Teismo praktikos rinkinys

TEISINGUMO TEISMO (didžioji kolegija) SPRENDIMAS

2022 m. rugsėjo 20 d.*

[Tekstas ištaisytas 2022 m. spalio 27 d. nutartimi]

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas elektroninių ryšių sektoriuje – Ryšių konfidencialumas – Elektroninių ryšių paslaugų teikėjai – Bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas – Direktyva 2002/58/EB – 15 straipsnio 1 dalis – Europos Sąjungos pagrindinių teisių chartija – 6, 7, 8 ir 11 straipsniai, 52 straipsnio 1 dalis – ESS 4 straipsnio 2 dalis“

Sujungtose bylose C-793/19 ir C-794/19

dėl *Bundesverwaltungsgericht* (Federalinis administracinis teismas, Vokietija) 2019 m. rugsėjo 25 d. nutartimis, kurias Teisingumo Teismas gavo 2019 m. spalio 29 d., pagal SESV 267 straipsnį pateiktų prašymų priimti prejudicinį sprendimą bylose

Bundesrepublik Deutschland, atstovaujama *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*,

prieš

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19)

TEISINGUMO TEISMAS (didžioji kolegija),

kurį sudaro pirmininkas K. Lenaerts, kolegijų pirmininkai A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis ir I. Ziemele, teisėjai T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (pranešėjas), N. Piçarra, L. S. Rossi ir A. Kumin,

generalinis advokatas M. Campos Sánchez-Bordona,

posėdžio sekretorius D. Dittert, skyriaus vadovas,

atsižvelgęs į rašytinę proceso dalį ir įvykus 2021 m. rugsėjo 13 d. posėdžiui,

* Proceso kalba: vokiečių.

išnagrinėjęs pastabas, pateiktas:

– *Bundesrepublik Deutschland*, atstovaujamos *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, atstovaujamos C. Mögelin,

– [Ištaisyta 2022 m. spalio 27 d. nutartimi] *SpaceNet AG*, atstovaujamos *Universitätsprofessor* M. Bäcker,

– *Telekom Deutschland GmbH*, atstovaujamos *Rechtsanwalt* T. Mayen,

– Vokietijos vyriausybės, atstovaujamos J. Möller, F. Halibi, M. Hellmann, D. Klebs ir E. Lankenau,

– Danijos vyriausybės, atstovaujamos M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen ir M. Søndahl Wolff,

– Estijos vyriausybės, atstovaujamos A. Kalbus ir M. Kriisa,

– Airijos, atstovaujamos A. Joyce ir J. Quaney, padedamų BL D. Fennelly ir SC P. Gallagher,

– Ispanijos vyriausybės, atstovaujamos L. Aguilera Ruiz,

– Prancūzijos vyriausybės, atstovaujamos A. Daniel, D. Dubois, J. Illouz, E. de Moustier ir T. Stéhelin,

– Kipro vyriausybės, atstovaujamos I. Neophytou,

– Nyderlandų vyriausybės, atstovaujamos M. K. Bulterman, A. Hanje ir C. S. Schillemans,

– Lenkijos vyriausybės, atstovaujamos B. Majczyna, D. Lutostańska ir J. Sawicka,

– Suomijos vyriausybės, atstovaujamos A. Laine ir M. Pere,

– Švedijos vyriausybės, atstovaujamos H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson ir H. Shev,

– Europos Komisijos, atstovaujamos G. Braun, S. L. Kalėdos, H. Kranenborg, M. Wasmeier ir F. Wilman,

– Europos duomenų apsaugos priežiūros pareigūno, atstovaujamo A. Buchta, D. Nardi, N. Stolič ir K. Ujazdowski,

susipažinęs su 2021 m. lapkričio 18 d. posėdyje pateikta generalinio advokato išvada,

priima šį

Sprendimą

1 Prašymai priimti prejudicinį sprendimą pateikti dėl 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 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), iš dalies pakeistos 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (OL L 337, 2009, p. 11) (toliau – Direktyva 2002/58), 15 straipsnio 1 dalies, siejamos su Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 6–8 ir 11 straipsniais, 52 straipsnio 1 dalimi ir ESS 4 straipsnio 2 dalimi, išaiškinimo.

