Byla C-793/19

Prašymo priimti prejudicinį sprendimą santrauka pagal Teisingumo Teismo procedūros reglamento 98 straipsnio 1 dalį

Gavimo data:

2019 m. spalio 29 d.

Prašymą priimti prejudicinį sprendimą pateikęs teismas:

Bundesverwaltungsgericht (Vokietija)

Nutarties dėl prašymo priimti prejudicinį sprendimą priėmimo data:

2019 m. rugsėjo 25 d.

Pareiškėja ir kita kasacinio proceso šalis:

SpaceNet AG

Atsakovė ir kasatorė:

Vokietijos Federacinė Respublika

Pagrindinės bylos dalykas

Ieškinys dėl pripažinimo, kad *SpaceNet* neprivalo saugoti *Telekommunikationsgesetz* (Telekomunikacijų įstatymas, toliau – TKG) 113b straipsnio 3 dalyje nurodytų savo klientų, kuriems ji teikia interneto prieigos paslaugas, telekomunikacijų srauto duomenų.

Prašymo priimti prejudicinį sprendimą dalykas ir teisinis pagrindas

Sąjungos teisės, visų pirma Direktyvos 2002/58 15 straipsnio 1 dalies ir Sprendimo *Tele2 Sverige ir Watson ir kt.* išaiškinimas; SESV 267 straipsnis

Prejudicinis klausimas

Ar, atsižvelgiant į Europos Sąjungos pagrindinių teisių chartijos 7, 8 ir 11 straipsnius bei 52 straipsnio 1 dalį, iš vienos pusės, ir į Europos Sąjungos pagrindinių teisių chartijos 6 straipsnį ir Europos Sąjungos Sutarties 4 straipsnį, iš kitos pusės, Direktyvos 2002/58/EB 15 straipsnį reikia aiškinti taip, kad jam

prieštarauja nacionalinės teisės norma, kuria viešai prieinamų elektroninių ryšių paslaugų teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis, jeigu šis įpareigojimas:

– nenustato jokių konkrečių pagrindų vietos, laiko ar teritorijos atžvilgiu,

– pareiga saugoti duomenis teikiant viešai prieinamas telefonijos paslaugas – įskaitant trumpųjų, multimedijos ir panašių žinučių perdavimą bei neatsakytus ar nesėkmingus skambučius – apima šiuos duomenis:

  – telefono numerius ar kitus identifikatorius, į kuriuos ir iš kurių skambinta, o skambučio perjungimo ar persiuntimo atvejais – telefono numerius ar kitus identifikatorius, į kuriuos skambutis buvo perjungtas ar persiųstas,

  – ryšio pradžios ir pabaigos datą ir laiką arba – trumposios, multimedijos ir pan. žinutės perdavimo atveju – žinutės išsiuntimo ir gavimo momentą, nurodant laiko juostą,

  – paslaugos, kuria naudojamasi, duomenis, jeigu telefonijos paslauga apima įvairių paslaugų galimybes,

  – be to, mobiliųjų telefonijos paslaugų atveju:

    – skambinančių abonentų ir abonentų, kuriems skambinama, tarptautinį identifikatorių,

    – galinio įrenginio, į kurį ir iš kurio skambinta, tarptautinį identifikatorių,

    – paslaugos pirmojo aktyvinimo datą ir laiką, nurodant laiko juostą, jeigu paslaugos buvo apmokėtos iš anksto,

    – ryšio prieigos taškų, kuriais skambinantysis abonentas ir abonentas, kuriam buvo skambinta, naudojosi ryšio pradžioje, pavadinimai,

  – internetinės telefonijos paslaugų atveju – ir skambinančiojo abonento bei abonento, kuriam buvo skambinta, interneto protokolo adresus bei priskirtus naudotojo identifikatorius,

– pareiga saugoti duomenis teikiant viešai prieinamas interneto prieigos paslaugas apima šiuos duomenis:

  – abonentui naudojimosi internetu tikslais priskirtą interneto protokolo adresą,

  – unikalų interneto prieigos taško identifikatorių bei priskirtą naudotojo identifikatorių,

  - interneto naudojimo per priskirtą interneto protokolo adresą pradžios ir pabaigos datą ir laiką, nurodant laiko juostą,

  - mobilaus naudojimosi atveju – ryšio prieigos taško, kuriuo buvo naudojamasi interneto ryšio pradžioje, pavadinimą,

- draudžiama saugoti šiuos duomenis:

  - pranešimo turinį,

  - duomenis apie iškviestus tinklapius,

  - elektroninio pašto paslaugų duomenis,

  - socialinei ar bažnytinei sričiai priklausančių asmenų, institucijų ir organizacijų, su kuriomis susisiekiama arba kurie susisiekia, ryšių duomenis,

- vietos nustatymo duomenų, t. y. naudoto ryšio prieigos taško pavadinimo, saugojimo trukmė yra keturios savaitės, kitų duomenų – dešimt savaičių,

- užtikrinama veiksminga saugomų duomenų apsauga nuo piktnaudžiavimo rizikos ir nuo neteisėtos prieigos, ir

- saugomus duomenis leidžiama naudoti tik ypač sunkių nusikalstamų veikų persekiojimo tikslu ir siekiant užkirsti kelią konkrečiam pavojui, kuris kilo asmens sveikatai, gyvybei ar laisvei arba valstybei ar federalinei žemei, išskyrus abonentui priskirtą interneto protokolo adresą, kurį leidžiama naudoti renkant informaciją bet kokių nusikalstamų veikų persekiojimo tikslu, siekiant užkirsti kelią pavojui, kuris kilo visuomenės saugumui ir viešajai tvarkai, bei vykdant žvalgybos uždavinius?

Nurodomos Sąjungos teisės nuostatos

Europos Sąjungos pagrindinių teisių chartija (toliau – Pagrindinių teisių chartija), 6, 7, 8, 11, 52 straipsniai

Europos Sąjungos sutartis (ESS), 4, 6 straipsniai

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) su pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (toliau – Direktyva 2002/58), 5, 6, 8, 9 straipsniai, visų pirma 15 straipsnis; 11 konstatuojamoji dalis

Nurodomos nacionalinės teisės nuostatos

Telekommunikationsgesetz (Telekomunikacijų įstatymas, toliau – TKG), 113a straipsnio 1 dalies pirmas sakinys („Įpareigoti asmenys“), 113b straipsnis („Pareigos saugoti srauto duomenis“), 113c straipsnis („Duomenų naudojimas“), 113d straipsnis („Duomenų saugumo užtikrinimas“), 113e straipsnis („Protokolavimas“ [atliekamas asmens, įpareigoto turėti prieigą prie saugomų duomenų]), 113f straipsnis („Reikalavimų sąrašas“ [dėl techninių ir kitų priemonių]), 99 straipsnio 2 dalis („Detali sąskaita“, detalių sąskaitų duomenys, kuriems netaikomas atpažįstamumas)

Strafprozessordnung (Baudžiamojo proceso kodeksas, toliau – *StPO*), 100g straipsnio 2 dalis („Srauto duomenų rinkimas“ pagal TKG 113b straipsnį)

Nurodoma Teisingumo Teismo jurisprudencija

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, toliau – Sprendimas *Tele2 Sverige ir Watson ir kt.*)

2014 m. balandžio 8 d. Sprendimas *Digital Rights Ireland ir Seitlinger ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238, toliau – Sprendimas *Digital Rights Ireland ir kt.*)

2017 m. liepos 26 d. Nuomonė 1/15 (EU:C:2017:592)

Be to: 2019 m. liepos 29 d. Sprendimas *Funke Medien* (C-469/17, EU:C:2019:623), 1978 m. kovo 9 d. Sprendimas *Simmenthal* (106/77, EU:C:1978:49), 2005 m. gegužės 3 d. Sprendimas *Berlusconi ir kt.* (C-387/02, C-391/02 ir C-403/02, EU:C:2005:270), 2010 m. birželio 22 d. Sprendimas *Melki ir Abdeli* (C-188/10 ir C-189/10, EU:C:2010:363), 2014 m. rugsėjo 18 d. Sprendimas *Vueling Airlines* (C-487/12, EU:C: 2014:2232).

