio intelekto technologijų mašininio mokymosi (*machine learning*) sistemos kontekste, nes tokios technologijos be žmogaus įsikišimo ir kontrolės gali pakeisti vertinimo procesą ir ypač vertinimo kriterijus, kuriais grindžiamas jų taikymo rezultatas ir šių kriterijų reikšmė. Minėti vertinimo kriterijai turėtų būti nustatyti taip, kad būtų užtikrinta, kad jie būtų taikomi konkrečiai tiems asmenims, kurių atžvilgiu yra pagrįstų įtarimų dėl jų dalyvavimo darant teroristinius nusikaltimus ar sunkius nusikaltimus, ir kad būtų atsižvelgta tiek į kaltinamuosius, tiek į išteisinamuosius elementus, kartu nesukeliant tiesioginės ar netiesioginės diskriminacijos[20].

---

[18] Iš tiesų vien tokios grėsmės buvimas gali leisti nustatyti atitinkamų duomenų perdavimo ir tvarkymo bei kovos su terorizmu ryšį. Taigi PNR direktyvos taikymas visiems ES vidaus skrydžiams iš atitinkamos valstybės narės ar į ją apibrėžtu laikotarpiu neviršija to, kas griežtai būtina, o sprendimą dėl tokio taikymo turi galėti patikrinti teismas arba nepriklausomas administracinis subjektas.

[19] T. y. duomenų bazės, susijusios su asmenimis ar daiktais, kurie yra ieškomi arba dėl kurių paskelbti perspėjimai, kaip tai suprantama pagal PNR direktyvos 6 straipsnio 3 dalies a punktą. Tačiau analizė, grindžiama įvairiomis duomenų bazėmis, gali būti viena iš duomenų gavybos (*data mining*) formų ir lemti neproporcingą šių duomenų naudojimą, suteikiant priemones nustatyti tikslų duomenų subjektų profilį vien dėl to, kad jie ketina keliauti lėktuvu.

[20] Iš anksto nustatyti kriterijai turi būti tiksliniai, proporcingi ir konkretūs ir reguliariai peržiūrimi (PNR direktyvos 6 straipsnio 4 dalis). Išankstinis vertinimas pagal iš anksto nustatytus kriterijus turi būti atliktas be diskriminacijos. Remiantis PNR direktyvos 6 straipsnio 4 dalies ketvirtu

- Atsižvelgiant į tokiam automatizuotam PNR duomenų tvarkymui būdingą paklaidos lygį ir didelį „klaidingų teigiamų rezultatų“, gautų taikant šias priemones 2018 ir 2019 m., skaičių, tikimybė, kad taikant pagal PNR direktyvą sukurtą sistemą bus pasiekti nustatyti tikslai, iš esmės priklauso nuo to, ar IKS antrame etape tinkamai atliks teigiamų rezultatų, gautų tvarkant šiuos duomenis, patikrą neautomatizuotomis priemonėmis. Šiuo klausimu valstybės narės turi numatyti aiškias ir tikslias taisykles, kurios reglamentuotų ir kuriomis būtų vadovaujamasi informacijos apie keleivius skyrių pareigūnams, atsakingiems už individualią peržiūrą, atliekant analizę, kad būtų paisoma Chartijos 7, 8 ir 21 straipsniuose įtvirtintų pagrindinių teisių ir, be kita ko, užtikrinta IKS nuosekli administracinė praktika, laikantis nediskriminavimo principo. Visų pirma jos turi užtikrinti, kad IKS nustatytų objektyvius peržiūros kriterijus, kuriais remdamiesi jų pareigūnai galėtų patikrinti, pirma, ar teigiama atitiktis (*hit*) iš tikrųjų susijusi su asmeniu, kuris gali būti susijęs su teroristiniais ar sunkiais nusikaltimais, ir, antra, ar automatizuotas duomenų tvarkymas yra nediskriminuojamojo pobūdžio. Esant šiam kontekstui, Teisingumo Teismas taip pat pabrėžė, kad kompetentingos institucijos turi užtikrinti, kad suinteresuotasis asmuo galėtų suprasti iš anksto nustatytų vertinimo kriterijų veikimą ir tuos kriterijus taikančias programas, kad žinodamas visas faktines aplinkybes galėtų nuspręsti, ar pasinaudoti teise į teisminę gynybą. Nagrinėdamas tokį skundą teismas, atsakingas už kompetentingų institucijų priimto sprendimo teisėtumo kontrolę, ir suinteresuotasis asmuo (išskyrus atvejus, kai kyla grėsmė valstybės saugumui) turi turėti galimybę susipažinti su visais motyvais ir įrodymais, kuriais remiantis buvo priimtas toks sprendimas, įskaitant iš anksto nustatytus vertinimo kriterijus ir informaciją, apie tuos kriterijus taikančių programų veikimą.

- PNR duomenų atskleidimas ir vėlesnis jų vertinimas, t. y. po duomenų subjekto atvykimo ar išvykimo, gali būti atliekamas tik remiantis naujomis aplinkybėmis ir objektyviais duomenimis, dėl kurių kyla pagrįstas įtarimas dėl to asmens dalyvavimo vykdant sunkų nusikaltimą, objektyviai (bent netiesiogiai) susijusį su keleivių vežimu oru, arba kurie leidžia manyti, kad konkrečiu atveju duomenys gali veiksmingai padėti kovoti su tokį ryšį su keleivių vežimu oru turinčiais teroristiniais nusikaltimais. PNR duomenų atskleidimą dėl tokio vėlesnio vertinimo turi iš anksto patikrinti teismas arba nepriklausoma administracinė institucija, gavusi pagrįstą kompetentingų institucijų prašymą, išskyrus tinkamai pagrįstus skubos atvejus, neatsižvelgiant į tai, ar toks prašymas buvo pateiktas iki pasibaigiant šešių mėnesių laikotarpiui, kai duomenys buvo perduoti IKS, ar jam pasibaigus[21].

sakiniu, kriterijai jokiomis aplinkybėmis neturi būti nustatomi asmens rasės ar etninės kilmės, politinių pažiūrų, religijos ar filosofinių įsitikinimų, narystės profesinėse sąjungose, sveikatos, lytinio gyvenimo ar seksualinės orientacijos pagrindu.

[21] Pagal PNR direktyvos 12 straipsnio 1 ir 3 dalis tokia kontrolė aiškiai numatyta tik prašymams atskleisti PNR duomenis, pateiktiems pasibaigus šešių mėnesių terminui po tokių duomenų perdavimo IKS.

2022 m. lapkričio 22 d. didžiosios kolegijos Sprendimas „Luxembourg Business Registers“ (C-37/20 ir C-601/20, EU:C:2022:912)

Kovos su pinigų plovimu ir teroristų finansavimu ir jų prevencijos tikslais pagal Kovos su pinigų plovimu direktyvą[22] valstybės narės įpareigojamos vesti registrą, kuriame būtų saugoma informacija apie jų teritorijoje įsteigtų bendrovių ir kitų juridinių asmenų tikruosius savininkus[23]. Po šios direktyvos pakeitimo Direktyva 2018/843[24] tam tikra informacija turi būti visais atvejais prieinama bet kuriam plačiosios visuomenės atstovui. Pagal taip pakeistą Kovos su pinigų plovimu direktyvą Liuksemburgo teisės aktuose buvo numatyta, kad įsteigiamas *Registre des bénéficiaires effectifs* (tikrųjų savininkų registras, toliau – RBE), kurio paskirtis – saugoti ir atskleisti tam tikrą informaciją apie tikruosius registruotų subjektų savininkus, su kuria turi galimybę susipažinti bet kuris asmuo.

Šiomis aplinkybėmis *tribunal d’arrondissement de Luxembourg* (Liuksemburgo apygardos teismas) inicijuotos dvi bylos: ieškinius pareiškė atitinkamai WM ir *Sovim SA*, kurie ginčija *Luxembourg Business Registers* (RBE valdytoja) sprendimą atmesti jų prašymus neleisti plačiajai visuomenei susipažinti su informacija apie WM, kaip nekilnojamojo turto bendrovės tikrąjį savininką (pirmoji byla), ir apie tikrąjį *Sovim SA* savininką (antroji byla). Šiose dviejose bylose *tribunal d’arrondissement de Luxembourg*, abejodamas dėl Sąjungos teisės nuostatų, kuriose įtvirtinta visuomenės prieigos prie informacijos apie tikruosius savininkus sistema, galiojimo, pateikė Teisingumo Teismui prejudicinį klausimą dėl galiojimo įvertinimo.

Savo sprendime Teisingumo Teismo didžioji kolegija pripažino Direktyvą 2018/843 negaliojančia tiek, kiek ja Kovos su pinigų plovimu direktyva buvo iš dalies pakeista įpareigojant valstybes nares užtikrinti, kad informaciją apie jų teritorijoje įsteigtų bendrovių ir kitų juridinių asmenų tikruosius savininkus visais atvejais galėtų gauti bet kuris plačiosios visuomenės atstovas[25].

Visu pirma Teisingumo Teismas konstatavo, kad iš dalies pakeistoje Kovos su pinigų plovimu direktyvoje numatyta plačiosios visuomenės galimybė susipažinti su informacija apie tikruosius savininkus yra didelis pagrindinių teisių į privataus gyvenimo gerbimą ir asmens duomenų apsaugą, įtvirtintų atitinkamai Chartijos 7 ir 8 straipsniuose, suvaržymas.

Šiuo klausimu Teisingumo Teismas pažymėjo: kadangi atitinkami duomenys apima informaciją apie fizinius asmenis, kurių tapatybė nustatyta, t. y. tikruosius valstybių narių

---

22 2015 m. gegužės 20 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/60/EB bei Komisijos direktyva 2006/70/EB (OL L 141, 2015, p. 73; toliau – Kovos su pinigų plovimu direktyva).

23 Pagal Kovos su pinigų plovimu direktyvos 3 straipsnio 6 punktą tikrieji savininkai yra fiziniai asmenys, kurie faktiškai yra kliento savininkai arba jį kontroliuoja, ir (arba) fiziniai asmenys, kurių vardu vykdomas sandoris ar veikla.

24 2018 m. gegužės 30 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/843, kuria iš dalies keičiama Direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos direktyvos 2009/138/EB ir 2013/36/ES (OL L 156, 2018, p. 43).

25 Pripažintas negaliojančiu Direktyvos 2018/843 1 straipsnio 15 punkto c papunktis, kuriuo iš dalies pakeistas Kovos su pinigų plovimu direktyvos 30 straipsnio 5 dalies pirmos pastraipos c punktas.

teritorijoje įsteigtų bendrovių ir kitų juridinių asmenų savininkus, bet kurio plačiosios visuomenės atstovo prieiga prie tokios informacijos daro poveikį pagrindinei teisei į privataus gyvenimo gerbimą. Be to, jos atskleidimas plačiajai visuomenei yra asmens duomenų tvarkymas. Jis pridūrė, kad toks atskleidimas plačiajai visuomenei yra minėtų dviejų pagrindinių teisių suvaržymas, nesvarbu, kaip pateikta informacija bus naudojama vėliau.

Dėl šio suvaržymo dydžio Teisingumo Teismas nurodė, kad tiek, kiek plačiajai visuomenei atskleidžiama informacija susijusi su tikrojo savininko tapatybe ir jo turimų naudos teisių bendrovėse ar kituose juridiniuose asmenyse pobūdžiu ir apimtimi, ji gali padėti išsiaiškinti tam tikrus asmens tapatybės duomenis, atitinkamo asmens turtinę padėtį, taip pat konkrečius ekonominius sektorius, šalis ir įmones, į kuriuos jis investavo. Be to, ši informacija tampa prieinama potencialiai neribotam skaičiui asmenų, todėl toks asmens duomenų tvarkymas gali leisti asmenims, kurie dėl su šios priemonės tikslu nesusijusių priežasčių siekia gauti informacijos apie tikrojo savininko turtinę ir finansinę padėtį, laisvai susipažinti su šiais duomenimis. Ši galimybė dar mažiau ribojama, kai su duomenimis galima susipažinti internete. Be to, pasekmės duomenų subjektams dėl galimo piktnaudžiavimo naudojant jų asmens duomenis gali būti dar didesnės dėl to, kad, atskleidus plačiajai visuomenei šiuos duomenis, jie gali būti ne tik laisvai prieinami, bet ir saugomi bei platinami ir kad dėl tokio vėlesnio tvarkymo šiems asmenims tampa dar sunkiau, gal net neįmanoma, veiksmingai apsiginti nuo piktnaudžiavimo.

Toliau nagrinėdamas ginčijamo teisių suvaržymo pateisinimąTeisingumo Teismas, pirma, pažymėjo, kad nagrinėjamu atveju laikytasi teisėtumo principo. Iš tikrųjų pirma nurodytų pagrindinių teisių įgyvendinimo apribojimas, kurį lemia plačiosios visuomenės galimybė susipažinti su informacija apie tikruosius savininkus, yra numatytas Sąjungos teisėkūros procedūra priimtame akte, t. y. iš dalies pakeistoje Kovos su pinigų plovimu direktyvoje. Be to, šioje direktyvoje konkrečiai nurodyta, kad ši informacija turi būti adekvati, tiksli ir aktuali, ir aiškiai išvardijama tam tikra informacija, su kuria turi būti leista susipažinti bet kuriam plačiosios visuomenės atstovui. Joje taip pat nustatytos sąlygos, kurioms esant valstybės narės gali numatyti tokios prieigos išimtis.

Antra, Teisingumo Teismas patikslino, kad nagrinėjamas suvaržymas nedaro poveikio Chartijos 7 ir 8 straipsniuose garantuojamų pagrindinių teisių esmei. Nors tiesa, kad iš dalies pakeistoje Kovos su pinigų plovimu direktyvoje nepateikiama išsamaus duomenų, su kuriais turi būti leista susipažinti bet kuriam plačiosios visuomenės atstovui, sąrašo ir kad valstybės narės turi teisę suteikti prieigą prie papildomos informacijos, galima gauti, saugoti, vadinasi, ir pateikti visuomenei tik adekvačią informaciją apie tikruosius savininkus ir jų turimas naudos teises, tad negalima pateikti informacijos, kuri nėra adekvačiai susijusi su iš dalies pakeistos Kovos su pinigų plovimu direktyvos tikslais. Vis dėlto neatrodo, kad tokį ryšį turinčios informacijos atskleidimas plačiajai visuomenei keltų kokį nors poveikį pirma nurodytų pagrindinių teisių esmei.

Trečia, Teisingumo Teismas pažymėjo, kad numatydamas galimybę plačiajai visuomenei susipažinti su informacija apie tikruosius savininkus Sąjungos teisės aktų leidėjas siekia

užkirsti kelią pinigų plovimui ir teroristų finansavimui, nustatydamas didesnį skaidrumą leidžiančią užtikrinti aplinką, kuri mažiau galėtų būti naudojama šiais tikslais, o tai yra bendrojo intereso tikslas, kuriuo galima pateisinti net ir didelius Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymus.

Ketvirta, vertindamas, ar nagrinėjamas suvaržymas yra tinkamas, būtinas ir proporcingas, Teisingumo Teismas konstatavo, kad iš tikrųjų plačiosios visuomenės prieiga prie informacijos apie tikruosius savininkus gali padėti įgyvendinti šį tikslą.

Vis dėlto jis pareiškė, kad šio suvaržymo negalima laikyti apribotu tuo, kas tikrai būtina. Pirma, šio suvaržymo tikroji būtinybė negali būti įrodyta remiantis aplinkybe, kad „teisėto intereso“, kurį pagal Kovos su pinigų plovimu direktyvos redakciją, galiojusią iki jos pakeitimo Direktyva 2018/843, turėjo turėti visi asmenys, norintys gauti informaciją apie tikruosius savininkus, kriterijų buvo sunku taikyti praktiškai ir kad jį taikant galėjo būti priimti savavališki sprendimai. Iš tikrųjų galimi sunkumai tiksliai apibrėžti atvejus ir sąlygas, kuriomis visuomenė gali susipažinti su informacija apie tikruosius savininkus, negali pateisinti to, kad Sąjungos teisės aktų leidėjas numatytų galimybę plačiajai visuomenei susipažinti su šia informacija.

Antra, Direktyvoje 2018/843 pateikti paaiškinimai taip pat negali įrodyti tikros nagrinėjamo suvaržymo būtinybės[26]. Kadangi, kaip matyti iš šių paaiškinimų, plačiosios visuomenės prieiga prie informacijos apie tikruosius savininkus turi leisti pilietinei visuomenei, įskaitant žiniasklaidą ir pilietinės visuomenės organizacijas, nuodugniau tikrinti informaciją, Teisingumo Teismas nurodė, kad tiek žiniasklaida, tiek pilietinės visuomenės organizacijos, susijusios su kova su pinigų plovimu ir kova su terorizmo finansavimu, turi teisėtą interesą susipažinti su atitinkama informacija. Tas pats pasakytina ir apie asmenis, kurie nori žinoti kurios nors bendrovės ar kito teisės subjekto tikruosius savininkus dėl to, kad jie gali sudaryti su jais sandorius, arba apie finansų įstaigas ir valdžios institucijas, kovojančias su nusikaltimais pinigų plovimo ir teroristų finansavimo srityje.

Be to, nagrinėjamas suvaržymas nėra ir proporcingas. Šiuo klausimu Teisingumo Teismas konstatavo, kad materialinės teisės normos, kuriose numatytas šis suvaržymas, neatitinka aiškumo ir tikslumo reikalavimo. Iš tiesų iš dalies pakeistoje Kovos su pinigų plovimu direktyvoje numatyta, kad bet kuris plačiosios visuomenės atstovas gali gauti „bent“ joje nurodytus duomenis, ir valstybėms narėms suteikiama galimybė suteikti prieigą prie papildomos informacijos, apimančios „bent“ atitinkamo tikrojo savininko gimimo datą arba kontaktinius duomenis. Iš vartojamo žodžio „bent“ matyti, kad pagal šias nuostatas visuomenei leidžiama atskleisti duomenis, kurie nėra pakankamai apibrėžti ar nustatytini.

Be to, kiek tai susiję su šio suvaržymo dydžio ir nurodyto bendrojo intereso tikslo svarbos lyginimu, Teisingumo Teismas pripažino, kad, atsižvelgiant į šio tikslo svarbą, jis

[26] Kalbama apie Direktyvos 2018/843 30 konstatuojamojoje dalyje pateiktus paaiškinimus.

gali pateisinti net didelius Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių apribojimus.

Vis dėlto, pirma, kova su pinigų plovimu ir teroristų finansavimu pirmiausia yra viešosios valdžios institucijų ir tokių subjektų, kaip kredito ir finansų įstaigos, kurioms dėl jų veiklos nustatomi specialūs įpareigojimai, kompetencijos sritis. Dėl šios priežasties iš dalies pakeistoje Kovos su pinigų plovimu direktyvoje numatyta, kad informaciją apie tikruosius savininkus visais atvejais turi galėti gauti kompetentingos institucijos ir finansinės žvalgybos padaliniai be jokių apribojimų, taip pat įpareigotieji subjektai, kai vykdomas deramas klientų tikrinimas[27].

Antra, palyginti su ankstesne tvarka, pagal kurią prieigos prie informacijos apie tikruosius savininkus galimybę turėjo ne tik kompetentingos institucijos ir kai kurios įstaigos, bet ir bet kuris asmuo arba organizacija, kurie galėjo įrodyti teisėtą interesą, Direktyvoje 2018/843 įtvirtinta tvarka daug labiau suvaržomos Chartijos 7 ir 8 straipsniuose garantuojamos pagrindinės teisės, ir šio didesnio suvaržymo negali kompensuoti dėl šios tvarkos, palyginti su pirmąja, galinti atsirasti nauda kovojant su pinigų plovimu ir teroristų finansavimu.

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)

Jau minėtame Sprendime *Digital Rights Ireland ir Seitlinger ir kt.* Direktyvą 2006/24 pripažinus negaliojančia, 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 Sprendimo *Digital Rights Ireland ir Seitlinger ir kt.* paskelbimo 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

[27] Iš dalies pakeistos Kovos su pinigų plovimu direktyvos 30 straipsnio 5 dalies pirmos pastraipos a ir b punktai.

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 su prašymais 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 pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, draudžiami nacionalinės teisės aktai, kaip antai galiojantys 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. Teisingumo Teismo teigimu, tokie teisės aktai viršija tai, kas griežtai būtina, ir negali būti laikomi pateisinamais demokratinėje visuomenėje, kaip to reikalaujama pagal minėtą 15 straipsnio 1 dalį, siejamą su minėtais Chartijos straipsniais.

Pagal tą pačią nuostatą, siejamą su tais pačiais Chartijos straipsniais, taip pat draudžiami nacionalinės teisės aktai, reglamentuojantys 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.

Vis dėlto Teisingumo Teismas konstatavo, kad pagal Direktyvos 2002/58 15 straipsnio 1 dalį nedraudžiami teisės aktai, 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. Dėl tokio apribojimo pažymėtina, kad 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.