2 Šie prašymai pateikti nagrinėjant *Bundesrepublik Deutschland* (Vokietijos Federacinė Respublika), atstovaujamos *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (Federalinė elektros energijos, dujų, telekomunikacijų, pašto ir geležinkelių tinklų tarnyba, Vokietija), ginčą su *SpaceNet AG* (byla C-793/19) ir *Telekom Deutschland GmbH* (byla C-794/19) dėl pastarosioms nustatytos pareigos saugoti jų klientų telekomunikacijų srauto ir vietos nustatymo duomenis.

Teisinis pagrindas

Sąjungos teisė

Direktyva 95/46/EB

3 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) nuo 2018 m. gegužės 25 d. panaikinta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46 (OL L 119, 2016, p. 1).

4 Direktyvos 95/46 3 straipsnio 2 dalyje buvo nustatyta:

„Ši direktyva netaikoma tvarkant asmens duomenis:

– kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, kaip antai veikla, kuri numatyta Europos Sąjungos sutarties V ir VI dalyse, taip pat kai atliekamos tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu (taip pat ir valstybės ekonomine gerove, kai tvarkymo operacija susijusi su valstybės saugumo klausimais) ir su valstybės veiksmais baudžiamosios teisės srityje;

– kai duomenis tvarko fizinis asmuo, užsiimdamas tik asmenine ar namų ūkio veikla.“

Direktyva 2002/58

5 Direktyvos 2002/58 2, 6, 7 ir 11 konstatuojamosiose dalyse nurodyta:

„(2) Šia direktyva siekiama gerbti pagrindines žmogaus teises ir laikomasi [Chartijos] principų; visų pirma šia direktyva siekiama užtikrinti visapusišką pagarbą [jos] 7 ir 8 straipsniuose išdėstytoms teisėms.

<…>

(6) Internetas keičia tradicines rinkos struktūras sukurdamas bendrą, pasaulinę infrastruktūrą įvairioms elektroninių ryšių paslaugoms teikti. Viešai prieinamos elektroninių ryšių interneto paslaugos atveria naujas galimybes naudotojams, bet dėl jų taip pat iškyla rizika asmens duomenims ir privatumui.

(7) Viešiesiems ryšių tinklams reikėtų nustatyti specifines teisines, normines ir technines nuostatas, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės bei juridinių asmenų teisėti interesai, visų prima dėl didėjančių automatinio duomenų, susijusių su abonentais ir naudotojais, kaupimo ir tvarkymo pajėgumų.

<…>

(11) Ši direktyva, kaip ir Direktyva [95/46], nenagrinėja pagrindinių teisių ir laisvių apsaugos klausimų, susijusių su veiklos rūšimis, kurių nereglamentuoja Bendrijos teisės aktai. Todėl ji nekeičia esamos pusiausvyros tarp fizinio asmens teisės į privatumą ir valstybių narių galimybės imtis šios direktyvos 15 straipsnio 1 dalyje nurodytų priemonių, kurių reikia užtikrinti visuomenės saugumą, gynybą, valstybės saugumą (įskaitant valstybės ekonominę gerovę, kai veiklos rūšys yra susijusios su valstybės saugumo klausimais) ir baudžiamosios teisės vykdymu. Tokiu būdu ši direktyva neturi jokio poveikio valstybių narių galimybėms teisėtu būdu perimti elektroninių ryšių pranešimus arba imtis kitų priemonių, kurių reikia minėtiems tikslams pasiekti laikantis Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos [pasirašytos 1950 m. lapkričio 4 d. Romoje], kaip išaiškinta Europos žmogaus teisių teismo nutarime [kaip ją savo sprendimuose aiškina Europos Žmogaus Teisių Teismas]. Tokios priemonės turi būti tinkamos, griežtai atitinkančios siekiamą tikslą ir būtinos demokratinėje visuomenėje, taip pat joms turi būti taikoma tinkama apsaugos garantija pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją.“

6 Šios direktyvos 1 straipsnyje „Taikymo sritis ir tikslas“ nustatyta:

„1. Šioje direktyvoje numatytas valstybių narių nuostatų, užtikrinančių vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatumą ir konfidencialumą, apsaugą, susijusių [kiek tai susiję] su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančių laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą Bendrijoje, suderinimas.