Trumpas faktinių aplinkybių ir proceso pagrindinėje byloje aprašymas

1 Kasatorė, *SpaceNet AG* (toliau – pareiškėja arba *SpaceNet*), teikia viešai prieinamas interneto prieigos paslaugas. Ji nesutinka su *Telekommunikationsgesetz* (Telekomunikacijų įstatymas, toliau – TKG), iš dalies pakeisto 2015 m. gruodžio 10 d. įstatymu, 113a straipsnio 1 dalyje, siejamoje su 113b straipsniu, nustatytu įpareigojimu nuo 2017 m. liepos 1 d. saugoti savo klientų telekomunikacijų srauto duomenis.

2 Pirmosios instancijos administracinis teismas konstatavo, kad *SpaceNet* neprivalo saugoti TKG 113b straipsnio 3 dalyje nurodytų savo klientų, kuriems ji suteikia interneto prieigą, telekomunikacijų srauto duomenų. Administracinio teismo

sprendimą kita kasacinio proceso šalis, Vokietijos Federacinė Respublika (toliau – atsakovė), apskundė tiesioginiu kasaciniu skundu.

3 Kasacinį skundą reikia patenkinti tik tuo atveju, jeigu minėtose TKG normose nustatyta viešai prieinamų telekomunikacijų paslaugų teikėjų (toliau – telekomunikacijų operatoriai) pareiga saugoti telekomunikacijų srauto duomenis nepažeidžia Sąjungos teisės.

4 Telekomunikacijų operatorių pareiga ribotą laiką saugoti tam tikrus srauto duomenis buvo naujai reglamentuota 2015 m. gruodžio 10 d. *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten* (Pareigos saugoti srauto duomenis ir maksimalaus saugojimo termino nustatymo įstatymas, toliau – 2015 m. gruodžio 10 d. įstatymas).

5 Naujai reglamentuoti ją reikėjo po to, kai *Bundesverfassungsgericht* (Federalinis Konstitucinis Teismas) 2010 m. sprendimu pripažino ankstesnes duomenų saugojimą reglamentuojančias normas pažeidžiančiomis pagrindines teises ir todėl negaliojančiomis, ir po to, kai Sprendimu *Digital Rights Ireland ir kt.* negaliojančia buvo pripažinta Direktyva 2006/24, kurią perkeliant į nacionalinę teisę šios ankstesnės normos buvo priimtos. 2015 m. gruodžio 10 d. įstatymu siekiama užpildyti spragas baudžiamojo persekiojimo ir saugumo srityje, atsižvelgiant į iš pirmiau minėtų sprendimų išplaukiančius konstitucinės ir Europos teisės reikalavimus.

6 Norint atsakyti į klausimą, ar TKG 113a straipsnio 1 dalyje, siejamoje su 113b straipsniu, nustatyta pareiga saugoti duomenis pažeidžia Sąjungos teisę, reikia, kad Teisingumo Teismas išaiškintų Direktyvą 2002/58; pirmiausia reikia atsakymo į tai, kaip turi būti aiškinamas Sprendimas *Tele2 Sverige ir Watson ir kt.*

Glaustas prašymo priimti prejudicinį sprendimą pagrindimas

7 TKG 113a straipsnio 1 dalies pirmame sakinyje, siejamame su 113b straipsniu, nustatyta pareiga saugoti telekomunikacijų srauto duomenis riboja Direktyvos 2002/58 5 straipsnio 1 dalyje, 6 straipsnio 1 dalyje ir 9 straipsnio 1 dalyje numatytas teises.