II. Asmens duomenų tvarkymas pagal bendrąjį šios srities reglamentavimą

1. Bendrojo reglamentavimo taikymo sritis

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

Kai 2001 m. rugsėjo 11 d. buvo įvykdyti teroristiniai išpuoliai, Jungtinės Amerikos Valstijos (JAV) priėmė teisės aktus, juose 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[28], 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 d. Taryba priėmė Sprendimą 2004/496[29], 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.

---

[28] 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).

[29] 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; klaidų ištaisymas OL L 255, 2005, p. 168).

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 paslaugoms suteikti, bet su duomenų tvarkymu, būtinu visuomenės saugumui apginti ir nubaudimo tikslais.

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.

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.

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,* taip pat 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.

Savo sprendime Teisingumo Teismas taip pat išnagrinėjo Direktyvos 95/46 teritorinę taikymo sritį.

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.

Tokiomis aplinkybėmis paieškos variklio eksploatuotojo veikla ir atitinkamoje valstybėje narėje esančio jo padalinio veikla, nors ir atskiros, iš tiesų yra 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.

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; jiems buvo iškeltos 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.

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.

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 reglamentuojamas asmens duomenų tvarkymas, galintis kelti pavojų pagrindinėms laisvėms, visų pirma teisei į privatų gyvenimą, būtina aiškinti atsižvelgiant į pagrindines teises, kurios yra įtrauktos į Chartiją, šios direktyvos 3 straipsnio 2 dalies antroje įtraukoje įtvirtinta nukrypstanti nuostata turi būti aiškinama griežtai. 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.

2024 m. sausio 16 d. didžiosios kolegijos Sprendimas „Österreichische Datenschutzbehörde“ (C-33/22, EU:C:2024:46)

Siekdama ištirti galimą politinę įtaką *Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (Federalinė Konstitucijos apsaugos ir kovos su terorizmu tarnyba, Austrija)[30], *Nationalrat* (Nacionalinė Taryba, Austrija) įsteigė tyrimo komitetą (toliau – BVT tyrimo komitetas). Šis komitetas apklausė WK kaip liudytoją. Nepaisant WK prašymo užtikrinti anonimiškumą, šios apklausos protokolas, kuriame buvo nurodyta visa jo pavardė ir vardai, buvo paskelbtas *Parlament Österreich* (Austrijos parlamentas) interneto svetainėje. Teigdamas, kad toks jo tapatybės atskleidimas prieštarauja BDAR ir Austrijos teisei, WK pateikė skundą *Österreichische Datenschutzbehörde* (Nacionalinė duomenų apsaugos institucija, Austrija) (toliau – *Datenschutzbehörde*). 2019 m. rugsėjo 18 d. sprendimu *Datenschutzbehörde* pripažino neturinti kompetencijos priimti sprendimo dėl skundo ir paaiškino, kad pagal valdžių padalijimo principą ji, kaip vykdomosios valdžios institucija, negali kontroliuoti BVT tyrimo komiteto, priskiriamo prie įstatymų leidžiamosios valdžios.

Bundesverwaltungsgericht (Federalinis administracinis teismas, Austrija) priėmus sprendimą, kuriuo buvo patenkintas WK skundas ir panaikintas *Datenschutzbehörde* sprendimas, ši pateikė kasacinį skundą Vyriausiajam administraciniam teismui.

Šiomis aplinkybėmis prašymą priimti prejudicinį sprendimą pateikęs teismas Teisingumo Teismo paklausė, ar valstybės narės parlamento įsteigto tyrimo komiteto veikla patenka į BDAR taikymo sritį ir ar šis reglamentas taikomas, kai ši veikla susijusi su nacionalinio saugumo užtikrinimu.

Pirma, Teisingumo Teismas priminė, kad BDAR 2 straipsnio 2 dalies a punkto, kuriame numatyta, kad šis reglamentas netaikomas asmens duomenų tvarkymui, atliekamam

[30] 2021 m. gruodžio 1 d. ši institucija tapo *Direktion Staatsschutz und Nachrichtendienst* (Valstybės saugumo ir žvalgybos tarnybos direkcija, Austrija).

vykdant veiklą, kuriai Sąjungos teisė netaikoma, vienintelis tikslas – į jo taikymo sritį neįtraukti duomenų tvarkymo, kurį atlieka valstybės institucijos, vykdydamos veiklą, kuria siekiama užtikrinti nacionalinį saugumą arba kuri gali būti priskirta prie tos pačios kategorijos. Taigi vien aplinkybės, kad veikla yra būdinga valstybei ar viešosios valdžios institucijai, nepakanka, kad ji automatiškai nepatektų į BDAR taikymo sritį.

Tokį aiškinimą, išplaukiantį iš to, kad nėra skirtumo, kas tvarko atitinkamus duomenis, patvirtina BDAR 4 straipsnio 7 punktas[31].

Teisingumo Teismas patikslino, kad BVT tyrimo komiteto parlamentinis pobūdis nereiškia, kad jo veikla nepatenka į BDAR taikymo sritį. Iš tiesų šio reglamento 2 straipsnio 2 dalies a punkte numatyta išimtis susijusi tik su veiklos kategorijomis, kurios dėl savo pobūdžio nepatenka į Sąjungos teisės taikymo sritį, o ne su asmenų kategorijomis. Taigi aplinkybė, kad asmens duomenis tvarko valstybės narės parlamento, naudojantis jam priklausančia vykdomosios valdžios kontrolės teise, įsteigtas tyrimo komitetas, savaime neleidžia daryti išvados, kad šie duomenys tvarkomi vykdant veiklą, kuri nepatenka į Sąjungos teisės taikymo sritį.

Antra, Teisingumo Teismas pažymėjo, kad nors pačios valstybės narės turi nustatyti savo esminius saugumo interesus ir imtis priemonių užtikrinti saugumą[32], vien tai, kad nacionalinė priemonė buvo priimta siekiant užtikrinti nacionalinį saugumą, nereiškia, kad Sąjungos teisė netaikoma ir kad valstybės narės neturi deramai jos laikytis. BDAR 2 straipsnio 2 dalies a punkte numatyta išimtis susijusi tik su veiklos kategorijomis, kurios dėl savo pobūdžio nepatenka į Sąjungos teisės taikymo sritį. Šiuo klausimu pažymėtina, jog vien aplinkybės, kad duomenų valdytojas yra viešosios valdžios institucija, kurios pagrindinė veikla – užtikrinti nacionalinį saugumą, nepakanka, kad į BDAR taikymo sritį nepatektų asmens duomenų tvarkymas, kurį ši institucija atlieka vykdydama kitokio pobūdžio veiklą.

Nagrinėjamu atveju neatrodo, kad BVT tyrimo komiteto vykdoma politinė kontrolė savaime yra veikla, kuria siekiama užtikrinti nacionalinį saugumą arba kuri gali būti priskirta prie tos pačios kategorijos. Darytina išvada, kad ši veikla patenka į BDAR taikymo sritį, tačiau tai turi patikrinti prašymą priimti prejudicinį sprendimą pateikęs teismas.

Vis dėlto parlamento tyrimo komitetas gali susipažinti su asmens duomenimis, kuriems dėl nacionalinio saugumo priežasčių turi būti taikoma ypatinga apsauga. Šiuo klausimu pažymėtina, kad BDAR numatytų teisių ir pareigų apribojimai gali būti nustatyti teisėkūros priemonėmis, siekiant, be kita ko, užtikrinti nacionalinį saugumą[33]. Taigi šiuo pagrindu galima pateisinti apribojimus, susijusius su asmens duomenų rinkimu, duomenų subjektų informavimu ir jų prieiga prie šių duomenų arba jų atskleidimu be

[31] Jame sąvoka „duomenų valdytojas“ apibrėžiama kaip „fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones“.

[32] Pagal ESS 4 straipsnio 2 dalį.

[33] Pagal BDAR 23 straipsnį.

duomenų subjektų sutikimo kitiems asmenims nei duomenų valdytojas, jeigu tokiais apribojimais paisoma duomenų subjektų pagrindinių teisių ir laisvių esmės ir demokratinėje visuomenėje jie yra būtina ir proporcinga priemonė.

Vis dėlto Teisingumo Teismas pažymėjo, kad iš jam pateiktos informacijos nematyti, jog BVT tyrimo komitetas būtų teigęs, kad duomenų subjekto asmens duomenų atskleidimas buvo būtinas nacionaliniam saugumui užtikrinti ir grindžiamas šiuo tikslu numatyta nacionaline teisėkūros priemone, o tai prireikus dar turi patikrinti prašymą priimti prejudicinį sprendimą pateikęs teismas.

2. Sąvoka „asmens duomenys“

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

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 sudarė „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 *a priori* neleido 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.

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 puslapio naudotojo tapatybei nustatyti, turi ne elektroninių paslaugų teikėjas, o šio naudotojo interneto prieigos teikėjas, negalima atmesti galimybės, kad elektroninių paslaugų teikėjo išsaugoti dinaminiai IP adresai jo atžvilgiu yra asmens duomenys, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą.

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.

2017 m. gruodžio 20 d. Sprendimas „Nowak“ (C-434/16, 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 punktas turi būti aiškinamas 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 egzaminuojamojo pateikti

raštiški atsakymai yra informacija, kuri, atsižvelgiant į jos turinį, tikslą ir poveikį, yra su juo susijusi, galioja ir tuomet, kai egzamine galima naudotis vadovėliais.

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.

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 su 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.

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.

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 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. Iš tiesų vykdant savanorišką ar religinę veiklą tokiam asmens duomenų tvarkymui netaikoma jokios šios direktyvos taikymo srities išimties, nes jis nepriskiriamas nei prie su visuomenės saugumu susijusios veiklos kategorijos, nei prie tik asmeninės ar namų ūkio veiklos kategorijų, kurioms ši direktyva netaikoma.

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 skyriaus 1 skirsnį „Bendro reglamentavimo taikymo sritis“)
Teisingumo Teismas turėjo galimybę 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. 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.

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

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 užsirašydavo informaciją lankydamiesi pas asmenis, kurių jie patys ar jų bendruomenė nepažįsta. Tokie duomenys buvo 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 tikėjimo 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.

2021 m. birželio 22 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[34], 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, siekiančius ją pakartotinai naudoti, ir tas 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.

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“[35], kuriam dėl aptariamų duomenų ypatingo jautrumo BDAR numatyta didesnė apsauga.

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.

---

[34] 1997 m. spalio 1 d. *Ceļu satiksmes likums* (Kelių eismo įstatymas; *Latvijas Vēstnesis*, 1997, Nr. 274/276) 14^1 straipsnio 2 dalis.

[35] BDAR 10 straipsnis.

Taigi, viena vertus, šio tvarkymo neapima išimtis, susijusi su BDAR netaikymu duomenų tvarkymui vykdant veiklą, kuriai netaikoma Sąjungos teisė[36]. 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 esminėms valstybės funkcijoms ir pagrindiniams visuomenės interesams apsaugoti. Su kelių eismo saugumu susijusia veikla nesiekiama šio tikslo, taigi jos negalima priskirti prie veiklos, kuria siekiama užtikrinti nacionalinį saugumą, kategorijos.

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[37]. Teisingumo Teismas konstatavo, kad atlikdama minėtą duomenų atskleidimą CSDD negali būti laikoma „kompetentinga institucija“[38].

Siekdamas nustatyti, ar galimybė susipažinti su asmens duomenimis apie kelių eismo taisyklių pažeidimus, kaip antai baudos taškais, yra asmens duomenų apie „nusikalstamas veikas“[39], 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 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

36 BDAR 2 straipsnio 2 dalies a punktas.

37 BDAR 2 straipsnio 2 dalies d punktas.

38 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.

39 BDAR 10 straipsnis.

papildomai, kartu su už tokį pažeidimą pritaikyta sankcija, ir šių taškų sumavimas sukelia teisinių padarinių, tam tikrais atvejais net draudimą vairuoti.

2023 m. gruodžio 5 d. didžiosios kolegijos Sprendimas „Nacionalinis visuomenės sveikatos centras“ (C-683/21, EU:C:2023:949)

Siekdamos geriau valdyti COVID-19 pandemiją Lietuvos valdžios institucijos 2020 m. nusprendė organizuoti mobiliosios IT programėlės įsigijimą. Ši programėlė turėjo padėti siekti epidemiologinės priežiūros tikslų, leisdama registruoti ir stebėti sąlytį su COVID-19 viruso nešiotojais turėjusių asmenų duomenis.

Šiuo tikslu Lietuvos nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (toliau – NVSC), atsakingas už šį įsigijimą, kreipėsi į bendrovę UAB „IT sprendimai sėkmei“ (toliau – bendrovė ITSS) ir pavedė jai sukurti tokią mobiliąją programėlę. Vėliau NVSC darbuotojai šiai bendrovei siuntė elektroninius laiškus dėl, be kita ko, programėlėje pateiktinų klausimų.

2020 m. balandžio ir gegužės mėn. bendrovės ITSS sukurta mobilioji programėlė buvo padaryta viešai prieinama. 3 802 asmenys ja pasinaudojo ir pateikė įvairių joje prašytų savo duomenų. Vis dėlto dėl finansavimo trūkumo NVSC nesudarė su bendrove ITSS viešojo pirkimo sutarties dėl mobiliosios programėlės oficialaus įsigijimo ir nutraukė su tuo susijusią pirkimo procedūrą.

Tuo metu nacionalinė priežiūros institucija pradėjo tyrimą dėl asmens duomenų, gautų naudojant šią programėlę, tvarkymo. Užbaigus tyrimą priimtu šios institucijos sprendimu administracinės baudos buvo skirtos ir NVSC, ir bendrovei ITSS, kuri pripažinta bendra duomenų valdytoja.

NVSC apskundė šį sprendimą Vilniaus apygardos administraciniam teismui. Abejodamas dėl kelių BDAR nuostatų aiškinimo, šis teismas kreipėsi į Teisingumo Teismą su prašymu priimti prejudicinį sprendimą.

Savo sprendime Teisingumo Teismas (didžioji kolegija) išaiškino, be kita ko, sąvoką „duomenų tvarkymas“. Šiuo klausimu jis nurodė, kad asmens duomenų naudojimas testuojant mobiliąją IT programėlę yra duomenų tvarkymas pagal BDAR. Tačiau taip nėra, jeigu tokie duomenys nuasmeninti taip, kad jų subjekto tapatybė negali arba nebegali būti nustatyta, arba tai yra netikri duomenys, nesusiję su jokiu esamu fiziniu asmeniu.

Iš tiesų klausimas, ar asmens duomenys naudojami testuojant IT programėlę, ar kitam tikslui, neturi įtakos atitinkamos operacijos pripažinimui „duomenų tvarkymu“. Be to, tik asmens duomenų tvarkymas yra „tvarkymas“, kaip tai suprantama pagal BDAR. Netikri ar anoniminiai duomenys nėra asmens duomenys.

4. Sąvoka „asmens duomenų susistemintas rinkinys“

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

Šiame sprendime (taip pat žr. II skyriaus 3 skirsnį „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.

5. Sąvoka „asmens duomenų valdytojas“

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

Šioje byloje (taip pat žr. II skyriaus 3 skirsnį „Sąvoka „asmens duomenų tvarkymas“ ir 4 skirsnį „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, tokių narių renkamų vykdant 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.

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

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 tikslų 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.

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*. Panašu, kad 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, priekaištavo *Fashion ID* dėl to, kad ši 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 duomenų rinkimą ir perdavimą. Tačiau, anot

Teisingumo Teismo, remiantis minėta informacija, *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.

Be to, Teisingumo Teismas pabrėžė, jog būtina, kad ir 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.

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.

2023 m. gruodžio 5 d. didžiosios kolegijos Sprendimas „Nacionalinis visuomenės sveikatos centras“ (C-683/21, EU:C:2023:949)

Šioje byloje (taip pat žr. II skyriaus 3 skirsnį „Sąvoka „asmens duomenų tvarkymas“) Teisingumo Teismas pažymėjo, kad subjektas, pavedęs įmonei sukurti mobiliąją IT programėlę ir prisidėjęs nustatant šia programėle atliekamo asmens duomenų tvarkymo tikslus ir priemones, gali būti laikomas duomenų valdytoju[40]. Šios išvados nepaneigia, aplinkybė, kad šis subjektas pats neatliko tokių duomenų tvarkymo veiksmų, nedavė aiškaus sutikimo atlikti konkrečius tokio tvarkymo veiksmus arba padaryti šią mobiliąją programėlę viešai prieinamą ir jos neįsigijo, nebent prieš padarant šią programėlę viešai prieinamą šis subjektas aiškiai išreiškė nepritarimą tokiam veiksmui ir jo nulemtam asmens duomenų tvarkymui.

6. Sąvoka „bendras duomenų valdytojas“

2023 m. gruodžio 5 d. didžiosios kolegijos Sprendimas „Nacionalinis visuomenės sveikatos centras“ (C-683/21, EU:C:2023:949)

Šioje byloje (taip pat žr. II skyriaus 3 skirsnį „Sąvoka „asmens duomenų tvarkymas“ ir 5 skirsnį „Sąvoka „asmens duomenų valdytojas“) Teisingumo Teismas nurodė, kad norint du subjektus pripažinti bendrais duomenų valdytojais nereikia, kad jie būtų sudarę susitarimą dėl asmens duomenų tvarkymo tikslų ir priemonių nustatymo arba

[40] Kaip tai suprantama pagal BDAR 4 straipsnio 7 punktą.

susitarimu nustatę bendro duomenų valdymo sąlygas. Žinoma, pagal BDAR[41] bendri duomenų valdytojai turi tarpusavio susitarimu skaidriai nustatyti savo atitinkamą atsakomybę už šiame reglamente nustatytų prievolių laikymąsi. Vis dėlto tokio susitarimo buvimas yra ne išankstinė sąlyga tam, kad du ar daugiau subjektų būtų laikomi „bendrais duomenų valdytojais“, o pareiga, pagal BDAR nustatyta bendrais duomenų valdytojais jau pripažintiems subjektams, kad jie laikytųsi jiems nustatytų šio reglamento reikalavimų. Taigi šį pripažinimą lemia jau vien kelių subjektų dalyvavimas nustatant duomenų tvarkymo tikslus ir priemones.

Kiek tai susiję su atitinkamų subjektų bendru duomenų tvarkymo tikslų ir priemonių nustatymu, Teisingumo Teismas patikslino, kad jų dalyvavimas atliekant šį nustatymą gali būti įvairių formų ir jį gali lemti ir bendras jų sprendimas, ir sutampantys sprendimai. Pastaruoju atveju šie sprendimai turi papildyti vienas kitą, kad kiekvienas jų turėtų konkretų poveikį nustatant duomenų tvarkymo tikslus ir priemones.

7. Asmens duomenų tvarkymo teisėtumo sąlygos

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

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

[41] BDAR 26 straipsnio 1 dalis, siejama su jo 79 konstatuojamąja dalimi.

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.

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 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 pripažinti, 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.

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 Europos Sąjungos piliečių vertinimas sistemiškai kovos su nusikalstamumu tikslu tvarkant tik asmens duomenis apie atitinkamos valstybės narės pilietybės neturinčius Europos Sąjungos piliečius yra pagal EB 12 straipsnio 1 dalį draudžiama diskriminacija.

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

Šiame sprendime (taip pat žr. II skyriaus 2 skirsnį „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. Nagrinėtu 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.

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.

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.

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.

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.

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 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[42] yra numatytas atvejų, kai asmens duomenų tvarkymą galima laikyti teisėtu, sąrašas. Konkrečiai kalbant, duomenų subjekto sutikimas turi būti duotas laisva valia, konkretus, informuotas ir

[42] Direktyvos 95/46 7 straipsnis ir BDAR 6 straipsnis.

nedviprasmiškas[43]. Šiuo aspektu sutikimas nėra tinkamas, jeigu jis duotas tylint, grindžiamas neveikimu arba langeliai pažymėti iš anksto.

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.

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. Prašymą priimti prejudicinį sprendimą pateikęs teismas turi atlikti tam reikalingus patikrinimus.

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 pažymėjo, 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.

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.

[43] Direktyvos 95/46 2 straipsnio h punktas ir BDAR 4 straipsnio 11 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 skyriaus 3 skirsnį „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, jog, 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.

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“[44]. 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 taškų 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.

Be to, Teisingumo Teismas konstatavo, kad, atsižvelgiant į šių duomenų jautrumą ir šio pagrindinių teisių suvaržymo stiprumą, šios teisės yra viršesnės tiek už viešąjį interesą turėti galimybę susipažinti su oficialiais dokumentais, kaip antai nacionalinių transporto priemonių ir jų vairuotojų registru, tiek už teisę į informacijos laisvę.

Dėl tų pačių priežasčių Teisingumo Teismas taip pat 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.

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

[44] 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. <...> “

Sąjungos teise, draudžiama nuspręsti, kad šių nuostatų teisiniai padariniai lieka galioti, kol bus paskelbtas galutinis jo sprendimas.