2. Šios direktyvos nuostatos smulkiau išaiškina ir papildo Direktyvą [95/46] šio straipsnio pirmoje dalyje nurodytais tikslais. Be to, jos numato abonentų, kurie yra juridiniai asmenys, teisėtų interesų apsaugą.

3. Ši direktyva netaikoma veiklos rūšims, kurios neįeina į [SESV] taikymo sritį, tokioms, kurios nurodytos [ES] sutarties V ir VI antraštinėse dalyse, ir visais atvejais veiklos rūšims, susijusioms su visuomenės saugumu, gynyba, valstybės saugumu (įskaitant valstybės ekonominę gerovę, kai atitinkamos veiklos rūšys yra susijusios su valstybės saugumo klausimais) bei valstybės veiksmais baudžiamosios teisės srityje.“

7 Šios direktyvos 2 straipsnyje „Sąvokų apibrėžimai“ nurodyta:

„Jeigu toliau nepateikta [nenurodyta] kitaip, šioje direktyvoje vartojamos sąvokos yra apibrėžiamos taip, kaip apibrėžta Direktyvoje [95/46] ir 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvoje 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva) [(OL L 108, 2002, p. 33; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 349)].

Šioje direktyvoje:

a) „naudotojas“ – tai bet kuris fizinis asmuo, vartojantis viešai prieinamą elektroninių ryšių paslaugą privačiais ar verslo tikslais, ir nebūtinai tai darantis išankstinio paslaugos užsakymo būdu;

b) „srauto duomenys“ – tai duomenys, tvarkomi pranešimui perduoti elektroninių ryšių tinklu, taip pat sąskaitoms už tokį perdavimą pateikti;

c) „vietos nustatymo duomenys“ – elektroninių ryšių tinkluose arba elektroninių ryšių paslaugų teikimo metu tvarkomi duomenys, nurodantys viešosios elektroninių ryšių paslaugos gavėjo galinių įrenginių geografinę padėtį;

d) „pranešimas“ – tai informacija, kuria apsikeičiama arba kuri perduodama tarp baigtinio skaičiaus šalių, naudojantis viešai prieinamomis elektroninių ryšių paslaugomis. Jam nepriskiriama informacija, perduodama kaip dalis viešojo transliavimo paslaugos, naudojant elektroninių ryšių tinklus, išskyrus tuos atvejus, kai tokia informacija gali būti susijusi su informaciją gaunančiu abonentu arba naudotoju, kurio tapatybę galima nustatyti;

<…>“

8 Direktyvos 2002/58 3 straipsnyje „Paslaugos“ numatyta:

„Ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais Bendrijoje, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius.“

9 Šios direktyvos 5 straipsnyje „Pranešimų konfidencialumas“ nustatyta:

„1. Valstybės narės užtikrina pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai teikiamas elektroninių ryšių paslaugas, konfidencialumą, taikydamos nacionalinės teisės aktus. Visų pirma jos draudžia be atitinkamų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus ir su jais susijusius srauto duomenis, išskyrus atvejus, kai tai galima teisėtai daryti pagal 15 straipsnio 1 dalį. Šios dalies nuostatos nedraudžia techninio saugojimo, būtino perduoti pranešimą nepažeidžiant konfidencialumo principo.