8 Ja kišamasi į direktyvos 5 straipsnio 1 dalies pirmu sakiniu saugomą elektroninių ryšių konfidencialumą ir ji prieštarauja principui, kad bet kuriam asmeniui, kuris nėra naudotojas, draudžiama be naudotojų sutikimo kaupti su elektroniniais ryšiais susijusius srauto duomenis.

9 Be to, ji neatitinka direktyvos 6 straipsnyje suformuluoto reikalavimo, kad srauto duomenis galima tvarkyti ir saugoti tik tokia apimtimi ir tiek laiko, kiek būtina siekiant abonentams pateikti sąskaitas už paslaugas bei tokių paslaugų teikimui ar rinkodarai.

10 Kai vietos nustatymo duomenys, nesudarantys srauto duomenų, susiję su viešųjų ryšių tinklų ar viešųjų elektroninių ryšių naudotojais ar abonentais, gali būti tvarkomi, Direktyvos 2002/58 9 straipsnio 1 dalies pirmame sakinyje nustatyta, kad juos galima tvarkyti tik jeigu jie yra pakeisti taip, kad taptų anoniminiais, arba jeigu naudotojai ar abonentai sutinka su tokiu tvarkymu tokia apimtimi ir tiek laiko, kiek yra būtina teikti pridėtinės vertės paslaugai. Šio reikalavimo įstatymo norma taip pat neatitinka, kiek pagal TKG 113b straipsnio 1 dalies 2 punktą, siejamą su 4 dalimi, privaloma saugoti ir ten nurodytus vietos nustatymo duomenis.

11 Direktyvos 2002/58/EB 5 straipsnio 1 dalyje, 6 straipsnio 1 dalyje ir 9 straipsnio 1 dalyje numatytų teisių ribojimas yra pagrįstas tik tada, kai TKG 113a straipsnio 1 dalies pirmą sakinį, siejamą su 113b straipsniu, galima pagrįsti Direktyvos 2002/58 15 straipsnio 1 dalimi.

12 Joje numatyta, kad valstybės narės gali patvirtinti teisines priemones, ribojančias šios direktyvos 5 ir 6 straipsniuose, 8 straipsnio 1, 2, 3 ir 4 dalyse ir 9 straipsnyje nustatytų teisių ir pareigų taikymą, jeigu toks ribojimas yra būtina, tinkama ir adekvati demokratinės visuomenės priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą, kaip nurodyta Direktyvos 95/46 13 straipsnio 1 dalyje. Tam valstybės narės gali, *inter alia*, patvirtinti teisines priemones, leidžiančias ribotą laikotarpį saugoti duomenis, remiantis šioje dalyje nustatytais motyvais. Visos šioje dalyje nurodytos priemonės turi atitikti bendruosius Bendrijos teisės principus, tarp jų ir nurodytus Europos Sąjungos Sutarties (ESS) 6 straipsnio 1 ir 2 dalyse.

13 Sprendime *Tele2 Sverige ir Watson ir kt.*, visų pirma 82 ir paskesniuose bei 108 ir paskesniuose punktuose, Teisingumo Teismas yra išaiškinęs, kad duomenų saugojimą reglamentuojanti nacionalinė teisės norma, grindžiama Direktyvos 2002/58 15 straipsnio 1 dalimi, yra leistina tik tuo atveju, jeigu yra pakankamas pagrindas. Tai reiškia, kad ji gali būti taikoma tik tiems asmenims, kurie suteikia pagrindo manyti, kad yra susiję su sunkiomis nusikalstamomis veikomis, kad priemonė taikoma tik tame regione, tuo laikotarpiu ir toms ryšių priemonėms, kurios yra susijusios su pagrindu, ir kad renkami tik tie duomenys, kurie yra būtini minėtoms nusikalstamoms veikoms išaiškinti.