III. Asmens duomenų tvarkymas pagal atskirų sektorių reglamentavimą

1. Asmens duomenų tvarkymas elektroninių ryšių sektoriuje

2018 m. spalio 2 d. didžiosios kolegijos Sprendimas „Ministerio Fiscal“ (C-207/16, EU:C:2018:788)

Toje 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 remiantis tuo, kad veiksmai, dėl kurių buvo vykdomas baudžiamosios veikos tyrimas, nelaikomi „sunkiu“ nusikaltimu, t. y. pagal Ispanijos teisę nusikaltimu, už kurį skiriama ilgesnė nei penkerių metų laisvės atėmimo bausmė, o suteikti galimybę susipažinti su atpažinimo 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 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 pažymėjo, 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 nurodytos „baudžiamosios veikos“ apskritai.

Tokiomis aplinkybėmis Teisingumo Teismas pažymėjo, jog Sprendime *Tele2 Sverige ir Watson ir kt.*[45] 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 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.

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 ir nustatyti „baudžiamąsias veikas“ apskritai, taip pat vykdyti baudžiamąjį persekiojimą už jas, ir nereikalaujama, kad šios nusikalstamos veikos būtų kvalifikuojamos kaip „sunkios“.

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)

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) (byla *Privacy International*, C-623/17), *Conseil d'État* (Valstybės Taryba, Prancūzija) (byla *La Quadrature du Net ir kt.*, sujungtos bylos C-511/18 ir C-512/18) ir *Cour constitutionnelle* (Konstitucinis Teismas, Belgija) (byla *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 numatoma elektroninių ryšių paslaugų teikėjų pareiga perduoti valdžios institucijai arba bendrai ir nediferencijuotai saugoti naudotojų srauto ir vietos nustatymo duomenis, teisėtumo.

Dviejuose 2020 m. spalio 6 d. didžiosios kolegijos sprendimuose Teisingumo Teismas visų pirma nusprendė, kad nacionalinės teisės aktai, kuriais elektroninių ryšių paslaugų

[45] 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).

teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis arba dėl nurodyto tikslo perduoti šiuos duomenis nacionalinėms saugumo ir žvalgybos tarnyboms, patenka į Direktyvos 2002/58 taikymo sritį.

Be to, Teisingumo Teismas priminė, kad pagal Direktyvą 2002/58[46] 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[47], apimtį, tik laikantis bendrųjų Sąjungos teisės principų, įskaitant proporcingumo principą, ir Chartijoje[48] garantuojamų pagrindinių teisių.

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 *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 lemia ypač didelius Chartijos garantuojamų pagrindinių teisių suvaržymus, nors asmenų, kurių duomenys tvarkomi, elgesys nėra susijęs su nagrinėjamais teisės aktais siekiamu tikslu. Pagal analogiją Teisingumo Teismas išaiškino BDAR 23 straipsnio 1 dalį, siejamą su Chartija, kaip draudžiančią 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.

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 laikotarpiu, neviršijančiu to, kas griežtai būtina, turi būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar

[46] Direktyvos 2002/58 15 straipsnio 1 ir 3 dalys.
[47] Direktyvos 2002/58 5 straipsnio 1 dalis.
[48] Konkrečiai kalbant, Chartijos 7, 8 ir 11 straipsniuose ir 52 straipsnio 1 dalyje.

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.

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.

Teisingumo Teismas taip pat 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.

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 pasinaudojus Sąjungos teisei prieštaraujančiu duomenų saugojimu, 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 pateikti pastabų dėl šių įrodymų.

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[49] 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.*[50], 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

[49] Konkrečiau kalbant, su Direktyvos 2002/58 15 straipsnio 1 dalimi, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi.
[50] 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).

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.

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 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.

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, taip pat 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 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.

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.

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 įvairių nagrinėjamų interesų ir teisių suderinimui užtikrinti. 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 dėl to jis turi būti apsaugotas nuo bet kokios išorinės įtakos.

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 kalbant, baudžiamojoje srityje nepriklausomumo reikalavimas reiškia, kad už šią išankstinę kontrolę atsakinga institucija, pirma, nedalyvauja vykdant nagrinėjamą baudžiamąjį tyrimą ir, antra, turi būti nešališka baudžiamojo proceso šalių atžvilgiu. Taip nėra prokuratūros, kuri, kaip Estijos prokuratūra, vadovauja ikiteisminiam tyrimui ir prireikus palaiko valstybinį kaltinimą, atveju. Vadinasi, prokuratūra negali atlikti minėtos išankstinės kontrolės.

2022 m. balandžio 5 d. didžiosios kolegijos Sprendimas „Commissioner of An Garda Síochána ir kt.“ (C-140/20, EU:C:2022:258)

Šioje byloje *Supreme Court* (Aukščiausiasis Teismas, Airija) pateikė prašymą priimti prejudicinį sprendimą vykstant civiliniam procesui, kurį inicijavo asmuo, nuteistas iki gyvos galvos už Airijoje įvykdytą nužudymą. Tas asmuo ginčijo kai kurių nacionalinio įstatymo dėl naudojantis elektroniniais ryšiais gautų duomenų saugojimo nuostatų atitiktį Sąjungos teisei. Pagal tą įstatymą elektroninių ryšių paslaugų teikėjai saugojo su kaltinamojo telefoniniais skambučiais susijusius srauto ir vietos nustatymo duomenis ir suteikė teisėsaugos institucijoms prieigą prie jų. Prašymą priimti prejudicinį sprendimą pateikusiam teismui abejonių kilo, be kita ko, dėl bendro ir nediferencijuoto tokių duomenų saugojimo kovos su sunkiais nusikaltimais tikslu suderinamumo su Direktyva 2002/58, siejama su Chartija.

Teisingumo Teismo didžioji kolegija savo sprendimu patvirtino Sprendime *La Quadrature du Net ir kt.*[51] suformuotą jurisprudenciją ir patikslino jos apimtį, primindama, kad neleidžiama bendrai ir nediferencijuojant saugoti elektroninių ryšių srauto ir vietos nustatymo duomenų kovos su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencijos tikslais. Teisingumo Teismas policijos pareigūno atžvilgiu taip pat patvirtino Sprendime *Prokuratuur (Prieigos prie elektroninių ryšių duomenų sąlygos)*[52] suformuotą jurisprudenciją, be kita ko, dėl pareigos kompetentingų nacionalinių institucijų prieigai prie minėtų saugomų duomenų taikyti išankstinę kontrolę, kurią atliktų teismas arba nepriklausoma administracinė institucija.

[51] 2020 m. spalio 6 d. Sprendimas *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791).
[52] 2021 m. kovo 2 d. Sprendimas *Prokuratuur (Prieigos prie elektroninių ryšių duomenų sąlygos)* (C-746/18, EU:C:2021:152).

Teisingumo Teismas nusprendė, pirma, kad pagal su Chartija siejamą Direktyvą 2002/58 draudžiamos teisėkūros priemonės, kuriomis prevenciškai, siekiant kovoti su sunkiais nusikaltimais ir užkirsti kelią didelei grėsmei visuomenės saugumui, numatoma bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis. Iš tiesų, atsižvelgiant, pirma, į atgrasomąjį poveikį naudojimuisi pagrindinėmis teisėmis[53], kurį gali sukelti toks saugojimas, ir, antra, į suvaržymo, kurį lemia toks duomenų saugojimas, dydį, šis saugojimas turi būti išimtis, o ne taisyklė šios direktyvos nustatytoje sistemoje, kad šie duomenys nebūtų sistemingai ir nuolat saugomi. Nusikalstamumas, net ypač sunkūs nusikaltimai, negali būti prilygintas grėsmei nacionaliniam saugumui, nes toks prilyginimas galėtų sukurti tarpinę nacionalinio saugumo ir visuomenės saugumo kategoriją, siekiant visuomenės saugumui taikyti nacionaliniam saugumui būdingus reikalavimus.

Priešingai, pagal su Chartija siejamą Direktyvą 2002/58 nedraudžiamos teisėkūros priemonės, kuriomis, siekiant kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui, numatomas tikslinis srauto ir vietos nustatymo duomenų saugojimas, kuris, remiantis objektyviais ir nediskriminaciniais veiksniais, ribojamas atsižvelgiant į duomenų subjektų kategorijas arba geografinius kriterijus laikotarpiu, neviršijančiu to, kas griežtai būtina, tačiau kurį galima pratęsti. Teisingumo Teismas pridūrė, kad tokia duomenų saugojimo priemonė, susijusi su vietomis ar infrastruktūra, kuriose reguliariai lankosi labai didelis asmenų skaičius, ar su strateginėmis vietomis, kaip antai oro uostais, stotimis, jūrų uostais arba rinkliavų zonomis, leidžia kompetentingoms institucijoms gauti informaciją apie asmenų, kurie naudojasi elektroninių ryšių priemone, buvimą šiose vietose ir daryti išvadas dėl jų buvimo ir veiklos minėtose vietose ar geografinėse zonose, siekiant kovoti su sunkiais nusikaltimais. Bet kuriuo atveju galimi sunkumai tiksliai apibrėžiant atvejus ir sąlygas, kuriomis galima vykdyti tikslinį saugojimą, nepateisina to, kad valstybės narės numato bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą.

Pagal šią direktyvą, aiškinamą atsižvelgiant į Chartiją, taip pat nedraudžiamos teisėkūros priemonės, kuriomis tais pačiais tikslais numatomas bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas laikotarpiu, neviršijančiu to, kas griežtai būtina, ir duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas. Dėl duomenų, susijusių su civiline tapatybe, Teisingumo Teismas konkrečiai nurodė, kad nei pagal Direktyvą 2002/58, nei pagal kokį nors kitą Sąjungos teisės aktą nedraudžiami nacionalinės teisės aktai, kuriais siekiama kovoti su sunkiais nusikaltimais ir pagal kuriuos elektroninių ryšių priemonės, kaip antai iš anksto apmokėtos SIM kortelės, įsigijimas siejamas su sąlyga, kad patikrinami oficialūs dokumentai, patvirtinantys pirkėjo tapatybę, ir kad pardavėjas registruoja juose esančią informaciją – pardavėjas prireikus privalo suteikti kompetentingoms nacionalinėms institucijoms prieigą prie tokios informacijos.

[53] Įtvirtintomis Chartijos 7–11 straipsniuose.

Tas pats pasakytina apie teisėkūros priemones kuriomis, siekiant kovoti su sunkiomis nusikalstamomis veikomis ir didele grėsme visuomenės saugumui, leidžiama kompetentingos institucijos, kuriai taikoma veiksminga teisminė kontrolė, sprendimu įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų, kuriuos turi šie paslaugų teikėjai, saugojimą (anglų k. *quick freeze*). Iš tiesų tik kova su sunkiais nusikaltimais ir *a fortiori* nacionalinio saugumo užtikrinimas gali pateisinti tokį duomenų saugojimą, su sąlyga, kad ši priemonė ir prieiga prie saugomų duomenų neviršija to, kas griežtai būtina. Teisingumo Teismas priminė, kad tokia priemonė gali apimti kitų asmenų nei tie, kurie įtariami planavę arba padarę sunkią nusikalstamą veiką ar keliantys grėsmę nacionaliniam saugumui, srauto ir vietos nustatymo duomenis, jeigu tie duomenys, remiantis objektyviais ir nediskriminaciniais veiksniais, gali padėti išaiškinti tokią nusikalstamą veiką ar grėsmę nacionaliniam saugumui; tai gali būti, pavyzdžiui, tokios nusikalstamos veikos aukos, jos socialinės ar profesinės aplinkos duomenys.

Vis dėlto Teisingumo Teismas nurodė, kad, taikant aiškias ir tikslias taisykles, visos minėtos priemonės turi užtikrinti, kad saugant nagrinėjamus duomenis būtų laikomasi su tokiu saugojimu susijusių materialinių ir procesinių sąlygų ir atitinkami asmenys turėtų veiksmingas garantijas nuo piktnaudžiavimo rizikos. Įvairios srauto ir vietos nustatymo duomenų saugojimo priemonės, atsižvelgiant į nacionalinio įstatymų leidėjo pasirinkimą ir laikantis to, kas griežtai būtina, gali būti taikomos kartu.

Be to, Teisingumo Teismas patikslino, kad kovos su sunkiais nusikaltimais tikslais suteikta prieiga prie srauto ir vietos nustatymo duomenų, kurie buvo saugomi bendrai ir nediferencijuojant, prieštarautų bendrojo intereso tikslų, kuriais remiantis galima būtų pateisinti pagal Direktyvą 2002/58 priimtą priemonę, hierarchijai. Iš tiesų tai reikštų, kad prieiga gali būti pateisinta mažesnės svarbos tikslu nei tas, kuriuo buvo grindžiamas saugojimas, t. y. nacionalinio saugumo užtikrinimas, dėl to kiltų grėsmė, kad draudimas bendrai ir nediferencijuojant saugoti duomenis kovos su sunkiais nusikaltimais tikslais galėtų tapti neveiksmingas.

Antra, Teisingumo Teismas nusprendė, kad pagal su Chartija siejamą Direktyvą 2002/58 draudžiami nacionalinės teisės aktai, pagal kuriuos, tiriant sunkius nusikaltimus ir vykdant baudžiamąjį persekiojimą už juos, policijos pateiktus prašymus leisti susipažinti su elektroninių ryšių paslaugų teikėjų saugomais duomenimis centralizuotai tvarko policijos pareigūnas, kuriam padeda policijoje įsteigtas padalinys, turintis tam tikrą autonomiją vykdant savo pareigas ir kurio sprendimams vėliau gali būti taikoma teisminė kontrolė. Iš tiesų toks pareigūnas neatitinka nepriklausomumo ir nešališkumo reikalavimų, taikomų administracinei institucijai, atliekančiai išankstinę kompetentingų nacionalinių institucijų pateiktų prašymų suteikti prieigą kontrolę, nes jis nėra trečiasis asmuo šių institucijų atžvilgiu. Be to, nors tokio pareigūno sprendimui gali būti taikoma *a posteriori* teisminė kontrolė, ji negali pakeisti nepriklausomos ir išankstinės, išskyrus tinkamai pagrįstus skubos atvejus, kontrolės.

Galiausiai, trečia, Teisingumo Teismas patvirtino savo jurisprudenciją, kuria remiantis pagal Sąjungos teisę nacionaliniam teismui draudžiama apriboti laiko atžvilgiu jo paties pagal nacionalinę teisę pripažinto negaliojančiu nacionalinės teisės akto, kuriuo elektroninių ryšių paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis, poveikį, kai toks teisės aktas nesuderinamas su Direktyva 2002/58. Atsižvelgdamas į tai Teisingumo Teismas priminė, kad, remiantis valstybių narių procesinės autonomijos principu, taip saugant duomenis gautų įrodymų priimtinumo klausimas sprendžiamas pagal nacionalinę teisę, laikantis, be kita ko, lygiavertiškumo ir veiksmingumo principų.

2022 m. rugsėjo 20 d. didžiosios kolegijos Sprendimas „VD ir SR“ (C-339/20 ir C-397/20, EU:C:2022:703)

Autorité des marchés financiers (AMF, Prancūzija) atlikus tyrimą, buvo iškeltos baudžiamosios bylos prieš du fizinius asmenis VD ir SR – jie apkaltinti prekyba vertybiniais popieriais pasinaudojant viešai neatskleista informacija, tokios veikos slėpimu ir bendrininkavimu ją atliekant, korupcija, taip pat pinigų plovimu. Atlikdama šį tyrimą AMF naudojo asmens duomenis iš VD ir SR pokalbių telefonu, gautus pagal Prancūzijos Pašto ir elektroninių ryšių kodeksą teikiant elektroninių ryšių paslaugas.

Kadangi dėl VD ir SR pradėti tyrimai buvo grindžiami AMF pateiktais srauto duomenimis, kiekvienas jų kreipėsi į *Cour d'appel de Paris* (Paryžiaus apeliacinis teismas, Prancūzija) ir, be kita ko, nurodė pagrindą, grindžiamą Direktyvos 2002/58 15 straipsnio 1 dalies, siejamos su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, pažeidimu. Remdamiesi jurisprudencija, suformuota Sprendime *Tele2 Sverige ir Watson ir kt.*[54], VD ir SR ginčijo tai, kad AMF, rinkdama minėtus duomenis, rėmėsi nagrinėjamomis nacionalinėmis nuostatomis, nors, anot jų, šios nuostatos, pirma, neatitiko Sąjungos teisės, nes jose buvo numatytas įpareigojimas bendrai ir nediferencijuojant saugoti prisijungimo duomenis, ir, antra, niekaip nebuvo apriboti AMF tyrėjų įgaliojimai gauti saugomus duomenis.

Dviem 2018 m. gruodžio 20 d. ir 2019 m. kovo 7 d. sprendimais *Cour d'appel de Paris* (Paryžiaus apeliacinis teismas) atmetė VD ir SR skundus. Siekdami atmesti minėtą pagrindą, bylą iš esmės nagrinėję teisėjai, be kita ko, rėmėsi tuo, kad pagal Piktnaudžiavimo rinka reglamentą[55] kompetentingoms valdžios institucijoms, jeigu tai leidžiama pagal nacionalinę teisę, galima reikalauti elektroninių ryšių paslaugų operatoriaus turimų srauto duomenų išklotinių, kai yra pagrindo įtarti, kad pažeistas prekybos vertybiniais popieriais pasinaudojant viešai neatskleista informacija draudimas ir jeigu tokios išklotinės gali būti svarbios atliekant tyrimą dėl šio pažeidimo.

---

54 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970).

55 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 596/2014 dėl piktnaudžiavimo rinka (Piktnaudžiavimo rinka reglamentas) ir kuriuo panaikinama Direktyva 2003/6 ir Komisijos direktyvos 2003/124/EB, 2003/125/EB ir 2004/72/EB (OL L 173, 2014, p. 1).

VD ir SR pateikė kasacinį skundą *Cour de cassation* (Kasacinis Teismas, Prancūzija), t. y. prašymą priimti prejudicinį sprendimą pateikusiam teismui.

Šiomis aplinkybėmis šiam teismui kilo klausimas dėl Direktyvos 2002/58 15 straipsnio 1 dalies, siejamos su Chartija, suderinimo su reikalavimais, kylančiais iš Piktnaudžiavimo rinka direktyvos[56] 12 straipsnio 2 dalies a ir d punktų ir Piktnaudžiavimo rinka reglamento 23 straipsnio 2 dalies g ir h punktų. Šis klausimas kilo dėl pagrindinėje byloje nagrinėjamų teisės aktų, pagal kuriuos elektroninių ryšių paslaugų operatoriams numatytas bendras ir nediferencijuotas srauto duomenų saugojimas vienus metus nuo įrašymo dienos, siekiant kovoti su piktnaudžiavimu rinka, įskaitant prekybą vertybiniais popieriais pasinaudojant viešai neatskleista informacija. Jeigu Teisingumo Teismas nuspręstų, kad pagrindinėje byloje nagrinėjami teisės aktai dėl prisijungimo duomenų saugojimo neatitinka Sąjungos teisės, prašymą priimti prejudicinį sprendimą pateikęs teismas iškėlė klausimą dėl laikino šių teisės aktų sukeliamų pasekmių išlaikymo, kad būtų išvengta teisinio nesaugumo ir leista anksčiau surinktus ir išsaugotus duomenis naudoti siekiant atskleisti prekybos vertybiniais popieriais pasinaudojant viešai neatskleista informacija operacijas ir vykdyti baudžiamąjį persekiojimą.

Savo sprendime Teisingumo Teismas (didžioji kolegija) nusprendė, kad siekiant kovoti su piktnaudžiavimu rinka draudžiama elektroninių ryšių paslaugų operatoriams prevenciškai vienus metus nuo įrašymo dienos bendrai ir nediferencijuojant saugoti srauto duomenis. Be to, jis patvirtino savo jurisprudenciją, pagal kurią remiantis Sąjungos teise nacionaliniam teismui draudžiama apriboti negaliojimo pripažinimo pasekmes laiko atžvilgiu, kiek tai susiję su nacionalinės teisės aktų nuostatomis, kurios nesuderinamos su Sąjungos teise.

Teisingumo Teismas pirmiausia priminė, kad aiškinant Sąjungos teisės nuostatą reikia atsižvelgti ne tik į jos formuluotę, bet ir į kontekstą, taip pat teisės akto, kuriame ji įtvirtinta, tikslus.