<…>

3. Valstybės narės užtikrina, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar naudotojo galiniame įrenginyje būtų leidžiama tik su sąlyga, jei atitinkamam abonentui ar naudotojui sutikus pagal Direktyvą [95/46] pateikiama aiški ir išsami informacija, *inter alia*, apie tokio duomenų tvarkymo tikslus. Ši nuostata nedraudžia vykdyti techninį saugojimą ar naudotis duomenimis, jei siekiama tik atlikti pranešimo perdavimą elektroninių ryšių tinklu, taip pat būtinais atvejais, kad informacinės visuomenės paslaugų teikėjas galėtų teikti paslaugas, kurių aiškiai paprašo abonentas ar naudotojas.“

10 Direktyvos 2002/58 6 straipsnyje „Srauto duomenys“ nustatyta:

„1. Su abonentais ir naudotojais susiję srauto duomenys, kuriuos tvarko ir saugo viešųjų ryšių tinklo ar viešai prieinamų elektroninių ryšių paslaugų teikėjas, turi būti sunaikinti arba pakeisti taip, kad taptų anoniminiais, kai šie duomenys nebėra reikalingi pranešimui perduoti, jeigu nepažeidžiamos šio straipsnio 2, 3 ir 5 dalių ir 15 straipsnio 1 dalies nuostatos.

2. Srauto duomenys gali būti tvarkomi, kai reikia abonentams pateikti sąskaitas ir atsiskaityti už tinklų sujungimą. Toks tvarkymas leistinas tol, kol nepasibaigęs terminas, per kurį sąskaita gali būti teisėtai užginčyta ar išieškotas apmokėjimas.

3. Elektroninių ryšių paslaugų rinkodaros arba pridėtinės vertės paslaugų teikimo tikslais viešųjų elektroninių ryšių paslaugų teikėjas gali tvarkyti 1 dalyje nurodytus duomenis tokia apimtimi ir tiek laiko, kiek būtina tokių paslaugų teikimui ar rinkodarai, jeigu abonentas ar naudotojas, su kuriuo duomenys yra susiję, yra iš anksto davęs sutikimą. Naudotojams ar abonentams sudaroma galimybė bet kuriuo metu atšaukti duotą sutikimą srauto duomenims tvarkyti.

<…>

5. Tvarkyti srauto duomenis pagal šio straipsnio 1, 2, 3 ir 4 dalis leidžiama tik asmenims, kurie veikdami pagal viešųjų ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjų įgaliojimą pateikia sąskaitas, valdo srautą, teikia informaciją klientams, nustato sukčiavimo atvejus, vykdo elektroninių ryšių paslaugų rinkodarą arba teikia pridėtinės vertės paslaugas. Šie asmenys gali atlikti tik tokius veiksmus, kurie yra būtini minėtos veiklos tikslams pasiekti.

<…>“

11 Šios direktyvos 9 straipsnio „Vietos nustatymo duomenys, nesudarantys srauto duomenų“ 1 dalyje numatyta:

„Kai vietos nustatymo duomenys, nesudarantys srauto duomenų, susiję su viešųjų ryšių tinklų ar viešųjų elektroninių ryšių naudotojais ar abonentais, gali būti tvarkomi, 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. Prieš gaudamas sutikimą, paslaugų teikėjas turi informuoti naudotojus ar abonentus apie tai, kokie vietos nustatymo duomenys, nesudarantys srauto duomenų, bus tvarkomi, kokiais tikslais ir kiek laiko, taip pat, ar šie duomenys bus perduoti trečiajai šaliai pridėtinės vertės paslaugai teikti. <…>“

12 Direktyvos 2002/58 15 straipsnio „Kai kurių Direktyvos [95/46] nuostatų taikymas“ 1 dalyje nurodyta:

„Valstybės narės gali patvirtinti teisines [teisėkūros] 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 [proporcinga] demokratinės visuomenės [demokratinėje visuomenėje] priemonė, skirta apsaugoti nacionalin[iam] saugum[ui] (t. y. valstybės saugum[ui]), gynyb[ai], visuomenės saugum[ui], taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą [taip pat užtikrinti baudžiamųjų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas], kaip nurodyta Direktyvos [95/46] 13 straipsnio 1 dalyje. 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 [ESS] 6 straipsnio 1 ir 2 dalyse.“