14 Atsakovės nuomonė, kad jau vien naudojimasis interneto prieigos arba telefonijos paslaugomis laikytinas pakankamu pagrindu duomenims saugoti, akivaizdžiai tam prieštarauja. Sprendime *Tele2 Sverige ir Watson ir kt.* nustatytos bendros prielaidos, kad bet koks neturintis pagrindo duomenų saugojimas prieštarauja Sąjungos teisei, nepaneigia ir atsakovės nuoroda į 2017 m. liepos 26 d. Teisingumo Teismo nuomonę dėl Kanados ir Europos Sąjungos susitarimo dėl keleivio duomenų įrašo (PNR) duomenų perdavimo. Teisingumo Teismas, pažymėdamas, kad susitarimu grindžiamas pagrindinių teisių į privataus gyvenimo gerbimą ir į asmens duomenų apsaugą ribojimas yra būtinas, pabrėžė, jog PNR duomenys Kanadai perduodami neatsižvelgiant į tai, ar yra kokių nors

objektyvių elementų, leidžiančių manyti, kad keleiviai gali kelti pavojų visuomenės saugumui Kanadoje. Tačiau tai nėra neturintis pagrindo duomenų saugojimas, nes jie saugomi ir perduodami vykdant patikrą pasienyje, kurią turi praeiti visi į Kanadą norintys atvykti arba išvykti iš jos oro keleiviai, laikydamiesi galiojančiuose Kanados teisės aktuose nustatytų sąlygų. Oro keleiviams išvykus iš Kanados, šis pagrindas saugoti duomenis išnyksta. Todėl po išvykimo gali būti saugomi tik tų keleivių PNR duomenys, kurių atžvilgiu egzistuoja objektyvių elementų, leidžiančių manyti, kad šie keleiviai gali kelti riziką kovojant su terorizmu ir sunkiais tarpvalstybiniais nusikaltimais (naujas pagrindas).

15 Jeigu Teisingumo Teismo jurisprudenciją reikia aiškinti taip, kad duomenų saugojimas be pagrindo jokiomis aplinkybėmis nėra suderinamas su Sąjungos teise, atsakovės kasacinis skundas, pareikštas dėl skundžiamo administracinio teismo sprendimo, negali būti patenkintas. Juk kaip ir Sprendime *Tele2 Sverige ir Watson ir kt.* nagrinėti Švedijos ir Didžiosios Britanijos teisės aktai, reglamentuojantys duomenų saugojimą, TKG 113a straipsnio 1 dalies pirmame sakinyje, siejamame su 113b straipsniu, nereikalaujama nei (kitokio, nei paprastas naudojimasis interneto prieigos arba telefonijos paslaugomis) pagrindo duomenims saugoti, nei saugomų duomenų ryšio su nusikalstama veika ar pavojumi visuomenės saugumui. Veikiau šiomis teisės normomis nurodoma be jokio pagrindo saugoti didžiąją visoje teritorijoje surenkamų atitinkamų telekomunikacijų srauto duomenų dalį, nediferencijuojant jų pagal asmenis, laiką ir geografiją.

16 Tačiau prašymą priimti prejudicinį sprendimą teikiantis teismas, nepaisant paaiškinimų Sprendime *Tele2 Sverige ir Watson ir kt.*, neatmeta galimybės, kad TKG 113a straipsnio 1 dalies pirmame sakinyje, siejamame su 113b straipsniu, nustatyta pareiga be pagrindo saugoti telekomunikacijų srauto duomenis gali būti grindžiama Direktyvos 2002/58 15 straipsnio 1 dalimi dėl toliau nurodytų priežasčių:

17 Pirma, pagal nagrinėjamas TKG normas nereikalaujama saugoti visų abonentų ir registruotų naudotojų visų telekomunikacijų srauto duomenų, kiek tai susiję su visomis elektroninių ryšių priemonėmis. Saugojimo pareiga netaikoma ne tik ryšių turiniui – draudžiama saugoti duomenis apie iškviestus tinklapius, elektroninio pašto paslaugų duomenis bei socialinei ar bažnytinei sričiai priklausančių asmenų, institucijų ir organizacijų, su kuriomis susisiekiama arba kurie susisiekia, ryšių duomenis (žr. TKG 113b straipsnio 5 ir 6 dalis). Saugojimo pareigos netaikant tam tikroms ryšių priemonėms ar duomenų kategorijoms, išsamaus atitinkamų asmenų profilio sukūrimo rizika išlieka, tačiau ji gerokai sumažinama.