Dėl prejudiciniuose klausimuose nurodytų nuostatų formuluotės Teisingumo Teismas konstatavo, kad Piktnaudžiavimo rinka direktyvos 12 straipsnio 2 dalies d punkte nurodyta AMF teisė „reikalauti turimų telefoninių pokalbių ir duomenų srauto išklotinių“, o Piktnaudžiavimo rinka reglamento 23 straipsnio 2 dalies g ir h punktuose nurodyta šios institucijos teisė, pirma, „reikalauti investicinių įmonių, kredito institucijų ar finansų įstaigų turimų telefoninių pokalbių įrašų <...> ir duomenų išklotinių“ ir, antra, „reikalauti, jei leidžiama pagal nacionalinės teisės aktus, telekomunikacijų operatoriaus turimų duomenų išklotinių“. Anot Teisingumo Teismo, iš šių nuostatų formuluotės aiškiai matyti, kad jose tik bendrai apibrėžiami AMF įgaliojimai „reikalauti“, kad šie operatoriai pateiktų „turimas“ duomenų išklotines, o tai atitinka galimybę susipažinti su šiais duomenimis. Be to, nuoroda į minėtų operatorių „turimas“ duomenų išklotines leidžia

[56] 2003 m. sausio 28 d. Europos Parlamento ir Tarybos direktyva 2003/6/EB dėl prekybos vertybiniais popieriais, pasinaudojant viešai neatskleista informacija, ir manipuliavimo rinka (piktnaudžiavimo rinka) (OL L 96, 2003, p. 16; 2004 m. Specialusis leidimas lietuvių k., 6 sk., 4 t., p. 367).

suprasti, kad Sąjungos teisės aktų leidėjas neketino reglamentuoti nacionalinės teisės aktų leidėjo galimybės nustatyti pareigą saugoti tokias išklotines. Teisingumo Teismo teigimu, tokį aiškinimą, be kita ko, patvirtina ir minėtų nuostatų kontekstas, ir teisės akto, kuriame šios nuostatos yra, tikslai.

Dėl nuostatų, kurios nurodytos prejudiciniuose klausimuose, konteksto Teisingumo Teismas pažymėjo, kad nors pagal Piktnaudžiavimo rinka direktyvos ir Piktnaudžiavimo rinka reglamento taikytinas nuostatas[57] Sąjungos teisės aktų leidėjas ketino įpareigoti valstybes nares imtis reikiamų priemonių, kad už finansus atsakingos institucijos turėtų visas būtinas priemones, įgaliojimus ir išteklius, taip pat būtinus priežiūros ir tyrimo įgaliojimus, kad būtų užtikrintas jų uždavinių veiksmingumas, šiose nuostatose nieko nenurodyta nei dėl potencialios valstybių narių galimybės šiais tikslais nustatyti elektroninių ryšių operatoriams pareigą bendrai ir nediferencijuojant saugoti srauto duomenis, nei dėl sąlygų, kuriomis šie operatoriai turi saugoti šiuos duomenis, kad prireikus juos perduotų kompetentingoms institucijoms.

Dėl nagrinėjamais teisės aktais siekiamų tikslų Teisingumo Teismas pažymėjo, kad iš Piktnaudžiavimo rinka direktyvos ir Piktnaudžiavimo rinka reglamento[58] matyti, kad šiais teisės aktais siekiama užtikrinti Sąjungos finansų rinkų vientisumą ir sustiprinti investuotojų pasitikėjimą šiomis rinkomis, o šis pasitikėjimas grindžiamas, be kita ko, tuo, kad jiems būtų sudarytos vienodos sąlygos ir jie būtų apsaugoti nuo neteisėto viešai neatskleistos informacijos naudojimo. Taigi minėtuose teisės aktuose įtvirtintu prekybos vertybiniais popieriais pasinaudojant viešai neatskleista informacija draudimu[59] siekiama užtikrinti akcijų biržos sandorio šalių lygybę, išvengiant to, kad viena iš jų, žinanti viešai neatskleistą informaciją ir dėl to esanti palankesnėje padėtyje, palyginti su kitais investuotojais, iš to gautų naudos šios informacijos nežinančių asmenų sąskaita. Nors pagal Piktnaudžiavimo rinka reglamentą[60] prisijungimo duomenų išklotinės yra svarbus ir dažnai vienintelis įrodymas siekiant nustatyti ir įrodyti prekybos vertybiniais popieriais pasinaudojant viešai neatskleista informacija ir manipuliavimo rinka atvejus, vis dėlto šiame reglamente nurodomos tik elektroninių ryšių paslaugų operatorių „turimos“ išklotinės ir finansų srityje kompetentingos institucijos teisė „reikalauti“ iš šių operatorių pateikti „turimus“ duomenis. Taigi iš šio teksto tikrai nėra akivaizdu, kad taip Sąjungos teisės aktų leidėjas ketino pripažinti valstybėms narėms teisę nustatyti elektroninių ryšių paslaugų operatoriams bendrą pareigą saugoti duomenis. Darytina išvada, kad nei Piktnaudžiavimo rinka direktyva, nei Piktnaudžiavimo rinka reglamentas negali būti aiškinami taip, kad jie gali būti bendros pareigos saugoti elektroninių ryšių paslaugų teikėjų turimus srauto duomenis, kad finansų srityje kompetentinga institucija galėtų pasinaudoti jai pagal šiuo teisės aktus suteiktais įgaliojimais, teisinis pagrindas.

---

57 Atitinkamai Piktnaudžiavimo rinka direktyvos 12 straipsnio 1 dalis ir Piktnaudžiavimo rinka reglamento 23 straipsnio 3 dalis, siejama su jo 62 konstatuojamąja dalimi.

58 Atitinkamai Piktnaudžiavimo rinka direktyvos 2 ir 12 konstatuojamosios dalys ir Piktnaudžiavimo rinka reglamento 1 straipsnis, siejamas su jo 2 ir 24 konstatuojamosiomis dalimis.

59 Piktnaudžiavimo rinka direktyvos 2 straipsnio 1 dalis ir Piktnaudžiavimo rinka reglamento 8 straipsnio 1 dalis.

60 Piktnaudžiavimo rinka reglamento 62 konstatuojamoji dalis.

Toliau Teisingumo Teismas priminė, kad Direktyva 2002/58 yra teisės aktas, kuriuo reikia remtis asmens duomenų saugojimo ir apskritai jų tvarkymo srityje elektroninių ryšių sektoriuje, todėl jos aiškinimas taip pat taikomas elektroninių ryšių paslaugų operatorių turimoms duomenų išklotinėms, kurių iš jų gali reikalauti finansų srityje kompetentingos institucijos, kaip tai suprantama pagal Piktnaudžiavimo rinka direktyvą ir Piktnaudžiavimo rinka reglamentą[61]. Vadinasi, elektroninių ryšių paslaugų operatorių turimų duomenų išklotinių tvarkymo teisėtumas[62] turi būti vertinamas atsižvelgiant į Direktyvoje 2002/58 numatytas sąlygas ir šios direktyvos aiškinimą Teisingumo Teismo jurisprudencijoje.

Taigi Teisingumo Teismas nusprendė, kad pagal Piktnaudžiavimo rinka direktyvą ir Piktnaudžiavimo rinka reglamentą, siejamus su Direktyva 2002/58 ir atsižvelgiant į Chartiją, draudžiami teisės aktai, kuriuose, siekiant kovoti su piktnaudžiavimu rinka, apimančiu prekybą vertybiniais popieriais pasinaudojant viešai neatskleista informacija, prevenciškai numatyta elektroninių ryšių paslaugų operatorių pareiga vienus metus nuo įrašymo dienos bendrai ir nediferencijuojant saugoti srauto duomenis.

Galiausiai Teisingumo Teismas patvirtino savo jurisprudenciją, pagal kurią remiantis Sąjungos teise nacionaliniam teismui draudžiama laiko atžvilgiu apriboti akto pripažinimo negaliojančiu pasekmes, kai jam pagal nacionalinę teisę tenka tokia pareiga, atsižvelgiant į nacionalines nuostatas, pagal kurias, pirma, reikalaujama, kad elektroninių ryšių paslaugų operatoriai bendrai ir nediferencijuojant saugotų srauto duomenis, ir, antra, tokius duomenis leidžiama pateikti finansų srityje kompetentingai institucijai, prieš tai negavus teismo ar nepriklausomos administracinės institucijos leidimo, dėl šių nuostatų nesuderinamumo su Direktyva 2002/58, aiškinama atsižvelgiant į Chartiją. Atsižvelgdamas į tai Teisingumo Teismas priminė, kad, remiantis valstybių narių procesinės autonomijos principu, taip saugant duomenis gautų įrodymų priimtinumo klausimas sprendžiamas pagal nacionalinę teisę, laikantis, be kita ko, lygiavertiškumo ir veiksmingumo principų. Pagal pastarąjį principą reikalaujama, kad nacionalinis baudžiamųjų bylų teismas neatsižvelgtų į informaciją ir įrodymus, gautus atliekant su Sąjungos teise nesuderinamą bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, jeigu duomenų subjektai negali veiksmingai pateikti pastabų dėl šios informacijos ir įrodymų, kurie priklauso teisėjams nežinomai sričiai ir gali daryti lemiamą įtaką vertinant faktines aplinkybes.

2024 m. balandžio 30 d. plenarinės sesijos Sprendimas „La Quadrature du Net ir kt. (Asmens duomenys ir kova su intelektinės nuosavybės pažeidimais)“ (C-470/21, EU:C:2024:370)

Gavęs *Conseil d'État* (Valstybės Taryba, Prancūzija) prašymą priimti prejudicinį sprendimą, Teisingumo Teismas, posėdžiaudamas plenarinėje sesijoje, išplėtojo su

[61] Atitinkamai pagal Piktnaudžiavimo rinka direktyvos 11 straipsnį ir Piktnaudžiavimo rinka reglamento 22 straipsnį.

[62] Kaip tai suprantama pagal Piktnaudžiavimo rinka direktyvos 12 straipsnio 2 dalies d punktą ir Piktnaudžiavimo rinka reglamento 23 straipsnio 2 dalies g ir h punktus.

Direktyva 2002/58 susijusią jurisprudenciją ir pateikė paaiškinimų, pirma, dėl sąlygų, kuriomis elektroninių ryšių paslaugų teikėjų atliekamas bendras IP adresų saugojimas gali būti nelaikomas dideliu Chartijoje įtvirtintų teisių į privataus gyvenimo gerbimą, asmens duomenų apsaugą ir saviraiškos laisvę[63] suvaržymu, ir, antra, dėl viešosios valdžios institucijos galimybės susipažinti su tam tikrais laikantis tokių sąlygų saugomais asmens duomenimis, kovojant su internete padarytais intelektinės nuosavybės teisių pažeidimais.

Nagrinėjamu atveju keturios asociacijos pateikė Ministrui Pirmininkui (Prancūzija) prašymą panaikinti Dekretą dėl automatizuoto asmens duomenų tvarkymo[64]. Kadangi nebuvo priimtas sprendimas dėl šio prašymo, šios asociacijos pateikė *Conseil d'État* (Valstybės Taryba) ieškinį dėl implicitinio sprendimo atmesti prašymą panaikinimo. Jų teigimu, šis dekretas ir jo teisinį pagrindą sudarančios nuostatos[65] pažeidžia Sąjungos teisę.

Pagal Prancūzijos teisės aktus *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (Vyriausioji kūrinių platinimo ir teisių apsaugos internete valdyba, toliau – *Hadopi*), siekdama nustatyti asmenis, atsakingus už autorių ar gretutinių teisių pažeidimus internete, turi teisę susipažinti su tam tikrais duomenimis, kuriuos elektroninių ryšių paslaugų teikėjai privalo saugoti. Šie duomenys susiję su IP adresą, kurį prieš tai surinko teisių turėtojų organizacijos, atitinkančia duomenų subjekto civiline tapatybe. Nustačius IP adreso, naudojamo veiklai, susijusiai su tokiu pažeidimu, turėtoją, *Hadopi* vykdo vadinamąją „laipsniško reagavimo" procedūrą. Konkrečiai kalbant, ji turi teisę išsiųsti šiam asmeniui dvi rekomendacijas, kurios prilygsta įspėjimams, ir, jei veikla tęsiama, pranešimą, kuriame nurodoma, kad už vykdomą veiklą gali būti taikoma baudžiamoji atsakomybė. Galiausiai ji turi teisę kreiptis į prokuratūrą, kad šis asmuo būtų patrauktas baudžiamojon atsakomybėn[66].

Šiomis aplinkybėmis *Conseil d'État* (Valstybės Taryba) kreipėsi į Teisingumo Teismą dėl su Chartija siejamos Direktyvos 2002/58[67] išaiškinimo.

Pirma, dėl duomenų, susijusių su civiline tapatybe ir atitinkamais IP adresais, saugojimo Teisingumo Teismas pabrėžė, kad bet koks bendras ir nediferencijuotas IP adresų saugojimas nebūtinai yra didelis Chartijoje įtvirtintų teisių į privataus gyvenimo gerbimą, asmens duomenų apsaugą ir saviraiškos laisvę suvaržymas.

Pareiga užtikrinti tokį saugojimą gali būti pateisinama kovos su nusikalstamomis veikomis apskritai tikslu, jeigu iš tikrųjų atmetama galimybė, kad toks saugojimas lems

63 Chartijos 7, 8 ir 11 straipsniai.

64 2010 m. kovo 5 d. Dekretas Nr. 2010-236 dėl automatizuoto asmens duomenų tvarkymo, leidžiamo pagal Intelektinės nuosavybės kodekso L. 331-29 straipsnį „Kūrinių apsaugos internete priemonių administravimo sistema" (JORF, Nr. 56, tekstas Nr. 19, 2010 m. kovo 7 d.), iš dalies pakeistas 2017 m. gegužės 6 d. Dekretu Nr. 2017-924 dėl teisių administravimo institucijos atliekamo autorių teisių ir gretutinių teisių administravimo, kuriuo iš dalies keičiamas Intelektinės nuosavybės kodeksas (JORF, Nr. 109, tekstas Nr. 176, 2017 m. gegužės 10 d.).

65 Visų pirma Intelektinės nuosavybės kodekso L. 331-21 straipsnio trečia–penkta pastraipos.

66 Nuo 2022 m. sausio 1 d. *Hadopi* buvo sujungta su *Conseil supérieur de l'audiovisuel* (Aukščiausioji audiovizualinės žiniasklaidos taryba; toliau – CSA), kuri yra kita nepriklausoma valdžios institucija, kad būtų įsteigta *Autorité de régulation de la communication audiovisuelle et numérique* (Audiovizualinių ir skaitmeninių ryšių reguliavimo tarnyba; toliau – ARCOM). Vis dėlto laipsniško reagavimo procedūra iš esmės nepasikeitė.

67 Direktyvos 2002/58 15 straipsnio 1 dalies.

didelius duomenų subjekto privataus gyvenimo suvaržymus, nes galima padaryti tikslias išvadas apie šį asmenį, be kita ko, susiejant šiuos IP adresus su visais srauto ar vietos nustatymo duomenimis.

Taigi valstybė narė, ketinanti elektroninių ryšių paslaugų teikėjams nustatyti tokią pareigą, turi užtikrinti, kad šių duomenų saugojimo tvarka būtų tokia, kad neleistų padaryti tikslių išvadų apie duomenų subjektų privatų gyvenimą.

Teisingumo Teismas patikslino, kad saugojimo tvarka šiuo tikslu turi būti susijusi su pačiu saugojimo pobūdžiu, ji iš esmės turi būti organizuojama taip, kad būtų užtikrintas veiksmingas įvairių saugomų duomenų kategorijų atskyrimas. Taigi nacionalinės taisyklės, nustatančios tokią tvarką, turi užtikrinti, kad kiekviena duomenų kategorija, įskaitant duomenis, susijusius su civiline tapatybe ir IP adresais, būtų saugoma visiškai atskirai nuo kitų saugomų duomenų kategorijų ir kad jie būtų veiksmingai atskirti, naudojant saugią ir patikimą informatikos priemonę. Be to, kadangi šiose taisyklėse numatyta galimybė susieti saugomus IP adresus su duomenų subjekto civiline tapatybe, siekiant kovoti su nusikalstamomis veikomis, jos turi leisti susieti šiuos duomenis tik naudojant veiksmingas technines priemones, nepaneigiančias šių kategorijų duomenų atskyrimo veiksmingumo. Tokio atskyrimo patikimumą turi reguliariai tikrinti kita valdžios institucija nei ta, kuri siekia gauti prieigą. Jeigu taikytinuose nacionalinės teisės aktuose numatyti tokie griežti reikalavimai, dėl šio IP adresų saugojimo atsirandantis suvaržymas negali būti laikomas „dideliu“.

Taigi Teisingumo Teismas padarė išvadą, kad, esant teisės akto nuostatai, užtikrinančiai, kad joks duomenų derinys neleis daryti tikslių išvadų apie asmenų, kurių duomenys saugomi, privatų gyvenimą, pagal Direktyvą 2002/58, siejamą su Chartija, valstybei narei nedraudžiama nustatyti pareigos bendrai ir nediferencijuojant saugoti IP adresus laikotarpiu, kuris neviršija to, kas griežtai būtina, siekiant kovoti su nusikalstamomis veikomis apskritai.

Antra, dėl prieigos prie IP adresus atitinkančių civilinės tapatybės duomenų Teisingumo Teismas nusprendė, kad pagal Direktyvą 2002/58, siejamą su Chartija, iš principo nedraudžiami nacionalinės teisės aktai, pagal kuriuos viešosios valdžios institucijai leidžiama susipažinti su šiais elektroninių ryšių paslaugų teikėjų atskirai ir veiksmingai saugomais duomenimis tik tam, kad ši valdžios institucija galėtų nustatyti tokių adresų turėtojus, įtariamus padarius autorių ir gretutinių teisių pažeidimų internete, ir imtis priemonių jų atžvilgiu. Tokiu atveju pagal nacionalinės teisės aktus tokią prieigą turintiems pareigūnams turi būti draudžiama, pirma, bet kokia forma atskleisti informaciją apie rinkmenų, su kuriomis susipažino šie turėtojai, turinį, išskyrus atvejus, kai siekiama kreiptis į prokuratūrą, antra, sekti šių adresų turėtojų naršymo kelius ir, trečia, naudoti šiuos IP adresus kitais tikslais, nei ketinant imtis šių priemonių.

Šiomis aplinkybėmis Teisingumo Teismas, be kita ko, priminė, kad nors saviraiškos laisvė ir asmens duomenų konfidencialumas yra itin svarbūs, šios pagrindinės teisės nėra absoliučios. Iš tiesų, vertinant nagrinėjamas teises ir interesus, kartais vienus jų nusveria

kitos pagrindinės teisės ir bendrojo intereso reikalavimai, kaip antai viešosios tvarkos apsauga ir nusikalstamų veikų prevencija, arba kitų asmenų teisių ir laisvių apsauga. Taip visų pirma yra tuo atveju, kai minėtiems itin svarbiems atvejams teikiama pirmenybė gali pakenkti baudžiamojo tyrimo veiksmingumui, be kita ko, kai tampa neįmanoma arba pernelyg sudėtinga veiksmingai nustatyti nusikalstamą veiką padariusį asmenį ir skirti jam sankciją.

Šiuo klausimu Teisingumo Teismas taip pat rėmėsi savo jurisprudencija, pagal kurią, kiek tai susiję su kova su nusikalstamomis veikomis, pažeidžiančiomis autorių ar gretutines teises internete, aplinkybė, kad prieiga prie IP adresų gali būti vienintelė tyrimo priemonė, leidžianti nustatyti atitinkamo asmens tapatybę, rodo, kad šių adresų saugojimas ir prieiga prie jų yra griežtai būtini siekiamam tikslui įgyvendinti, taigi atitinka proporcingumo reikalavimą. Be to, tokios prieigos nesuteikimas reikštų realų sisteminio nebaudžiamumo už internete padarytas nusikalstamas veikas, kurių padarymą ar parengimą palengvina interneto ypatumai, pavojų. Toks pavojus yra reikšminga aplinkybė siekiant įvertinti, ar, nustatant įvairių esamų teisių ir interesų pusiausvyrą, teisių į privataus gyvenimo gerbimą, asmens duomenų apsaugą ir saviraiškos laisvę suvaržymas yra proporcinga priemonė, atsižvelgiant į tikslą kovoti su nusikalstamomis veikomis.

Trečia, priimdamas sprendimą dėl to, ar viešosios valdžios institucijos prieiga prie IP adresą atitinkančių civilinės tapatybės duomenų turi būti siejama su išankstine teismo arba nepriklausomos administracinės institucijos kontrole, Teisingumo Teismas nurodė, kad tokios kontrolės reikalavimas taikomas, kai nacionalinės teisės aktuose numatyta tokia prieiga kelia didelio duomenų subjekto pagrindinių teisių suvaržymo pavojų, nes ji leistų valdžios institucijai padaryti tikslias išvadas apie jo privatų gyvenimą ir prireikus nustatyti išsamų jo profilį. Ir atvirkščiai, šis išankstinės kontrolės reikalavimas netaikomas, kai pagrindinių teisių suvaržymas negali būti kvalifikuojamas kaip didelis.

Šiuo klausimu Teisingumo Teismas patikslino, kad tuo atveju, kai taikomas saugojimo mechanizmas, kuriuo užtikrinamas įvairių saugomų duomenų kategorijų atskyrimas, valdžios institucijos prieigai prie IP adresus atitinkančių civilinės tapatybės duomenų iš principo netaikomas išankstinės kontrolės reikalavimas. Iš tiesų tokia prieiga, vien siekiant nustatyti IP adreso turėtojo tapatybę, paprastai nėra didelis minėtų teisių suvaržymas.

Vis dėlto Teisingumo Teismas neatmetė galimybės, kad, esant netipinėms situacijoms, viešosios valdžios institucija per tokią procedūrą, kaip pagrindinėje byloje nagrinėjama laipsniško reagavimo procedūra, gali padaryti tikslias išvadas apie duomenų subjekto privatų gyvenimą, be kita ko, kai jis pakartotinai ar net dideliu mastu lygiarangių tinkluose vykdo autorių teises ar gretutines teises pažeidžiančią veiklą, susijusią su saugomais konkrečių rūšių kūriniais, galinčiais atskleisti informaciją (tam tikrais atvejais jautrią) apie minėto asmens privatų gyvenimą.

Nagrinėjamu atveju IP adreso turėtojui toks pavojus gali kilti ypač tada, kai valdžios institucija turi nuspręsti, ar kreiptis į prokuratūrą dėl jo patraukimo baudžiamojon atsakomybėn. Iš tiesų teisės į privataus gyvenimo gerbimą pažeidimo intensyvumas gali didėti, kai nuosekliai vykdoma laipsniško reagavimo procedūra pereina įvairius ją sudarančius etapus. Kompetentingos institucijos prieiga prie visų per įvairius šios procedūros etapus gautų duomenų apie duomenų subjektą, susiejant šiuos duomenis, gali leisti padaryti tikslias išvadas apie jo gyvenimą. Taigi nacionalinės teisės aktuose turi būti numatyta, kad išankstinę kontrolę reikia atlikti prieš valdžios institucijai susiejant civilinės tapatybės duomenis su visais kitais duomenimis ir prieš išsiunčiant pranešimą, kuriame konstatuota, kad asmuo padarė veiksmus, už kuriuos gali būti taikoma baudžiamoji atsakomybė. Be to, vykdant šią kontrolę turi būti išsaugotas laipsniško reagavimo procedūros veiksmingumas, visų pirma leidžiant nustatyti atvejus, kai nagrinėjamas neteisėtas elgesys gali pasikartoti iš naujo. Šiuo tikslu ši procedūra turi būti organizuojama ir struktūrizuota taip, kad asmenys, atsakingi už faktinių aplinkybių nagrinėjimą kompetentingoje valdžios institucijoje, automatiškai negalėtų susieti asmens civilinės tapatybės duomenų, atitinkančių iš anksto internete surinktus IP adresus, su jos jau turima informacija, kuri leistų padaryti tikslias išvadas apie šio asmens privatų gyvenimą.

Be to, dėl išankstinės kontrolės dalyko Teisingumo Teismas pažymėjo, kad tais atvejais, kai duomenų subjektas įtariamas padaręs nusikalstamą veiką, priskiriamą prie nusikalstamų veikų apskritai, teismas arba nepriklausoma administracinė institucija, atsakinga už šią kontrolę, turi atsisakyti leisti susipažinti su duomenimis, jeigu tai leistų prašančiai valdžios institucijai padaryti tikslias išvadas apie minėto asmens privatų gyvenimą. Vis dėlto net prieiga, leidžianti padaryti tokias tikslias išvadas, turėtų būti leidžiama tais atvejais, kai įtariama, kad duomenų subjektas padarė nusikaltimus, atitinkamos valstybės narės kvalifikuojamus kaip pažeidžiančius pagrindinį visuomenės interesą, taigi priskiriamus prie sunkių nusikaltimų.

Teisingumo Teismas taip pat patikslino, kad išankstinė kontrolė jokiu būdu negali būti visiškai automatizuota, nes, kiek tai susiję su baudžiamuoju tyrimu, vykdant tokią kontrolę reikia užtikrinti, pirma, teisėtų interesų, susijusių su kova su nusikalstamumu, ir, antra, privataus gyvenimo gerbimo ir asmens duomenų apsaugos pusiausvyrą. Siekiant užtikrinti tokią pusiausvyrą būtinas fizinio asmens įsikišimas, juo labiau kad dėl nagrinėjamo duomenų tvarkymo automatizuoto pobūdžio ir didelio masto kyla pavojus privačiam gyvenimui.

Taigi Teisingumo Teismas padarė išvadą, kad galimybė asmenims, atsakingiems už minėtos valdžios institucijos atliekamą faktinių aplinkybių nagrinėjimą, susieti IP adresus atitinkančius civilinės tapatybės duomenis su rinkmenomis, kuriose yra duomenų, leidžiančių nustatyti saugomų kūrinių, kurių padarymas prieinamų internete pateisina teisių turėtojų organizacijų atliekamą IP adresų rinkimą, pavadinimus, jeigu tas pats asmuo vėl pradeda vykdyti veiklą, kuria pažeidžiamos autorių ar gretutinės teisės, būtų suteikiama su sąlyga, kad taikoma teismo arba nepriklausomos administracinės

institucijos kontrolė. Ši kontrolė negali būti visiškai automatizuota ir turi būti atlikta prieš susiejant duomenis su rinkmenomis, nes tokiais atvejais gali būti įmanoma padaryti tikslias išvadas apie asmens, kurio IP adresas buvo naudojamas veiklai, galinčiai pažeisti autorių ar gretutines teises, privatų gyvenimą.

Galiausiai, ketvirta, Teisingumo Teismas pažymėjo būtinumą, kad valdžios institucijos naudojamą duomenų tvarkymo sistemą reguliariai tikrintų nepriklausoma įstaiga, kuri yra su ta institucija nesusijusi trečioji šalis. Šios kontrolės tikslas – patikrinti sistemos vientisumą, įskaitant veiksmingas apsaugos priemones nuo piktnaudžiavimo pavojaus ir nuo bet kokios neteisėtos prieigos prie tų duomenų ar jų neteisėto naudojimo, taip pat jos veiksmingumą ir patikimumą nustatant galimus trūkumus.

Šiuo klausimu Teisingumo Teismas pažymėjo, kad nagrinėjamu atveju automatizuotas asmens duomenų tvarkymas, kurį atlieka valdžios institucija, remdamasi informacija, susijusia su teisių turėtojų organizacijų nustatytais intelektinės nuosavybės teisių pažeidimais, gali būti susijęs su tam tikru klaidingų rezultatų skaičiumi ir ypač pavojumi, kad trečiosios šalys gali pasisavinti potencialiai labai didelį kiekį asmens duomenų piktnaudžiavimo ar neteisėtais tikslais. Be to, jis pridūrė, kad toks duomenų tvarkymas turi atitikti specialias asmens duomenų tvarkymo taisykles, numatytas Direktyvoje 2016/680. Iš tiesų nagrinėjamu atveju, nors pagal taikytiną nacionalinę teisę valdžios institucija neturi įgaliojimų priimti sprendimų, vykstant vadinamajai laipsniško reagavimo procedūrai, ji turi būti laikoma „valdžios institucija“, dalyvaujančia nusikalstamų veikų prevencijos ir atskleidimo veikloje, taigi patenka į direktyvos taikymo sritį. Tokioje procedūroje dalyvaujantiems asmenims turi būti suteiktos visos Direktyvoje 2016/680 numatytos materialinės ir procedūrinės garantijos, o prašymą priimti prejudicinį sprendimą pateikęs teismas turi patikrinti, ar jos numatytos nacionalinės teisės aktuose.

2. Asmens duomenų tvarkymas baudžiamosiose bylose

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[68] 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 būti 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[69].

Šiomis aplinkybėmis Vysbadeno administracinis teismas nusprendė kreiptis į Teisingumo Teismą dėl *ne bis in idem* principo taikymo, 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 kaip nedraudžiančios 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.

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[70]. 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*

---

68 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).

69 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).

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

principas[71]. Toks valstybių narių institucijų atliekamas duomenų tvarkymas gali būti būtinas būtent siekiant patikrinti, ar taikytinas minėtas principas.

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, 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[72].

Kita vertus, kai *ne bis in idem* principas taikomas, Interpolo raudonajame pranešime nurodytų asmens duomenų įrašymas į valstybių narių ieškomų asmenų sąrašus nebėra būtinas, 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 pridėta informacija, kad atitinkamas asmuo nebegali būti persekiojamas valstybėje narėje ar susitariančiojoje valstybėje už tas pačias veikas, nes taikomas *ne bis in idem* principas.

2022 m. birželio 21 d. didžiosios kolegijos Sprendimas „Ligue des droits humains“ (C-817/19, EU:C:2022:491)

Šioje byloje (taip pat žr. I skyriaus 1 skirsnį „Sąjungos antrinės teisės suderinamumas su teise į asmens duomenų apsaugą“) patvirtinęs PNR direktyvos galiojimą, Teisingumo Teismas patikslino kai kurių jos nuostatų aiškinimą[73].

Pirma, jis pažymėjo, kad direktyvoje išsamiai išvardyti tikslai, kurių siekiama tvarkant PNR duomenis. Taigi šia direktyva draudžiami nacionalinės teisės aktai, pagal kuriuos PNR duomenis leidžiama tvarkyti kitais tikslais nei kova su teroristiniais ir sunkiais nusikaltimais. Nacionalinės teisės aktai, kuriuose žvalgybos ir saugumo tarnybų atliekama stebėjimo veikla nurodoma kaip PNR duomenų tvarkymo tikslas, gali paneigti išsamų šio tikslų sąrašo pobūdį. PNR direktyva sukurta sistema taip pat negali būti skirta sienų kontrolei gerinti ir kovai su nelegalia imigracija. Iš to taip pat išplaukia, kad PNR duomenys negali būti saugomi vienoje duomenų bazėje, kurioje būtų galima atlikti paiešką tiek PNR direktyvoje numatytais, tiek kitais tikslais.

Antra, Teisingumo Teismas paaiškino nepriklausomos nacionalinės valdžios institucijos, kompetentingos patikrinti, ar įvykdytos PNR duomenų atskleidimo sąlygos, kad vėliau jie

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

72 Žr. Direktyvos 2016/680 1 straipsnio 1 dalį ir 8 straipsnio 1 dalį

73 Konkrečiai kalbant, PNR direktyvos 2 straipsnio „[Direktyvos] taikymas ES vidaus skrydžiams“, 6 straipsnio „PNR duomenų tvarkymas“ ir 12 straipsnio „Duomenų saugojimo laikotarpis ir nuasmeninimas“.

galėtų būti įvertinti ir būtų patvirtintas toks atskleidimas, sąvoką. Konkrečiai kalbant, institucija, įsteigta kaip informacijos apie keleivius skyrius (IKS), negali būti laikoma tokia nepriklausoma institucija, nes neturi trečiojo asmens statuso prieigos prie duomenų prašančios institucijos atžvilgiu. Iš tiesų, kadangi IKS darbuotojai gali būti valdžios institucijų deleguoti tarnautojai, jis neišvengiamai susijęs su šiomis valdžios institucijomis. Taigi pagal PNR direktyvą draudžiami nacionalinės teisės aktai, pagal kuriuos institucija, įsteigta kaip IKS, taip pat yra kompetentinga nacionalinė institucija, įgaliota patvirtinti PNR duomenų atskleidimą, praėjus šešių mėnesių laikotarpiui po šių duomenų perdavimo IKS.

Trečia, dėl PNR duomenų saugojimo termino Teisingumo Teismas nusprendė, kad pagal PNR direktyvos 12 straipsnį, siejamą su Chartijos 7, 8 straipsniais ir 52 straipsnio 1 dalimi, draudžiami nacionalinės teisės aktai, kuriuose numatyta bendra penkerių metų šių duomenų saugojimo trukmė, vienodai taikoma visiems oro transporto keleiviams.

Iš tiesų, Teisingumo Teismo teigimu, pasibaigus pirminiam šešių mėnesių saugojimo laikotarpiui, neatrodo, kad PNR duomenų saugojimas apsiriboja tuo, kas griežtai būtina, kiek tai susiję su oro transporto keleiviais, dėl kurių nei išankstinis vertinimas, nei galimi patikrinimai, atlikti per pirminį šešių mėnesių saugojimo laikotarpį, nei kitos aplinkybės neatskleidė objektyvių duomenų (pavyzdžiui, kad egzistuoja atitinkamų keleivių teigiama PNR duomenų atitiktis, patikrinta atliekant išankstinį vertinimą), kuriais remiantis galima nustatyti teroristinių nusikaltimų ar sunkių nusikaltimų, kurie objektyviai (bent netiesiogiai) susiję su šių keleivių kelione lėktuvu, riziką. Tačiau jis nustatė, kad visų oro transporto keleivių, kuriems taikoma šioje direktyvoje nustatyta sistema, PNR duomenų saugojimas pirminiu šešių mėnesių laikotarpiu iš esmės neviršija to, kas griežtai būtina.

Ketvirta, Teisingumo Teismas pateikė gaires dėl galimo PNR direktyvos taikymo kitoms transporto rūšims, vežančioms keleivius Sąjungoje, siekiant kovoti su teroristiniais ir sunkiais nusikaltimais. Pagal direktyvą, siejamą su ESS 3 straipsnio 2 dalimi, SESV 67 straipsnio 2 dalimi ir Chartijos 45 straipsniu, draudžiama tokia PNR duomenų perdavimo ir tvarkymo sistema, kuri yra susijusi su vežimu kitomis transporto priemonėmis Sąjungos viduje, nesant tikros, esamos ar numatomos terorizmo grėsmės, kuri kyla atitinkamai valstybei narei. Tokiu atveju, kaip ir kalbant apie ES vidaus skrydžius, pagal PNR direktyvą nustatyta sistema turi būti taikoma tik PNR duomenims, susijusiems su vežimu, be kita ko, tam tikrais maršrutais, kelionių schemomis, traukinių stotimis ar jūrų uostais, dėl kurių yra duomenų, galinčių pateisinti tokį taikymą. Atitinkama valstybė narė turi atrinkti vežimo būdus, dėl kurių tokia informacija egzistuoja, ir reguliariai peržiūrėti minėtą taikymą, atsižvelgdama į jų atranką pateisinusių sąlygų pokyčius.

IV. Asmens duomenų perdavimas į trečiąsias šalis

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

Šioje byloje (taip pat žr. II skyriaus 3 skirsnį „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.

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 draudžiantis 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.

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

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) savo 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/EB[74] Komisija konstatavo, jog pagal „saugaus uosto“ (anglų k. *safe harbour*)[75] 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

[74] 2000 m. liepos 26 d. Komisijos sprendimas 2000/520/EB dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“ (OL L 215, 2000, p. 7; 2004 m. specialusis leidimas lietuvių k., 16 sk., 1 t., p. 119).

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

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.

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 buvo pažeisti 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.

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. Teisingumo Teismas padarė išvadą, kad Sprendimo 2000/520 1 ir 3 straipsnių negaliojimas turi įtakos viso šio sprendimo galiojimui.

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 egzistuoja didelis neteisėtos prieigos prie šių duomenų pavojus.

Maža to, visų pirma pagrindinės teisės į privataus gyvenimo gerbimą apsauga Sąjungos lygiu reikalauja, kad nukrypti nuo asmens duomenų apsaugos leidžiančios nuostatos ir šios apsaugos apribojimai neviršytų to, kas yra griežtai būtina. Nėra apribotas tuo, kas griežtai būtina, toks reglamentavimas, kuris apskritai leidžia saugoti visų asmenų, kurių duomenys buvo perduoti iš Sąjungos, visus asmens duomenis nediferencijuojant, nenustatant jokių apribojimų arba išimčių pagal siekiamą tikslą ir nenumatant objektyvių kriterijų, leidžiančių nubrėžti ribas valstybės institucijų prieigai prie duomenų ir jų vėlesniam naudojimui konkrečiais, griežtai ribojamais tikslais, galinčiais pateisinti

prieigos prie šių duomenų ir jų naudojimo sukeliamą teisių apribojimą. Konkrečiai kalbant, teisės aktai, leidžiantys valstybės institucijoms apskritai susipažinti su elektroninės komunikacijos turiniu, kelia pavojų pagrindinės teisės į privatų gyvenimą esmei. Be to, reglamentavimu, nenumatančiu asmeniui jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti, nepaisoma Chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės.

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 Chartija, konkrečiai – su nuostatomis, susijusiomis su privataus gyvenimo gerbimu ir asmens duomenų apsauga.

Europos Sąjunga ir Kanada vedė derybas dėl susitarimo dėl oro transporto keleivių duomenų perdavimo ir tvarkymo (susitarimas dėl PNR); 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, jame numatyta ir teisė susipažinti su duomenimis, juos ištaisyti ir pašalinti, taip pat galimybė pateikti administracinį skundą ar ieškinį.

PNR duomenys, apie kuriuos kalbama numatytame sudaryti susitarime, be oro keleivių pavardžių, vardų ir 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, 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.

Be to, jis pabrėžė, 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 transporto 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.).

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.

Antra, Teisingumo Teismas laikėsi nuomonės, kad, oro transporto keleiviams išvykus iš Kanados, numatytame sudaryti susitarime nurodytas visų keleivių PNR duomenų kaupimas neapsiriboja tuo, kas griežtai būtina. Kiek tai susiję su oro transporto 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 transporto keleivių, dėl kurių buvo objektyvių įrodymų, leidžiančių manyti, kad jie netgi išvykę iš Kanados galėjo kelti riziką kovojant su terorizmu ir sunkiais tarpvalstybiniais nusikaltimais, PNR duomenis leidžiama saugoti ir jiems išvykus iš šios šalies, netgi penkerius metus.

Trečia, Teisingumo Teismas konstatavo, kad Chartijos 7 straipsnyje įtvirtinta teisė į privatų gyvenimą reiškia, jog duomenų subjektas 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 numatytam sudaryti susitarimui svarbu, kad oro transporto 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 transporto 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 transporto keleivius reikia informuoti individualiai. Tas pats taikytina tuo atveju, kai su oro transporto 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.

2020 m. liepos 16 d. didžiosios kolegijos Sprendimas „Facebook Ireland ir Schrems“ (C-311/18, EU:C:2020:559)

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[76]. 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[77]. Be to, BDAR aiškiai nustatytos sąlygos, kuriomis galima atlikti tokį perdavimą nesant sprendimo dėl tinkamumo arba tinkamų apsaugos priemonių[78].

Maximillian Schrems yra Austrijoje gyvenantis šios šalies pilietis; nuo 2008 m. jis yra *Facebook* vartotojas. M. Schrems, kaip ir kitų Sąjungoje 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

[76] BDAR 45 straipsnis.
[77] BDAR 46 straipsnio 1 dalis ir 2 dalies c punktas.
[78] BDAR 49 straipsnis.

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[79] 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 I*)[80].

Paskelbus Sprendimą *Schrems I* 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/ES[81] priede pateiktomis standartinėmis apsaugos sąlygomis, arba uždrausti tokį perdavimą ateityje. 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 sprendimą. Pradėjus šią procedūrą, Komisija priėmė Sprendimą (ES) 2016/1250 dėl ES ir JAV duomenų apsaugos skydo užtikrinamos apsaugos tinkamumo[82].

Prašymą priimti prejudicinį sprendimą pateikęs teismas Teisingumo Teismui uždavė klausimų dėl BDAR taikytinumo asmens duomenų perdavimui remiantis Sprendime 2010/87 pateiktomis standartinėmis apsaugos sąlygomis, dėl pagal šį reglamentą 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 konstatavo, kad išnagrinėjus Sprendimą 2010/87 atsižvelgiant į Chartiją nenustatyta nieko, kas galėtų paveikti jo galiojimą. Tačiau jis pripažino Sprendimą 2016/1250 negaliojančiu.

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

[79] 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).

[80] 2015 m. spalio 6 d. Sprendimas *Schrems* (C-362/14, EU:C:2015:650).

[81] 2010 m. vasario 5 d. Komisijos sprendimas dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas (OL L 39, 2010, p. 5), iš dalies pakeistas 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimu (ES) 2016/2297 (OL L 344, 2016, p. 100).

[82] 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46 (OL L 207, 2016, p. 1).

tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais. Jis pažymėjo, jog tai, kad trečiosios šalies institucijos atlieka tokį duomenų tvarkymą, nereiškia, kad jis nepatenka į BDAR taikymo sritį.

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.

Dėl priežiūros institucijoms tokio perdavimo aplinkybėmis 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.

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.

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 visai nematyti, kad juose yra įtvirtintų įgaliojimų įgyvendinti šias programas apribojimų ar garantijų ne JAV piliečiams, kuriems gali būti taikomos šios programos. Teisingumo Teismas pridūrė, kad nors tuose teisės aktuose numatyti reikalavimai, kurių turi laikytis JAV valdžios institucijos įgyvendindamos atitinkamas stebėjimo programas, pagal juos duomenų subjektams nesuteikiama įgyvendinamų teisių, kuriomis jie galėtų remtis teismuose JAV valdžios institucijų atžvilgiu.

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.

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 skyriaus 1 skirsnį „Bendrojo reglamentavimo taikymo sritis“ ir 3 skirsnį „Sąvoka „asmens duomenų tvarkymas“) Teisingumo Teismas patikslino Direktyvoje 95/46 numatytos teisės susipažinti su asmens duomenimis ir teisės prieštarauti dėl jų tvarkymo internete apimtį.