18 Antra, dar svaresnį skirtumą tarp šioje byloje nagrinėjamų TKG normų ir ankstesnių Direktyvos 2006/24 normų bei jomis grindžiamų Švedijos ir Didžiosios Britanijos teisės aktų, kurie buvo nagrinėjami Sprendime *Tele2 Sverige ir Watson ir kt.*, prašymą priimti prejudicinį sprendimą teikiantis teismas įžvelgia aplinkybėje, kad nuo šešių mėnesių iki dviejų metų siekiantis saugojimo

laikotarpis (žr. Direktyvos 2006/24 6 straipsnį) TKG 113b straipsnio 1 dalyje gerokai sutrumpintas – iki keturių–dešimties savaičių.

19 Pavojus, kad bus sudarytas išsamus atitinkamų asmenų profilis, laikytinas tuo mažesniu, kuo trumpesni yra laikotarpiai, kurių metu saugomi srauto duomenys. Kuo trumpesnis saugojimo laikotarpis, su tuo didesnėmis spragomis savaime bus asmenybės profilis ir tuo mažiau ribojamos pagrindinės teisės.

20 Trečia, nagrinėjamoms TKG normoms taikomi griežti apribojimai saugomų duomenų apsaugos ir prieigos prie jų požiūriu. Viena vertus, TKG 113d ir paskesnių straipsnių reikalavimais užtikrinama veiksminga saugomų duomenų apsauga nuo piktnaudžiavimo rizikos ir neteisėtos prieigos. Kita vertus, saugomus duomenis pagal TKG 113c straipsnio 1 dalį leidžiama naudoti tik ypač sunkių nusikalstamų veikų persekiojimo tikslu ir siekiant užkirsti kelią konkrečiam pavojui, kuris kilo asmens sveikatai, gyvybei ar laisvei arba valstybei ar federalinei žemei.

21 Pagal *StPO* 100g straipsnio 2 dalį rinkti srauto duomenis baudžiamojo persekiojimo tikslais leidžiama tik tuo atveju, jeigu asmuo įtariamas įstatyme aiškiai apibrėžtomis ypač sunkiomis nusikalstamomis veikomis, nusikalstama veika ir konkrečiu atveju yra labai sunki, ištirti bylos aplinkybes arba nustatyti įtariamojo buvimo vietą kitais būdais būtų labai sunku arba neįmanoma ir duomenų rinkimas yra proporcingas bylos reikšmei. Pagal *StPO* 100g straipsnio 4 dalį draudžiama rinkti arba tvarkyti *StPO* 53 straipsnio 1 dalies pirmo sakinio 1-5 punktuose nurodytų profesinę paslaptį privalančių saugoti asmenų, kuriems priklauso, pavyzdžiui, advokatai, gydytojai arba žurnalistai, srauto duomenis. Be to, *StPO* 101a straipsnio 1 dalyje nustatyta, kad rinkti srauto duomenis, kaip tai numatyta *StPO* 100g straipsnyje, galima tik gavus teismo leidimą.

22 Šie prieigos apribojimai netaikomi abonentui naudojimosi internetu tikslais priskirtam interneto protokolo adresui. TKG 113c straipsnio 1 dalies 3 punkte numatyta, kad jį leidžiama naudoti renkant informaciją bet kokių nusikalstamų veikų persekiojimo tikslu, siekiant užkirsti kelią pavojui, kuris kilo visuomenės saugumui ir viešajai tvarkai, bei bendrai vykdant žvalgybos uždavinius. Tiesa, manytina, kad informacija, kuris abonentas jau žinomu interneto protokolo adresu buvo prisijungęs internete, neleidžia sudaryti asmenybės ir judėjimo profilių.