Nagrinėdamas klausimą 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 tą asmenį. Teisingumo Teismas pažymėjo, kad tokia pareiga gali kilti ir tais atvejais, kai šis asmenvardis arba informacija nėra prieš tai ištrinti arba tuo pačiu metu ištrinami iš šių tinklalapių, net jei atitinkami duomenys šiuose tinklalapiuose paskelbti teisėtai.

Be to, paklaustas, ar pagal šią direktyvą duomenų subjektas 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. Todėl jei duomenų subjekto 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. Šiomis aplinkybėmis duomenų subjekto teisės į tai, kad su juo susijusi informacija rezultatų sąrašuose nebebūtų siejama su jo asmenvardžiu, konstatavimas nesiejamas su nustatymu, kad atitinkamos informacijos įtraukimas į rezultatų sąrašą sukelia duomenų subjektui neigiamų padarinių.

Galiausiai Teisingumo Teismas pažymėjo: kadangi duomenų subjektas, 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, kai dėl konkrečių aplinkybių, kaip antai šio subjekto vaidmens viešajame gyvenime, paaiškėtų, kad šių pagrindinių teisių apribojimą pateisina viršesnis šios visuomenės interesas turėti dėl įtraukimo į rezultatų sąrašus suteiktą prieigą prie atitinkamos informacijos.

2. Asmens duomenų tvarkymas ir intelektinės nuosavybės teisės

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

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. viena vertus, teisės į privataus gyvenimo gerbimą ir, kita vertus, 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/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva)[83], Direktyva 2001/29/EB dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo[84], Direktyva 2004/48/EB dėl intelektinės nuosavybės teisių gynimo[85] ir Direktyva 2002/58 neįpareigoja valstybių narių, užtikrinant veiksmingą autorių teisių apsaugą, numatyti pareigos 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 ji atitiktų šias direktyvas, bet ir nesivadovauti tokiu jų aiškinimu, kuris pažeistų minėtas pagrindines teises arba kitus bendruosius Bendrijos teisės principus, kaip antai proporcingumo principą.

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*

[83] 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB 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).

[84] 2001 m. gegužės 22 d. Europos Parlamento ir Tarybos direktyva 2001/29/EB 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).

[85] 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos direktyva 2004/48/EB dėl intelektinės nuosavybės teisių gynimo (OL L 157, 2004, p. 45; 2004 m. specialusis leidimas lietuvių k., 17 sk., 2 t., p. 32).

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 pagal Direktyvos 2004/48 8 straipsnio 3 dalį, siejamą su Direktyvos 2002/58 15 straipsnio 1 dalimi, valstybėms narėms nedraudžiama įtvirtinti pareigos perduoti asmens duomenis privatiems asmenims, kad civilines bylas nagrinėjančiuose teismuose būtų galima iškelti bylą dėl autorių teisių pažeidimų, 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.

Šiuo aspektu jis konstatavo, kad pagal nagrinėjamą nacionalinės teisės aktą, be kita ko, reikalaujama, jog tam, kad būtų galima nustatyti įpareigojimą atskleisti aptariamus duomenis, turi egzistuoti faktiniai intelektinės nuosavybės teisės į kūrinį pažeidimo 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.

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.

3. Asmens duomenų pašalinimas

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

Šiame sprendime Teisingumo Teismo didžioji kolegija patikslino paieškos sistemos eksploatuotojo pareigas, susijusias su prašymu pašalinti nuorodas, turinčias jautrių duomenų.

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[86]. Kiek tai susiję su duomenų apie nusikalstamas veikas, apkaltinamuosius nuosprendžius arba kardomąsias priemones tvarkymu, pažymėtina, kad tokius duomenis iš principo galima tvarkyti tik prižiūrint valdžios institucijai arba jeigu nacionalinėje teisėje yra numatytos tinkamos ir specialios apsaugos priemonės[87].

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.

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

[86] Direktyvos 95/46 8 straipsnio 1 dalis ir Reglamento 2016/679 9 straipsnio 1 dalis.
[87] Direktyvos 95/46 8 straipsnio 5 dalis ir Reglamento 2016/679 10 straipsnis.

apribojimai šiam eksploatuotojui taikomi tik dėl nuorodos teikimo, todėl įgyvendinami pagal duomenų subjekto pateiktą prašymą atliekant patikrinimą, prižiūrimą kompetentingų nacionalinių institucijų.

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[88], jeigu tokių nuorodų teikimas atitinka kitas asmens duomenų tvarkymo teisėtumo sąlygas, nebent šis asmuo dėl priežasčių, susijusių su jo konkrečia padėtimi, turi teisę prieštarauti dėl minėto nuorodų teikimo[89].

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 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, koks šio asmens vaidmuo viešajame gyvenime.

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.

[88] Direktyvos 95/46 8 straipsnio 2 dalies e punktas ir Reglamento 2016/679 9 straipsnio 2 dalies e punktas.
[89] Direktyvos 95/46 14 straipsnio pirmos pastraipos a punktas ir Reglamento 2016/679 21 straipsnio 1 dalis.

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

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[90].

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[91] visiškai nematyti, kad siekdamas įgyvendinti šį tikslą teisės aktų 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 ir 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.

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 interneto Sąjungoje vartotojams būtų užkirstas kelias arba bent jau jie būtų labai atgrasyti turėti prieigą atitinkamais atvejais iš paieškos sistemos versijos, kuri apima trečiąją valstybę, prie

[90] Direktyvos 95/46 4 straipsnio 1 dalies a punktas ir Reglamento 2016/679 3 straipsnio 1 dalis.
[91] Direktyvos 95/46 12 straipsnio b punktas ir 14 straipsnio pirmos pastraipos a punktas ir Reglamento 2016/679 17 straipsnio 1 dalis.

nuorodų, kurias prašoma pašalinti, o nacionalinis teismas turi patikrinti, ar eksploatuotojo nustatytos priemonės tenkina šį reikalavimą.

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.

2022 m. gruodžio 8 d. didžiosios kolegijos Sprendimas „Google (Tariamai netikslaus turinio pašalinimas)“ (C-460/20, EU:C:2022:962)

Su ieškovais pagrindinėje byloje, t. y. TU, kuris eina atsakingas pareigas ir turi įvairių bendrovių akcijų, ir RE, kuri buvo jo partnerė ir iki 2015 m. gegužės mėn. – vienos iš šių bendrovių prokuristė, buvo susiję trys straipsniai, kuriuos 2015 m. interneto svetainėje paskelbė šios svetainės operatorė G LLC. Šiuose straipsniuose, iš kurių vienas iliustruotas keturiomis nuotraukomis, kuriose pavaizduoti ieškovai ir iš kurių buvo galima suprasti, kad jie gyvena prabangų gyvenimą, buvo kritiškai pristatytas kelių jų bendrovių investavimo modelis. Straipsnius buvo galima rasti į *Google LLC* (toliau – *Google*) valdomą paieškos sistemą įvedus ieškovų vardus ir pavardes atskirai arba kartu su tam tikrų bendrovių pavadinimais. Rezultatų sąraše buvo pateikiamos nuorodos į šiuos straipsnius, taip pat į nuotraukas, rodomas miniatiūrų („thumbnails“) pavidalu.

Ieškovai pagrindinėje byloje paprašė *Google*, kaip asmens duomenų, tvarkomų jos paieškos sistemoje, valdytojos, pašalinti iš paieškos rezultatų sąrašo, pirma, nuorodas į nagrinėjamus straipsnius, nes tuose straipsniuose tariamai buvo netikslių teiginių ir šmeižikiškų nuomonių, ir, antra, miniatiūras. *Google* atsisakė tenkinti šį prašymą.

Kadangi tiek pirmojoje, tiek apeliacinėje instancijose ieškovų pagrindinėje byloje prašymai buvo atmesti, jie pateikė kasacinį skundą *Bundesgerichtshof* (Aukščiausiasis Federalinis Teismas, Vokietija), o jį nagrinėdamas šis teismas pateikė Teisingumo Teismui prašymą priimti prejudicinį sprendimą dėl BDAR ir Direktyvos 95/46[92] išaiškinimo.

Didžiosios kolegijos priimtame sprendime Teisingumo Teismas plėtojo savo jurisprudenciją dėl sąlygų, taikomų paieškos sistemos operatoriui skirtiems prašymams pašalinti nuorodas remiantis asmens duomenų apsaugos taisyklėmis. Visų pirma jis analizavo klausimą, viena vertus, dėl paieškos sistemos operatoriui tenkančių pareigų ir atsakomybės apimties nagrinėjant prašymą pašalinti nuorodas, grindžiamą tariamu į

[92] Atitinkamai BDAR 17 straipsnio 3 dalies a punkto ir Direktyvos 95/46 12 straipsnio b punkto ir 14 straipsnio pirmos pastraipos a punkto.

nurodomą turinį įtrauktos informacijos netikslumu, ir, kita vertus, dėl duomenų subjektui tenkančios šio netikslumo įrodinėjimo pareigos. Be to, jis sprendė dėl būtinumo nagrinėjant prašymą pašalinti nuotraukas, rodomas miniatiūrų pavidalu vaizdų paieškos rezultatų sąraše, atsižvelgti į pirminį šių nuotraukų paskelbimo internete kontekstą.

Pirma, Teisingumo Teismas nusprendė, kad lyginant teisę į privataus gyvenimo gerbimą ir asmens duomenų apsaugą su teise į saviraiškos ir informacijos laisvę[93], nagrinėjant paieškos sistemos operatoriui pateiktą prašymą iš paieškos rezultatų sąrašo pašalinti nuorodą į turinį, kuriame yra tariamai netikslios informacijos, toks pašalinimas nėra siejamas su sąlyga, kad nurodomo turinio tikslumo klausimas yra bent laikinai išspręstas to asmens inicijuotoje byloje prieš turinio teikėją.

Visų pirma tam, kad būtų galima patikrinti, kokiomis aplinkybėmis paieškos sistemos operatorius privalo patenkinti prašymą pašalinti nuorodas iš rezultatų sąrašo, rodomo atlikus paiešką pagal duomenų subjekto vardą ir pavardę, ir ištrinti nuorodą į tinklalapį, kuriame yra teiginių, kuriuos šis asmuo laiko netiksliais, Teisingumo Teismas, be kita ko, priminė:

• kadangi paieškos sistemos veikimas gali daryti didelį neigiamą poveikį pagrindinėms teisėms į privataus gyvenimo gerbimą ir asmens duomenų apsaugą ir šis poveikis yra papildomas, palyginti su tuo, kurį daro interneto svetainių rengėjai, šis paieškos sistemos operatorius, kaip subjektas, kuris nustato šios veiklos tikslus ir būdus, turi užtikrinti, kiek tai patenka į jo atsakomybės, kompetencijos ir galimybių sritį, kad Direktyvoje 95/46 ir BDAR numatytos garantijos galėtų tapti visiškai veiksmingos, o veiksminga ir visapusiška duomenų subjektų apsauga – iš tiesų įgyvendinta;

• paieškos sistemos operatorius, gavęs prašymą pašalinti nuorodas, turi patikrinti, ar nuorodos į nagrinėjamą interneto tinklalapį įtraukimas į rezultatų sąrašą yra būtinas, kad interneto naudotojai, potencialiai suinteresuoti gauti prieigą prie šio tinklalapio pagal tokią paiešką, galėtų pasinaudoti teise į saviraiškos ir informacijos laisvę;

• BDAR aiškiai įtvirtintas reikalavimas palyginti, pirma, pagrindines teises į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą ir, antra, pagrindinę teisę į informacijos laisvę.

Visų pirma Teisingumo Teismas pabrėžė, kad nors teisė į privataus gyvenimo gerbimą ir teisė į asmens duomenų apsaugą paprastai yra viršesnės už teisėtą interneto naudotojų interesą susipažinti su atitinkama informacija, ši pusiausvyra vis dėlto gali priklausyti nuo atitinkamų konkretaus atvejo aplinkybių, ypač nuo šios informacijos pobūdžio ir jos įtakos duomenų subjekto privačiam gyvenimui, taip pat nuo visuomenės intereso susipažinti su tokia informacija, kuris gali skirtis, nelygu, koks šio asmens vaidmuo viešajame gyvenime.

[93] Pagrindinės teisės, įtvirtintos atitinkamai Chartijos 7, 8 ir 11 straipsniuose.

Klausimas, ar nurodytas turinys yra tikslus, ar ne, taip pat yra svarbus veiksnys atliekant šį vertinimą. Taigi tam tikromis aplinkybėmis interneto naudotojų teisė į informaciją ir turinio teikėjo saviraiškos laisvė gali būti viršesnės už teisę į privataus gyvenimo apsaugą ir teisę į asmens duomenų apsaugą, ypač kai duomenų subjektas atlieka svarbų vaidmenį viešajame gyvenime. Vis dėlto šis santykis pasikeičia, kai paaiškėja, kad bent dalis prašyme pašalinti nuorodas pateiktos informacijos, kuri nėra mažareikšmė atsižvelgiant į visą turinį, yra netiksli. Tokiu atveju į teisę teikti informaciją ir teisę būti informuotam negali būti atsižvelgta, nes šios teisės negali apimti teisės skleisti tokią netikslią informaciją ir turėti prieigą prie jos.

Be to, kiek tai susiję, pirma, su pareiga nustatyti nurodomame turinyje esančios informacijos tikslumą ar netikslumą, Teisingumo Teismas pabrėžė, kad asmuo, prašantis pašalinti nuorodas dėl tokios informacijos netikslumo, privalo įrodyti akivaizdų tokios informacijos arba bent jau tos informacijos dalies, kuri, atsižvelgiant į visą šį turinį, nėra mažareikšmė, netikslumą. Vis dėlto, kad šiam asmeniui nebūtų nustatyta per didelės naštos, galinčios pakenkti teisės į nuorodų pašalinimą veiksmingumui, jis turi tik pateikti įrodymų, kurių, atsižvelgiant į nagrinėjamo atvejo aplinkybes, galima iš jo pagrįstai reikalauti. Iš esmės iš šio asmens negalima reikalauti, kad jis, siekdamas pagrįsti minėtą prašymą pašalinti nuorodas, ikiteisminėje stadijoje pateiktų teismo sprendimą – net ir sprendimą dėl laikinųjų apsaugos priemonių taikymo, – priimtą dėl interneto svetainės rengėjo.

Antra, dėl paieškos sistemos operatoriui tenkančių pareigų ir atsakomybės Teisingumo Teismas pažymėjo, kad šis operatorius, siekdamas patikrinti, ar turinys ir toliau gali būti įtrauktas į paieškos, atliktos per paieškos sistemą po to, kai buvo pateiktas prašymas pašalinti nuorodas, rezultatų sąrašą, turi remtis visomis esančiomis teisėmis ir interesais, taip pat visomis konkretaus atvejo aplinkybėmis. Vis dėlto negalima reikalauti, kad šis operatorius būtų įpareigotas tirti faktus ir šiuo tikslu pradėti ginčo procedūrą su turinio teikėju, siekdamas gauti trūkstamos informacijos apie nurodomo turinio tikslumą. Pareiga prisidėti nustatant nurodomo turinio tikslumą ar netikslumą reikštų, kad šiam operatoriui tenka našta, viršijanti tai, ko iš jo galima pagrįstai tikėtis atsižvelgiant į jo atsakomybę, kompetenciją ir galimybes. Dėl tokio sprendimo kiltų didelė rizika, kad turinys, kuris atitinka teisėtą ir svarbų visuomenės informacijos poreikį, bus pašalintas ir jį bus sunku rasti internete. Taigi kiltų reali grėsmė, kad naudojimasis saviraiškos ir informacijos laisve gali turėti atgrasomąjį poveikį, jei minėtas operatorius tokį nuorodų pašalinimą vykdytų beveik sistemingai, siekdamas išvengti naštos, susijusios su atitinkamų faktų tyrimu, tam, kad būtų nustatyta, ar nurodomas turinys yra tikslus, ar ne.

Vadinasi, tuo atveju, kai prašymą pašalinti nuorodas pateikęs asmuo pateikia įrodymų, patvirtinančių, kad nurodomame turinyje esanti informacija arba bent jau dalis šios informacijos, kuri nėra mažareikšmė atsižvelgiant į visą šį turinį, yra akivaizdžiai netiksli, paieškos sistemos operatorius privalo patenkinti tokį prašymą pašalinti nuorodas. Tas pats pasakytina ir tuo atveju, kai šis prašymą pateikęs asmuo pateikia teismo sprendimą

dėl interneto svetainės rengėjo, kuris grindžiamas išvada, kad nurodomame turinyje pateikta informacija, kuri nėra mažareikšmė atsižvelgiant į visą šį turinį, bent jau iš pirmo žvilgsnio yra netiksli. Vis dėlto tuo atveju, kai iš prašymą pateikusio asmens pateiktų įrodymų nėra akivaizdu, kad tokia nurodomame turinyje esanti informacija yra netiksli, paieškos sistemos operatorius, nesant tokio teismo sprendimo, neprivalo tenkinti prašymo pašalinti nuorodas. Kai nagrinėjama informacija gali prisidėti prie bendrojo intereso diskusijų, teisei į saviraiškos ir informacijos laisvę turi būti teikiama ypatinga reikšmė, atsižvelgiant į visas kitas bylos aplinkybes.

Galiausiai Teisingumo Teismas pridūrė, kad, paieškos sistemos operatoriui nepatenkinus prašymo pašalinti nuorodas, duomenų subjektas turi galėti kreiptis į priežiūros ar teisminę institucijas, kad šios atliktų reikiamus patikrinimus ir prireikus nurodytų šiam operatoriui imtis privalomų priemonių. Šiuo klausimu būtent teisminės institucijos turi užtikrinti konkuruojančių interesų pusiausvyrą, nes jos gali geriau atlikti sudėtingą ir išsamų palyginimą, atsižvelgdamos į visus atitinkamoje jurisprudencijoje nustatytus kriterijus ir visas aplinkybes.

Antra, Teisingumo Teismas konstatavo, kad, lyginant nurodytas pagrindines teises, kai nagrinėjamas prašymas pašalinti nuorodas, kuriuo iš vaizdų paieškos, atliktos pagal fizinio asmens vardą ir pavardę, rezultatų siekiama pašalinti tą asmenį vaizduojančias nuotraukas, rodomas miniatiūrų pavidalu, reikia atsižvelgti į šių nuotraukų informacinę vertę nepriklausomai nuo jų paskelbimo tinklalapyje, iš kurio jos buvo paimtos, konteksto. Vis dėlto reikia atsižvelgti į bet kokį tekstinį elementą, kuris paieškos rezultatuose tiesiogiai pateikiamas kartu su šiomis rodomomis nuotraukomis ir gali atskleisti jų informacinę vertę.

Darydamas šią išvadą Teisingumo Teismas pabrėžė, kad vaizdų paieškai, atliekamai per interneto paieškos sistemą pagal asmens vardą ir pavardę, taikomi tie patys principai, kurie taikomi tinklalapių ir juose esančios informacijos paieškai. Jis nurodė, kad duomenų subjekto nuotraukų rodymas miniatiūrų pavidalu, atlikus paiešką pagal vardą ir pavardę, gali ypač riboti šio asmens teises į privataus gyvenimo ir į asmens duomenų apsaugą.

Taigi, kai paieškos sistemos operatorius gauna prašymą pašalinti nuorodas, kuriuo iš vaizdų paieškos, atliktos pagal asmens vardą ir pavardę, rezultatų siekiama pašalinti tą asmenį vaizduojančias nuotraukas, rodomas miniatiūrų pavidalu, jis turi patikrinti, ar aptariamų nuotraukų rodymas yra būtinas, kad interneto naudotojai, potencialiai suinteresuoti atlikus tokią paiešką gauti prieigą prie šių nuotraukų, galėtų pasinaudoti teise į informacijos laisvę.

Kadangi paieškos sistemoje duomenų subjekto nuotraukos rodomos ne tame kontekste, kuriame jos paskelbtos tinklalapyje, į kurį daroma nuoroda, dažniausiai siekiant iliustruoti tame puslapyje esančius tekstinius elementus, būtina nustatyti, ar į šį kontekstą vis dėlto reikia atsižvelgti lyginant konkuruojančias teises ir interesus. Šiomis aplinkybėmis klausimas, ar į minėtą vertinimą taip pat turi būti įtrauktas tinklalapio su

nuotrauka, kurios prašoma nerodyti miniatiūros pavidalu, turinys, priklauso nuo nagrinėjamo tvarkymo objekto ir pobūdžio.

Pirma, dėl nagrinėjamo tvarkymo objekto reikia pažymėti, kad nuotraukų, kaip neverbalinės komunikacijos priemonės, skelbimas interneto naudotojams gali turėti didesnį poveikį nei tekstinės publikacijos. Iš tiesų nuotraukos yra svarbi interneto naudotojų dėmesio pritraukimo priemonė, galinti paskatinti susidomėjimą susipažinti su jomis iliustruojamais straipsniais. Tačiau, ypač atsižvelgiant į tai, kad nuotraukas dažnai galima interpretuoti įvairiai, jų kaip miniatiūrų rodymas paieškos rezultatų sąraše gali būti ypač rimtas duomenų subjekto teisės į jo atvaizdo apsaugą apribojimas, į kurį reikia atsižvelgti lyginant konkuruojančias teises ir interesus. Reikia atskirai atlikti palyginimą remiantis tuo, ar kalbama, pirma, apie tinklalapio rengėjo paskelbtas nuotraukas, kurios, atsižvelgiant į jų pirminį kontekstą, iliustruoja šiuose straipsniuose pateiktą informaciją ir juose išreikštas nuomones, ar, antra, apie nuotraukas, kurias miniatiūrų pavidalu rezultatų sąraše paieškos sistemos operatorius pateikia ne tame kontekste, kuriame jos buvo paskelbtos pirminiame tinklalapyje.

Šiuo klausimu Teisingumo Teismas priminė, kad ne tik motyvas, pateisinantis asmens duomenų paskelbimą interneto svetainėje, nebūtinai sutampa su tuo, kuris taikytinas paieškos sistemų veikimo operacijų atveju, bet net tuomet, kai jie sutampa, atitinkamų teisių ir interesų palyginimo, kurį reikia atlikti, rezultatas gali skirtis, nelygu tai, ar duomenis tvarko paieškos sistemos operatorius, ar to tinklalapio rengėjas. Viena vertus, gali skirtis teisėti interesai, kuriais pateisinamos tvarkymo operacijos, ir, kita vertus, šių tvarkymo operacijų padariniai duomenų subjektui, visų pirma jo privačiam gyvenimui, nebūtinai yra tokie patys.

Antra, kalbėdamas apie paieškos sistemos operatoriaus atliekamo duomenų tvarkymo pobūdį, Teisingumo Teismas konstatavo, kad, rasdamas internete paskelbtas fizinių asmenų nuotraukas ir jas atskirai miniatiūrų pavidalu rodydamas vaizdų paieškos rezultatuose, paieškos sistemos operatorius teikia tam tikrą paslaugą, kuri susijusi su asmens duomenų tvarkymu ir yra savarankiška ir atskira tiek nuo duomenų tvarkymo, vykdomo tinklalapio, iš kurio paimtos nuotraukos, rengėjo, tiek nuo duomenų tvarkymo, už kurį tas operatorius taip pat atsakingas ir kuris susijęs su nuorodų įtraukimu į tą tinklalapį.

Taigi reikia atlikti nepriklausomą paieškos sistemos operatoriaus veiklos, kuria siekiama rodyti vaizdų paieškos rezultatus miniatiūrų pavidalu, vertinimą, nes dėl tokios veiklos gali būti ypač stipriai pažeidžiamos pagrindinės teisės dėl to, kad atliekant paiešką pagal vardą ir pavardę apibendrinama visa internete rasta informacija apie duomenų subjektą. Atliekant šį nepriklausomą vertinimą reikia atsižvelgti į tai, kad nuotraukų rodymas internete miniatiūrų pavidalu pats savaime yra rezultatas, kurio ieško interneto naudotojas, nepriklausomai nuo to, ar jis vėliau nusprendžia prisijungti prie pirminio tinklalapio, ar ne.

Vis dėlto Teisingumo Teismas pažymėjo, kad toks konkretus palyginimas, kuriuo atsižvelgiama į paieškos sistemos operatoriaus atliekamą savarankišką tvarkymo pobūdį, neturi įtakos galimai tekstinių elementų, kurie paieškos rezultatų sąraše gali būti tiesiogiai pateikiami kartu su rodoma nuotrauka, svarbai, nes tokie elementai gali atskleisti tos nuotraukos informacinę vertę visuomenei ir taip paveikti susijusių teisių ir interesų palyginimą.

4. Interneto svetainės naudotojo sutikimas dėl informacijos saugojimo

2019 m. spalio 1 d. didžiosios kolegijos Sprendimas „Planet49“ (C-673/17, EU:C:2019:801)

Tame sprendime Teisingumo Teismas nusprendė, kad sutikimas dėl informacijos saugojimo arba prieigos prie jos suteikimo 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 buvo 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[94], siejamoje su Direktyva 95/46/EB[95] ir BDAR[96], vartojamos sąvokos „sutikimas“ aiškinimu.

Pirma, Teisingumo Teismas pažymėjo, kad Direktyvos 95/46/EB 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 [tinkamai informuoto duomenų subjekto savanorišką 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. O 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,

94 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.

95 Direktyvos 95/46 2 straipsnio h punktas.

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

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[97], 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“.

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

Antra, Teisingumo Teismas konstatavo, kad pagal Direktyvos 2002/58 5 straipsnio 3 dalį 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.

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.

5. Asmens duomenų tvarkymas internetiniuose socialiniuose tinkluose

2023 m. liepos 4 d. didžiosios kolegijos Sprendimas „Meta Platforms ir kt. (Bendrosios socialinio tinklo naudojimo sąlygos)“ (C-252/21, EU:C:2023:537)

Bendrovė *Meta Platforms* yra internetinio socialinio tinklo *Facebook*, kuriuo privatūs naudotojai naudojasi nemokamai, savininkė. Šio socialinio tinklo verslo modelis grindžiamas finansavimu iš internetinės reklamos, kuri asmeniškai pritaikoma individualiems naudotojams. Tokia reklama techniškai įmanoma automatiškai parengiant išsamius tinklo ir internetinių paslaugų, siūlomų *Meta* grupės lygmeniu, naudotojų profilius. Taigi tam, kad galėtų naudotis šiuo socialiniu tinklu,

[97] Ten pat.

registruodamiesi naudotojai turi sutikti su *Meta Platforms* nustatytomis bendrosiomis sąlygomis, kuriose daroma nuoroda į šios bendrovės nustatytą duomenų naudojimo ir slapukų politiką. Pagal šią politiką, be duomenų, kuriuos šie naudotojai pateikia tiesiogiai registruodamiesi, *Meta Platforms* taip pat renka duomenis, susijusius su šių naudotojų veikla socialiniame tinkle ir už jo ribų ir susieja juos su atitinkamų naudotojų *Facebook* paskyromis. Už socialinio tinklo ribų renkami duomenys, dar vadinami „*off Facebook* duomenimis“, visų pirma apima duomenis, susijusius su lankymusi trečiųjų šalių interneto svetainėse ir taikomosiose programėlėse, ir, antra, duomenis, susijusius su naudojimusi kitomis *Meta* grupei priklausančiomis internetinėmis paslaugomis (įskaitant *Instagram* ir *WhatsApp*). Taip surinkti duomenys, vertinami bendrai, leidžia daryti išsamias išvadas apie naudotojų pageidavimus ir interesus.

2019 m. vasario 6 d. sprendimu *Bundeskartellamt* (Federalinė konkurencijos institucija, Vokietija) uždraudė *Meta Platforms*, pirma, Vokietijoje gyvenančių privačių naudotojų naudojimąsi socialiniu tinklu *Facebook* tuo metu galiojančiose bendrosiose sąlygose susieti su tokių naudotojų *off Facebook* duomenų tvarkymu ir, antra, be jų sutikimo tvarkyti šiuos duomenis. Be to, federalinė konkurencijos institucija įpareigojo *Meta* pakeisti bendrąsias sąlygas taip, kad iš jų būtų aiškiai matyti, jog tokie duomenys nebus nei renkami, nei susieti su *Facebook* naudotojų paskyromis, nei naudojami be atitinkamo naudotojo sutikimo. Galiausiai ši institucija pabrėžė, kad toks sutikimas negalioja, kai tai yra naudojimosi socialiniu tinklu sąlyga. Savo sprendimą ji motyvavo tuo, kad tvarkant nagrinėjamus duomenis, kai toks tvarkymas neatitinka BDAR, yra piktnaudžiaujama dominuojančia *Meta Platforms* padėtimi internetinių socialinių tinklų rinkoje.

Meta Platforms apskundė šį sprendimą *Oberlandesgericht Düsseldorf* (Diuseldorfo aukštesnysis apygardos teismas, Vokietija). Abejodamas dėl, be kita ko, kelių BDAR nuostatų aiškinimo ir taikymo, šis teismas kreipėsi į Teisingumo Teismą su prašymu priimti prejudicinį sprendimą.

Savo sprendime Teisingumo Teismo didžioji kolegija pateikė paaiškinimų dėl galimybės socialinio tinklo operatoriui tvarkyti „neskelbtinus“ tokio tinklo naudotojų duomenis, dėl tokio operatoriaus atliekamo duomenų tvarkymo teisėtumo sąlygų, taip pat dėl duomenų subjekto sutikimo, kurį dėl tokio tvarkymo naudotojai davė bendrovei, užimančiai dominuojančią padėtį nacionalinėje internetinių socialinių tinklų rinkoje, galiojimo.

Dėl specialių kategorijų asmens duomenų[98] tvarkymo Teisingumo Teismas nusprendė, kad tuo atveju, kai internetinio socialinio tinklo naudotojas lankosi interneto svetainėse ar taikomosiose programėlėse, susijusiose su viena ar keliomis tokiomis kategorijomis, ir prireikus į jas įkelia duomenis užsiregistruodamas arba pateikdamas užsakymus internetu, šio internetinio socialinio tinklo operatoriaus atliekamas asmens duomenų

[98] Nurodytų BDAR 9 straipsnio 1 dalyje. Šioje nuostatoje numatyta: „[d]raudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją“.

tvarkymas[99] turi būti laikomas „specialių kategorijų asmens duomenų tvarkymu“, kaip tai suprantama pagal BDAR 9 straipsnio 1 dalį, jeigu jis leidžia atskleisti prie vienos iš šių specialių kategorijų priskiriamą informaciją, nesvarbu, ar ši informacija susijusi su šio tinklo naudotoju, ar su bet kuriuo kitu fiziniu asmeniu. Toks duomenų tvarkymas iš esmės draudžiamas, išskyrus tam tikras išimtis[100].

Pastaruoju klausimu Teisingumo Teismas patikslino, kad, kai internetinio socialinio tinklo naudotojas lankosi interneto svetainėse ar taikomosiose programose, susijusiose su viena ar keliomis minėtomis specialiomis duomenų kategorijomis, jis akivaizdžiai viešai neskelbia[101] su tokiu lankymusi susijusių duomenų, kuriuos šio internetinio socialinio tinklo operatorius surinko naudodamas slapukus ar panašias įrašymo technologijas. Be to, kai į šias interneto svetaines arba taikomąsias programėles įkelia duomenis arba aktyvuoja jose integruotus atrankos mygtukus, pavyzdžiui, mygtukus „Patinka“ ar „Bendrinti“ arba mygtukus, leidžiančius naudotojui šiose interneto svetainėse ar taikomosiose programėlėse identifikuoti save naudojant internetinio socialinio tinklo naudotojo paskyros prisijungimo identifikatorius, telefono numerį ar elektroninio pašto adresą, laikoma, kad toks naudotojas akivaizdžiai viešai paskelbia taip įkeltus ar aktyvuojant šiuos mygtukus gautus duomenis, tik jeigu jis aiškiai išreiškė savo išankstinį pasirinkimą, prireikus remdamasis individualiai pasirinktais nustatymais ir žinodamas tokių veiksmų pasekmes, padaryti viešai prieinamus su juo susijusius duomenis neribotam asmenų skaičiui.

Kiek tai bendrai susiję su asmens duomenų tvarkymo teisėtumo sąlygomis, Teisingumo Teismas priminė, kad pagal BDAR duomenų tvarkymas yra teisėtas tuo atveju, jeigu duomenų subjektas davė sutikimą, kad jo duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais[102]. Nesant tokio sutikimo arba kai šis sutikimas nebuvo duotas laisva valia, konkrečiai, informuotai ir nedviprasmiškai, toks duomenų tvarkymas vis dėlto yra pateisinamas, jeigu atitinka vieną iš būtinumo reikalavimų[103], kuriuos reikia aiškinti siaurai. Internetinio socialinio tinklo operatoriaus atliekamas tokio tinklo naudotojų asmens duomenų tvarkymas gali būti laikomas būtinu sutarčiai, kurios šalys yra šie naudotojai, įvykdyti tik su sąlyga, kad toks tvarkymas yra objektyviai būtinas siekiant tikslo, kuris yra tiems patiems naudotojams skirtos sutartinės paslaugos sudedamoji

---

99 Šį tvarkymą sudaro duomenų, gautų apsilankius šiose interneto svetainėse ir taikomose programose, taip pat naudotojo įterptų duomenų rinkimas, naudojant integruotas sąsajas, slapukus ar panašias įrašymo technologijas, visų šių duomenų susiejimas su naudotojo socialinio tinklo paskyra ir šio operatoriaus atliekamas minėtų duomenų naudojimas.

100 Jos numatytos BDAR 9 straipsnio 2 dalyje. Ši nuostata suformuluota taip: „1 dalis netaikoma, jei taikoma viena iš toliau nurodytų sąlygų:

a) duomenų subjektas aiškiai sutiko, kad tokie asmens duomenys būtų tvarkomi vienu ar keliais nurodytais tikslais, išskyrus atvejus, kai Sąjungos arba valstybės narės teisėje numatyta, kad 1 dalyje nurodyto draudimo duomenų subjektas negali panaikinti; <...>

e) tvarkomi asmens duomenys, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai;

f) tvarkyti duomenis būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus arba tuo atveju, kai teismai vykdo savo teisminius įgaliojimus;

<...>“

101 Kaip tai suprantama pagal BDAR 9 straipsnio 2 dalies e punktą.

102 Kaip nurodyta BDAR 6 straipsnio 1 dalies pirmos pastraipos a punkte.

103 Nurodytų BDAR 6 straipsnio 1 dalies pirmos pastraipos b–f punktuose. Pagal šias nuostatas duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu ir tiek, kiek jis būtinas, be kita ko, siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas (BDAR 6 straipsnio 1 dalies pirmos pastraipos b punktas), kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė (BDAR 6 straipsnio 1 dalies pirmos pastraipos c punktas), arba siekiant teisėtų duomenų valdytojo ar trečiosios šalies interesų (BDAR 6 straipsnio 1 dalies pirmos pastraipos f punktas).

dalis, todėl pagrindinis sutarties dalykas negalėtų būti pasiektas neatliekant tokio duomenų tvarkymo.

Be to, Teisingumo Teismo teigimu, nagrinėjamas duomenų tvarkymas gali būti laikomas būtinu siekiant teisėtų duomenų valdytojo ar trečiojo asmens interesų tik su sąlyga, kad minėtas operatorius naudotojams, iš kurių duomenys buvo surinkti, nurodė teisėtą interesą, kurio siekiama juos tvarkant, ir kad toks tvarkymas atliekamas neviršijant to, kas griežtai būtina šiam teisėtam interesui pasiekti, ir jei palyginus priešingus interesus, atsižvelgiant į visas svarbias aplinkybes, matyti, kad šių naudotojų interesai ar pagrindinės laisvės ir teisės nėra viršesni už minėtą teisėtą duomenų valdytojo ar trečiosios šalies interesą. Teisingumo Teismas, be kita ko, nurodė, kad, nesant minėtų naudotojų sutikimo, jų interesai ir pagrindinės teisės yra viršesni už internetinio socialinio tinklo operatoriaus interesą asmeniškai pritaikyti reklamą, kuria jis finansuoja savo veiklą.

Galiausiai Teisingumo Teismas patikslino, kad nagrinėjamas duomenų tvarkymas yra pateisinamas, kai iš tiesų būtina įvykdyti duomenų valdytojui pagal Sąjungos teisę ar atitinkamos valstybės narės teisę nustatytą teisinę pareigą, jeigu šis teisinis pagrindas atitinka viešojo intereso tikslą, yra proporcingas siekiamam teisėtam tikslui ir jei toks tvarkymas atliekamas neviršijant to, kas griežtai būtina.

Dėl atitinkamų naudotojų sutikimo tvarkyti jų duomenis pagal BDAR galiojimo Teisingumo Teismas nusprendė, kad aplinkybė, jog internetinio socialinio tinklo operatorius, kaip duomenų valdytojas, užima dominuojančią padėtį socialinių tinklų rinkoje, savaime netrukdo šio socialinio tinklo naudotojams duoti galiojantį duomenų subjekto sutikimą, kad šis operatorius tvarkytų jų asmens duomenis. Vis dėlto atsižvelgiant į tai, kad tokia dominuojanti padėtis gali paveikti šių naudotojų pasirinkimo laisvę ir dėl jos gali atsirasti akivaizdus naudotojų ir minėto operatoriaus padėties disbalansas, ji yra svarbus veiksnys nustatant, ar sutikimas iš tikrųjų buvo galiojantis ir, be kita ko, duotas laisva valia, o tai turi įrodyti minėtas operatorius[104].

Konkrečiai kalbant, atitinkamo socialinio tinklo naudotojai turi turėti laisvę atskirai, vykstant sutarties sudarymo procedūrai, atsisakyti duoti sutikimą dėl konkrečių duomenų tvarkymo operacijų, kurios nėra būtinos sutarčiai vykdyti, tačiau jie neprivalo visiškai atsisakyti naudotis internetinio socialinio tinklo operatoriaus siūloma paslauga, o tai reiškia, kad minėtam naudotojui, jeigu reikia – už tinkamą atlygį, turėtų būti pasiūlyta lygiavertė alternatyva, kai netaikomos tokios duomenų tvarkymo operacijos. Be to, dėl *off Facebook* duomenų tvarkymo turi būti galima duoti atskirą sutikimą.

[104] Pagal BDAR 7 straipsnio 1 dalį.

VI. Nacionalinės priežiūros institucijos

1. Nepriklausomumo reikalavimo apimtis

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

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, 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.

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, nei jos pačios nebūtų

šališki. Todėl, anot Teisingumo Teismo, nacionalinių priežiūros institucijų atžvilgiu vykdoma valstybės kontrolė nėra suderinama su nepriklausomumo reikalavimu.

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.

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.

Teisingumo Teismas pažymėjo, kad nebūtina numatyti atskiros nacionalinei priežiūros institucijai skirtos biudžeto eilutės, kaip tai padaryta Reglamento 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 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.

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

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/EB neįvykdo ta valstybė narė, kuri pirma laiko nutraukia asmens duomenų apsaugos priežiūros institucijos kadenciją.

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 kokių nurodymų ir išorinės įtakos – tiesioginės ar netiesioginės, galinčios pakreipti jų sprendimus kuria nors linkme ir taip sutrukdyti joms vykdyti pavestą užduotį nustatyti teisingą teisės į privatų gyvenimą apsaugos ir laisvo asmens duomenų judėjimo pusiausvyrą.

Be to, Teisingumo Teismas priminė: kadangi vien 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 jų 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 nekeldama jokių įtarimų šališkumu.

2. Taikytinos teisės ir kompetentingos priežiūros institucijos nustatymas

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

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 valstybės narės nei ta, kur asmens duomenų valdytojas registruotas, 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.

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. 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 perduota informacija.

3. Nacionalinių priežiūros institucijų įgaliojimai

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 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.

Dėl įgaliojimų vykdyti asmens duomenų perdavimo į trečiąsias šalis kontrolę Teisingumo Teismas nusprendė, kad iš Direktyvos 95/46 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.

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.

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

Šiame sprendime (taip pat žr. II skyriaus 5 skirsnį „Sąvoka „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*).

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.

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[105] 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 vykusiame 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[106] 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.

Didžiosios kolegijos priimtame sprendime Teisingumo Teismas patikslino nacionalinių priežiūros institucijų įgaliojimus pagal BDAR. Jis, be kita ko, nusprendė, kad pagal šį

[105] Pavyzdžiui, mygtukus „Patinka“ arba „Bendrinti“.

[106] BDAR 56 straipsnio 1 dalyje nustatyta: „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“.

reglamentą valstybės narės priežiūros institucijai tam tikromis sąlygomis leidžiama naudotis savo įgaliojimais dėl tariamų BDAR pažeidimų kreiptis į tos valstybės teismą ir pradėti teismo procesą dėl tarpvalstybinio duomenų tvarkymo[107], nors šio tvarkymo atveju ji nėra vadovaujanti institucija.

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 pagal BDAR šiai priežiūros institucijai turi būti suteikta kompetencija priimti sprendimą, kuriuo konstatuojama, kad toks duomenų tvarkymas pažeidžia šiame reglamente nustatytas taisykles, ir šiuo įgaliojimu turi būti naudojamasi laikantis minėtame reglamente numatytų bendradarbiavimo ir nuoseklumo užtikrinimo procedūrų[108].

Tarpvalstybinio duomenų tvarkymo atveju BDAR numatytas vieno langelio mechanizmas[109], 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[110], o kitų nacionalinių priežiūros institucijų kompetencija priimti tokį sprendimą, net ir laikiną, yra išimtis[111]. 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.