23 Net ir pripažįstant *SpaceNet* argumentus ir laikant, kad vis labiau naudojami techniniai būdai, kurių atveju interneto protokolo adresas rodo ne konkretų telekomunikacijų tinklo adresą, o didesnę adresų grupę, ir todėl informacijos rinkimas yra tapęs labai plačia priemone, visgi renkant informaciją tokiu būdu į asmenų teises kišamasi daug mažiau negu tuo atveju, kai renkami ir tvarkomi telekomunikacijų srauto duomenys.

24 Ketvirta, prielaidą, kad TKG 113a straipsnio 1 dalies pirmame sakinyje, siejamame su 113b straipsniu, nustatyta pareiga be pagrindo saugoti telekomunikacijų srauto duomenis gali būti grindžiama Direktyvos 2002/58

15 straipsnio 1 dalimi, patvirtina ir tai, kad nacionalinis teisės aktų leidėjas, ją nustatydamas, įvykdė savo pareigas, valstybėms narėms numatytas Pagrindinių teisių chartijos 6 straipsnyje, kuris garantuoja teisę į saugumą. Sprendime *Digital Rights Ireland ir kt.* Teisingumo Teismas aiškiai paminėjo Pagrindinių teisių chartijos 6 straipsnį, pažymėdamas, kad kova su tarptautiniu terorizmu siekiant palaikyti tarptautinę taiką ir saugumą yra bendrasis Sąjungos tikslas ir kad tas pat pasakytina apie kovą su sunkiais nusikaltimais siekiant užtikrinti visuomenės saugumą.

25 Atsižvelgdamas į tai, prašymą priimti prejudicinį sprendimą teikiantis teismas abejoja, ar suformuotą Teisingumo Teismo jurisprudenciją reikia aiškinti taip, kad neturintis pagrindo duomenų saugojimas draudžiamas ne tik toks, koks buvo konkrečiai numatytas Direktyvoje 2006/24 ir ja grindžiamuose Švedijos ir Didžiosios Britanijos teisės aktuose, bet kad jo apskritai negalima grįsti Direktyvos 2002/58 15 straipsnio 1 dalimi. Juk pagrindinės duomenų saugojimo koncepcijos neįmanoma suderinti su Teisingumo Teismo besąlygiškai suformuluotu reikalavimu saugant duomenis diferencijuoti pagal asmenis, laikotarpius ir geografines sritis.

26 Prielaidą, kad neturintis pagrindo srauto duomenų saugojimas *per se* yra nesuderinamas su Pagrindinių teisių chartija, prašymą priimti prejudicinį sprendimą teikiančio teismo nuomone, paneigia ir reikalavimas išlaikyti pusiausvyrą tarp valstybėms narėms tenkančios pareigos užtikrinti jų teritorijoje esančių asmenų saugumą ir Pagrindinių teisių chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių gerbimo.

27 Todėl prašymą priimti prejudicinį sprendimą teikiantis teismas negali būti visiškai tikras, kad pagal Teisingumo Teismo jurisprudenciją nacionaliniai teisės aktų leidėjai nebeturi turėti galimybės, įvertinę visas reikšmingas aplinkybes, taikyti (jei reikia, papildant griežtu prieigos reglamentavimu) duomenų saugojimą be pagrindo siekiant užkirsti kelią konkretiems pavojams, susijusiems su naujomis telekomunikacijų priemonėmis.

28 Penkta, prašymą priimti prejudicinį sprendimą teikiantis teismas pažymi, kad tuo atveju, jeigu paaiškėtų, jog neturinčio pagrindo duomenų saugojimo apskritai negalima grįsti Direktyvos 2002/58 15 straipsnio 1 dalimi ir kad todėl konkretus atitinkamų komunikacijos priemonių, saugotinų duomenų kategorijų, saugojimo trukmės, prieigos prie saugomų duomenų sąlygų ir apsaugos nuo piktnaudžiavimo reglamentavimas neturi reikšmės, nacionalinių teisės aktų leidėjų veiksmų laisvė baudžiamojo persekiojimo ir viešojo saugumo srityje, už kurią pagal ESS 4 straipsnio 2 dalies trečią sakinį iš principo ir toliau atsako valstybės narės, būtų gerokai apribota.