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[112], yra suderinama su Chartijos 7, 8 ir 47 straipsniais, kuriuose

[107] Kaip tai suprantama pagal BDAR 4 straipsnio 23 punktą.
[108] Numatytų BDAR 56 ir 60 straipsniuose.
[109] BDAR 56 straipsnio 1 dalis.
[110] BDAR 60 straipsnio 7 dalis.
[111] BDAR 56 straipsnio 2 dalyje ir 66 straipsnyje įtvirtintos vadovaujančios priežiūros institucijos principinės kompetencijos priimti sprendimus išimtys.
[112] Numatytos BDAR 55 ir 56 straipsniuose, siejamuose su jo 60 straipsniu.

asmenims atitinkamai užtikrinama teisė į asmens duomenų apsaugą ir teisė į veiksmingą teisinę gynybą.

Antra, Teisingumo Teismas nusprendė, kad tarpvalstybinio duomenų tvarkymo atveju valstybės narės priežiūros institucijai, kuri nėra vadovaujanti priežiūros institucija, siekiant pasinaudoti įgaliojimu pareikšti ieškinį[113] 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[114], o tai reiškia, kad tarpvalstybinį duomenų tvarkymą vykdantis duomenų valdytojas arba duomenų tvarkytojas turi turėti buveinę Sąjungos teritorijoje.

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. Nagrinėtu atveju, kadangi Belgijoje esančios *Facebook* grupės buveinės veikla buvo neatsiejamai susijusi su pagrindinėje byloje nagrinėtu asmens duomenų tvarkymu, už kurį Sąjungos teritorijoje yra atsakinga *Facebook Ireland*, toks tvarkymas laikytas atliekamu „duomenų valdytojo [buveinei vykdant] savo veiklą“, todėl visiškai patenkančiu į BDAR taikymo sritį.

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 ir nuoseklumo užtikrinimo procedūrų.

Galiausiai, penkta, Teisingumo Teismas pripažino tiesioginį BDAR nuostatos, pagal kurią kiekviena valstybė narė įstatymuose numato, kad jos priežiūros institucija yra įgaliota

[113] Pagal BDAR 58 straipsnio 5 dalį.

[114] 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“.

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.

2024 m. sausio 16 d. didžiosios kolegijos Sprendimas „Österreichische Datenschutzbehörde“ (C-33/22, EU:C:2024:46)

Šioje byloje (taip pat žr. II skyriaus 1 skirsnį „Bendroji reglamentavimo taikymo sritis“) Teisingumo Teismas pažymėjo, kad dėl BDAR nuostatų, susijusių su nacionalinių priežiūros institucijų kompetencija ir teise pateikti skundą[115], nereikia priimti nacionalinių įgyvendinimo priemonių ir jos yra pakankamai aiškios, tikslios ir besąlyginės, kad būtų taikomos tiesiogiai. Darytina išvada, kad nors BDAR pripažinta valstybių narių diskrecija dėl įsteigtinų priežiūros institucijų skaičiaus[116], vis dėlto jame nustatyta šių institucijų kompetencijos prižiūrėti šio BDAR taikymą apimtis. Taigi tuo atveju, kai valstybė narė nusprendžia įsteigti vienintelę nacionalinę priežiūros instituciją, ši neišvengiamai turi visus šiame reglamente numatytus įgaliojimus. Bet koks kitas aiškinimas pakenktų šių BDAR nuostatų veiksmingumui ir galėtų susilpninti visų kitų jo nuostatų, su kuriomis gali būti susijęs skundas, veiksmingumą.

Dėl aplinkybės, kad pagal konstitucinio lygmens nacionalinės teisės nuostatas priežiūros institucija, kuri priskiriama prie vykdomosios valdžios, negali prižiūrėti, kaip įstatymų leidžiamosios valdžios organas taiko BDAR, Teisingumo Teismas pabrėžė, kad būtent paisant valstybių narių konstitucinės sandaros BDAR tik reikalaujama, kad jos įsteigtų bent vieną priežiūros instituciją, kartu suteikiant joms galimybę įsteigti kelias tokias institucijas. Taigi šiuo reglamentu kiekvienai valstybei narei pripažįstama diskrecija, leidžianti jai įsteigti tiek priežiūros institucijų, kiek jų reikia, be kita ko, pagal jos konstitucinę sandarą.

Be to, valstybės narės rėmimasis nacionalinės teisės nuostatomis negali pakenkti Sąjungos teisės vienodam taikymui ir veiksmingumui. Iš tiesų Sąjungos teisės viršenybės principas daro poveikį visoms valstybės narės institucijoms ir tam negali kliudyti net ir konstitucinio lygmens vidaus nuostatos.

Taigi, jeigu naudodamasi savo diskrecija valstybė narė nusprendė įsteigti vienintelę priežiūros instituciją, ji negali remtis net konstitucinio lygmens nacionalinės teisės nuostatomis, siekdama į BDAR taikymo sritį patenkančiam asmens duomenų tvarkymui netaikyti šios institucijos vykdomos priežiūros.

[115] Atitinkamai BDAR 55 straipsnio 1 dalis ir 77 straipsnio 1 dalis.
[116] Pagal BDAR 51 straipsnio 1 dalį.

4. Administracinių baudų skyrimo sąlygos

2023 m. gruodžio 5 d. didžiosios kolegijos Sprendimas „Nacionalinis visuomenės sveikatos centras“ (C-683/21, EU:C:2023:949)

Šioje byloje (taip pat žr. I skyriaus 3 skirsnį „Sąvoka „asmens duomenų tvarkymas“, 5 skirsnį „Sąvoka „asmens duomenų valdytojas“ ir 6 skirsnį „Sąvoka „bendras duomenų valdytojas“) Teisingumo Teismas konstatavo, kad pagal BDAR 83 straipsnį administracinė bauda duomenų valdytojui gali būti skirta tik nustačius, kad jis tyčia ar dėl aplaidumo pažeidė šiame reglamente nustatytas taisykles[117].

Šiuo klausimu Teisingumo Teismas pažymėjo, kad Sąjungos teisės aktų leidėjas nepaliko valstybėms narėms diskrecijos dėl materialinių sąlygų, kurių turi laikytis priežiūros institucija, kai nusprendžia skirti duomenų valdytojui administracinę baudą pagal šią nuostatą. Tai, kad BDAR valstybėms narėms suteikta galimybė numatyti išimtis jų teritorijoje įsteigtoms valdžios institucijoms ir įstaigoms[118], taip pat procedūrinius reikalavimus, kurių turi laikytis priežiūros institucijos, kad galėtų skirti administracinę baudą[119], visai nereiškia, kad šioms valstybėms suteikta teisė taip pat numatyti materialines sąlygas.

Dėl šių sąlygų Teisingumo Teismas pažymėjo, kad tarp BDAR išvardytų veiksnių, į kuriuos atsižvelgdama priežiūros institucija skiria duomenų valdytojui administracinę baudą, yra aplinkybė, „ar pažeidimas padarytas tyčia, ar dėl aplaidumo“[120]. Tačiau nė vienas iš tų veiksnių nepatvirtina galimybės patraukti duomenų valdytoją atsakomybėn nesant jo kaltės. Taigi administracinė bauda pagal šio reglamento 83 straipsnį duomenų valdytojui gali būti skirta tik už tyčia arba dėl aplaidumo padarytus BDAR nuostatų pažeidimus.

Teisingumo Teismas pridūrė, kad tokį aiškinimą patvirtina BDAR bendra sistema ir tikslas. Šiomis aplinkybėmis jis patikslino, kad sankcijų sistema, leidžianti skirti administracinę baudą pagal BDAR 83 straipsnį, kai to reikia atsižvelgiant į konkrečias kiekvieno atvejo aplinkybes, skatina duomenų valdytojus ir duomenų tvarkytojus laikytis šio reglamento, o administracinės baudos dėl atgrasomojo poveikio prisideda prie duomenų subjektų apsaugos stiprinimo. Vis dėlto Sąjungos teisės aktų leidėjas nemanė, kad būtina numatyti administracinių baudų skyrimą nesant kaltės. Atsižvelgiant į tai, kad BDAR siekiama lygiavertės ir vienodos apsaugos ir kad dėl to jis turi būti nuosekliai taikomas visoje Sąjungoje, šiam tikslui prieštarautų leidimas valstybėms narėms numatyti tokią baudų skyrimo sistemą.

Be to, Teisingumo Teismas padarė išvadą, kad tokia bauda gali būti skirta duomenų valdytojui už asmens duomenų tvarkymo veiksmus, kuriuos jo vardu atlieka duomenų

---

117 83 straipsnio 4–6 dalyse numatyti pažeidimai.

118 Pagal BDAR 83 straipsnio 7 dalį, kurioje numatyta, kad „<...> kiekviena valstybė narė gali nustatyti taisykles, reglamentuojančias tai, ar ir kokiu mastu administracinės baudos gali būti skiriamos valdžios institucijoms ir įstaigoms, įsisteigusioms toje valstybėje narėje“.

119 Pagal BDAR 83 straipsnio 8 dalį, siejamą su jo 129 konstatuojamąja dalimi.

120 BDAR 83 straipsnio 2 dalies b punktas.

tvarkytojas, išskyrus atvejus, kai atlikdamas tokius veiksmus duomenų tvarkytojas tvarko duomenis savo tikslais arba tokiu būdu, kuris nesuderinamas su duomenų valdytojo nustatyta duomenų tvarkymo sistema ar tvarka, arba taip, kad negalima pagrįstai manyti, jog duomenų valdytojas tam pritarė. Tokiu atveju pats duomenų tvarkytojas turi būti laikomas atsakingu už tokį duomenų tvarkymą.

2023 m. gruodžio 5 d. didžiosios kolegijos Sprendimas „Deutsche Wohnen“ (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (toliau – DW) yra nekilnojamojo turto bendrovė, kuri, turėdama įvairių bendrovių kapitalo dalių, netiesiogiai valdo nemažai komercinės ir gyvenamosios paskirties objektų. Vykdydama komercinę veiklą ji tvarko šių objektų nuomininkų asmens duomenis.

2017 ir 2019 m. atlikusi du patikrinimus *Berliner Beauftragter für den Datenschutz* (Berlyno duomenų apsaugos institucija, Vokietija) nustatė, kad DW padarė įvairių BDAR pažeidimų. Todėl 2019 m. spalio 30 d. sprendimu duomenų apsaugos institucija jai skyrė administracines baudas.

DW šį sprendimą apskundė *Landgericht Berlin* (Berlyno apygardos teismas, Vokietija), o šis bylą nutraukė. To teismo teigimu, vadovaujantis Vokietijos teise[121], tik fizinis, o ne juridinis, asmuo gali būti pripažintas padaręs administracinį nusižengimą. Be to, juridinio asmens atsakomybė kyla tik tuomet, kai jam gali būti priskirti jo organų narių ar atstovų veiksmai. *Staatsanwaltschaft Berlin* (Berlyno prokuratūra, Vokietija) šį sprendimą apskundė *Kammergericht Berlin* (Berlyno aukštesnysis apygardos teismas, Vokietija). Šiomis aplinkybėmis minėtas teismas kreipėsi į Teisingumo Teismą su prašymu priimti prejudicinį sprendimą dėl BDAR išaiškinimo.

Teisingumo Teismo didžioji kolegija sprendime pareiškė nuomonę dėl administracinių baudų skyrimo pagal BDAR sąlygų. Pirmiausia ji nagrinėjo klausimą, ar valstybės narės gali administracinės baudos skyrimą juridiniam asmeniui susieti su sąlyga, kad šio reglamento pažeidimas prieš tai būtų priskirtas konkrečiam fiziniam asmeniui. Antra, kaip ir pirma minėtame Sprendime *Nacionalinis visuomenės sveikatos centras*, ji analizavo, ar BDAR nuostatų pažeidimas, už kurį skiriamos sankcijos, turi būti padarytas tyčia arba dėl aplaidumo.

Dėl administracinės baudos skyrimo pagal BDAR juridiniam asmeniui Teisingumo Teismas iš pradžių pažymėjo, kad BDAR numatyti principai, draudimai ir pareigos visų pirma skirti „duomenų valdytojams“, kurių atsakomybė apima bet kokį jų pačių arba jų vardu atliekamą asmens duomenų tvarkymą. Būtent ši atsakomybė BDAR nuostatų pažeidimų atveju yra administracinės baudos skyrimo duomenų valdytojui pagal šio reglamento 83 straipsnį pagrindas. Vis dėlto Sąjungos teisės aktų leidėjas, nustatydamas

[121] 1968 m. gegužės 24 d. *Gesetz über Ordnungswidrigkeiten* (Administracinių nusižengimų įstatymas; *BGBl.*, 1968 I, p. 481) (1987 m. vasario 19 d. paskelbta redakcija (*BGBl.*, 1987 I, p. 602)), iš dalies pakeistas 2020 m. birželio 19 d. įstatymu (*BGBl.*, 2020 I, p. 1350).

atsakomybę, nediferencijavo fizinių ir juridinių asmenų, nes ji siejama su vienintele sąlyga, pagal kurią šie asmenys patys arba kartu su kitais turi nustatyti asmens duomenų tvarkymo tikslus ir priemones[122]. Taigi iš esmės bet kuris šią sąlygą atitinkantis asmuo yra atsakingas už visus savo paties arba jo vardu padarytus BDAR pažeidimus. Tai reiškia, viena vertus, kad juridiniai asmenys yra atsakingi ne tik už savo atstovų, direktorių ar vadovų, bet ir už bet kurio kito asmens, veikiančio įgyvendinant šių juridinių asmenų komercinę veiklą ir jų vardu, padarytus pažeidimus. Kita vertus, BDAR numatytas administracines baudas už tokius pažeidimus turi būti galima skirti tiesiogiai juridiniams asmenims, jeigu jie gali būti laikomi duomenų valdytojais.

Toliau Teisingumo Teismas pažymėjo, kad nė viena BDAR nuostata neleidžia manyti, kad administracinės baudos skyrimas juridiniam asmeniui kaip duomenų valdytojui turi būti siejamas su reikalavimu prieš tai konstatuoti, kad šį pažeidimą padarė konkretus fizinis asmuo. Be to, Sąjungos teisės aktų leidėjas nepaliko valstybėms narėms diskrecijos šiuo klausimu. Tai, kad pagal BDAR joms yra suteikta galimybė numatyti procedūros, kurią turi taikyti priežiūros institucijos skirdamos administracinę baudą, reikalavimus[123], visiškai nereiškia, kad jos taip pat yra įgaliotos numatyti materialines sąlygas, papildančias numatytąsias BDAR.

Atsižvelgdamas į tai, Teisingumo Teismas patikslino, kad jeigu valstybėms narėms būtų leidžiama vienašališkai ir kaip būtinos administracinės baudos skyrimo pagal BDAR 83 straipsnį duomenų valdytojui, kuris yra juridinis asmuo, sąlygos reikalauti, kad aptariamas pažeidimas prieš tai būtų priskirtas arba galėtų būti priskiriamas konkrečiam fiziniam asmeniui, tai prieštarautų BDAR tikslui. Be to, toks papildomas reikalavimas galiausiai galėtų susilpninti juridiniams asmenims kaip duomenų valdytojams skiriamų administracinių baudų veiksmingumą ir atgrasomąjį poveikį.

Galiausiai Teisingumo Teismas pabrėžė, kad sąvoka „įmonė“, kaip ji suprantama pagal SESV 101 ir 102 straipsnius[124], neturi įtakos klausimui, ar ir kokiomis sąlygomis administracinė bauda pagal BDAR gali būti skirta duomenų valdytojui, kuris yra juridinis asmuo, ir yra reikšminga tik nustatant tokios baudos dydį.

Taigi Teisingumo Teismas priėjo prie išvados, kad pagal BDAR[125] draudžiama tokia nacionalinė reglamentavimo tvarka, pagal kurią administracinė bauda gali būti skiriama juridiniam asmeniui kaip duomenų valdytojui už šio reglamento pažeidimą[126] tik jeigu toks pažeidimas prieš tai buvo priskirtas konkrečiam fiziniam asmeniui.

Dėl klausimo, ar valstybės narės gali numatyti administracinių baudų skyrimą net jeigu pažeidimas, už kurį skiriama bauda, nebuvo padarytas tyčia ar dėl aplaidumo, Teisingumo Teismas visų pirma priminė, kad materialinės sąlygos, kurių turi paisyti priežiūros institucija, skirdama administracinę baudą duomenų valdytojui, patenka tik į

[122] BDAR 4 straipsnio 7 punktas.
[123] Kaip matyti iš BDAR 58 straipsnio 4 dalies ir 83 straipsnio 8 dalies, siejamų su jo 129 konstatuojamąja dalimi.
[124] Nurodyta BDAR 150 konstatuojamojoje dalyje.
[125] BDAR 58 straipsnio 2 dalies i punktas ir 83 straipsnio 1–6 dalys.
[126] Numatytą BDAR 83 straipsnio 4–6 dalyse.

Sąjungos teisės taikymo sritį, o valstybės narės šiuo klausimu neturi jokios diskrecijos. Remdamasis taip pačiais argumentais, kurie buvo išdėstyti minėtame Sprendime *Nacionalinis visuomenės sveikatos centras*, Teisingumo Teismas konstatavo, kad administracinė bauda pagal BDAR 83 straipsnį gali būti skirta tik tuo atveju, jeigu įrodyta, kad duomenų valdytojas, kuris kartu yra juridinis asmuo ir įmonė, šiame reglamente įtvirtintas nuostatas pažeidė tyčia arba dėl aplaidumo.

5. Nacionalinių priežiūros institucijų ir kitų nacionalinių valdžios institucijų įgaliojimų sąsaja

2023 m. liepos 4 d. didžiosios kolegijos Sprendimas „Meta Platforms ir kt. (Bendrosios socialinio tinklo naudojimo sąlygos)“ (C-252/21, EU:C:2023:537)

Šioje byloje (taip pat žr. V skyriaus 5 skirsnį „Asmens duomenų tvarkymas internetiniuose socialiniuose tinkluose“) dėl konkurencijos institucijos įgaliojimų konstatuoti, kad asmens duomenų tvarkymas neatitinka BDAR, Teisingumo Teismas nusprendė, kad tokia institucija, jeigu laikosi lojalaus bendradarbiavimo su duomenų apsaugos priežiūros institucijomis pareigos[127], nagrinėdama įmonės piktnaudžiavimą dominuojančia padėtimi[128], gali konstatuoti, kad šios įmonės nustatytos bendrosios naudojimo sąlygos asmens duomenų tvarkymo srityje ir jų įgyvendinimas neatitinka šio reglamento, kai tokia išvada būtina siekiant nustatyti piktnaudžiavimą dominuojančia padėtimi. Vis dėlto, kai konkurencijos institucija, konstatuodama piktnaudžiavimą dominuojančia padėtimi, nustato BDAR pažeidimą, ji nepakeičia priežiūros institucijų.

Taigi, atsižvelgiant į lojalaus bendradarbiavimo principą, kai nacionalinės konkurencijos institucijos, vykdydamos savo įgaliojimus, turi išnagrinėti, ar įmonės elgesys atitinka BDAR nuostatas, jos turi tartis ir lojaliai bendradarbiauti su atitinkamomis nacionalinėmis priežiūros institucijomis arba vadovaujančia priežiūros institucija. Vadinasi, visos šios institucijos privalo laikytis savo atitinkamų įgaliojimų, kad būtų paisoma iš BDAR kylančių pareigų, šio reglamento tikslų ir užtikrintas jų veiksmingumas. Darytina išvada, kad, kai konkurencijos institucija, nagrinėdama įmonės piktnaudžiavimą dominuojančia padėtimi, mano, kad būtina išnagrinėti, ar šios įmonės elgesys atitinka BDAR nuostatas, ji turi patikrinti, ar dėl šio arba panašaus elgesio jau buvo priimtas kompetentingos nacionalinės priežiūros institucijos, vadovaujančios priežiūros institucijos arba Teisingumo Teismo sprendimas. Jei taip yra, konkurencijos institucija negali nukrypti nuo tokio sprendimo, tačiau gali padaryti savo išvadas dėl konkurencijos teisės taikymo.

Kai konkurencijos institucijai kyla abejonių dėl kompetentingos nacionalinės priežiūros institucijos arba vadovaujančios priežiūros institucijos atlikto vertinimo apimties, kai šios

[127] Įtvirtintos ESS 4 straipsnio 3 dalyje.
[128] Kaip tai suprantama pagal SESV 102 straipsnį.

institucijos tuo pačiu metu nagrinėja atitinkamą ar panašų elgesį, arba, nesant minėtų institucijų tyrimo, ji mano, kad įmonės elgesys neatitinka BDAR nuostatų, prieš pradėdama savo vertinimą ji turi konsultuotis su šiomis institucijomis ir prašyti jų bendradarbiauti, kad išsklaidytų savo abejones arba nustatytų, ar prieš pradėdama savo vertinimą turi laukti, kol atitinkama priežiūros institucija priims sprendimą. Jeigu priežiūros institucijos neprieštarauja arba neatsako per pagrįstą laikotarpį, nacionalinė konkurencijos institucija gali tęsti savo tyrimą.

EUROPOS SĄJUNGOS
TEISINGUMO TEISMAS

Tyrimų ir dokumentacijos direktoratas

2024 m. liepos mėn.