29 Galiausiai, šešta, prašymą priimti prejudicinį sprendimą teikiančiam teismui, net ir atsižvelgiant į naujesnę Europos Žmogaus Teisių Teismo (toliau – EŽTT) jurisprudenciją, lieka neaišku, ar Teisingumo Teismo paaiškinimus Sprendime *Tele2 Sverige ir Watson ir kt.* reikia suprasti kaip draudimą valstybėms narėms

pareigos be pagrindo saugoti telekomunikacijų srauto duomenis taikymą grįsti Direktyvos 2002/58 15 straipsnio 1 dalimi.

30 2018 m. birželio 19 d. sprendime EŽTT nusprendė, kad Švedijos teisės aktai, reglamentuojantys masinį tarpvalstybinių duomenų srautų stebėjimą, yra suderinami su Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (EŽTK) 8 straipsniu. EŽTT konstatavo, kad, atsižvelgiant į valstybėms šiuo metu kylančias grėsmes, įskaitant globalų terorizmą ir kitus sunkius nusikaltimus, kaip antai prekyba narkotikais, prekyba žmonėmis, seksualinis vaikų išnaudojimas ir elektroniniai nusikaltimai, bei dėl techninės pažangos, kuri padeda teroristams ir nusikaltėliams išvengti aptikimo internete, ir dėl negalėjimo numatyti, kokiais būdais bus perduoti elektroniniai duomenys, sprendimas taikyti masinį stebėjimą siekiant identifikuoti iki šiol nežinomas grėsmes nacionaliniam saugumui ir toliau išlieka valstybės diskrecijoje (2018 m. birželio 19 d. EŽTT sprendimas Nr. 35252/08 [CE:ECHR:2018:0619JUD003525208], *Centrum för Rättvisa / Švedija*, 112 punktas). EŽTT, darydamas nuorodą į negalėjimą numatyti, kokiais būdais bus perduoti elektroniniai duomenys, bei į techninę pažangą, kuri padeda teroristams ir nusikaltėliams išvengti aptikimo internete, labiau nei Europos Sąjungos Teisingumo Teismas pabrėžia galimus specifinius pavojus, susijusius su naujomis ryšių priemonėmis.

31 Prašymą priimti prejudicinį sprendimą teikiantis teismas daro nuorodą į Direktyvos 2002/58 11 konstatuojamąją dalį ir Pagrindinių teisių chartijos 52 straipsnio 3 dalį, iš kurių matyti, kad siekiama užtikrinti būtiną Chartijoje įtvirtintų teisių, atitinkančių EŽTK užtikrinamas teises, darnumą, nedarant neigiamos įtakos Sąjungos teisės ir Europos Sąjungos Teisingumo Teismo autonomijai.

32 Pabaigoje prašymą priimti prejudicinį sprendimą teikiantis teismas nurodo kitus nagrinėjamus prašymus priimti prejudicinį sprendimą, kuriuose prašoma išaiškinti Sprendimą *Tele2 Sverige ir Watson ir kt.*, klausiant, ar iš pastarojo galima kildinti bendrą draudimą saugoti duomenis be pagrindo ir ar, nepaisant grėsmių viešajam saugumui rimtumo, šis draudimas neišnyksta net ir „kompensuojant“ duomenų rinkimo priemonių griežtu prieigos prie jų reglamentavimu ir aukštais saugumo reikalavimais.

33 Minimi *Investigatory Powers Tribunal – London* (Jungtinė Karalystė) prašymas priimti prejudicinį sprendimą (C-623/17), *Conseil d'État* (Prancūzija) prašymai priimti prejudicinį sprendimą (C-511/18 ir C-512/18) ir Belgijos *Verfassungsgerichtshof* prašymas priimti prejudicinį sprendimą (C-520/18).