Vokietijos teisė

TKG

13 Pagrindinės bylos aplinkybėms taikytinos redakcijos 2004 m. birželio 22 d. *Telekommunikationsgesetz* (Telekomunikacijų įstatymas, *BGBl.* 2004 I, p. 1190, toliau – TKG) 113a straipsnio 1 dalies pirmas sakinys suformuluotas taip:

„113b–113g straipsniuose nustatyti įpareigojimai, susiję su srauto duomenų saugojimu, naudojimu ir saugumu, taikomi operatoriams, kurie galutiniams naudotojams teikia viešai prieinamas telekomunikacijų paslaugas.“

14 TKG 113b straipsnyje nustatyta:

„1. 113a straipsnio 1 dalyje nurodyti operatoriai duomenis šalies teritorijoje turi saugoti taip:

1. 2 ir 3 dalyse nurodytus duomenis – 10 savaičių;

2. 4 dalyje nurodytus vietos nustatymo duomenis – 4 savaites.

2) Viešai prieinamų telefonijos paslaugų teikėjai saugo:

1. 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;

2. ryšio pradžios ir pabaigos datą ir laiką, nurodant laiko juostą;

3. paslaugos, kuria naudojamasi, duomenis, jeigu telefonijos paslauga apima įvairių paslaugų galimybes;

4. be to, mobiliosios telefonijos paslaugų atveju:
   a) skambinančių abonentų ir abonentų, kuriems skambinama, tarptautinį identifikatorių;
   b) galinių įrenginių, į kuriuos ir iš kurių skambinta, tarptautinį identifikatorių;

c) paslaugos pirmojo aktyvavimo datą ir laiką, nurodant laiko juostą, jeigu paslaugos buvo apmokėtos iš anksto;

5. internetinės telefonijos paslaugų atveju – taip pat skambinančiojo abonento ir abonento, kuriam buvo skambinta, IP (interneto protokolo) adresus bei priskirtus identifikatorius.

1 dalis *mutatis mutandis* taikoma:

1. SMS, multimedijos ir panašių žinučių perdavimui; šiuo atveju 1 dalies 2 punkte nurodyti duomenys pakeičiami duomenimis apie žinutės išsiuntimo ir gavimo momentą;

2. skambučiams, į kuriuos neatsiliepta arba kurie buvo nutraukti įsikišus tinklo administratoriui <…>

3) Viešai prieinamų interneto prieigos paslaugų teikėjai saugo:

1. IP adresą, abonentui skirtą siekiant naudotis internetu;

2. aiškius ryšio identifikacinius duomenis, suteikiančius prieigą prie interneto, ir paskirtą identifikacinį numerį;

3. naudojimosi internetu pradžios ir pabaigos datą ir laiką pagal paskirtą IP adresą, nurodant laiko juostą.

4) Jei naudojamasi mobiliosios telefonijos paslaugomis, turi būti saugomas skambinančiojo ir asmens, kuriam skambinta, ryšio pradžioje naudotų ryšio prieigos taškų pavadinimas. Mobilaus naudojimosi atveju, teikiant viešai prieinamas interneto prieigos paslaugas, turi būti saugomas interneto ryšio pradžioje naudotų ryšio prieigos taškų pavadinimas. Taip pat turi būti saugomi duomenys, leidžiantys sužinoti atitinkamą ryšio prieigos tašką aptarnaujančių antenų geografinę padėtį ir didžiausios spinduliuotės kryptis.

5) Pagal šią nuostatą negalima saugoti pranešimo turinio, duomenų apie interneto svetaines, kuriose lankytasi, ir elektroninio pašto paslaugų duomenų.

6) Pagal šią nuostatą negalima saugoti duomenų, susijusių su 99 straipsnio 2 dalyje numatytu bendravimu. Tai *mutatis mutandis* taikoma 99 straipsnio 2 dalyje nurodytų subjektų bendravimui telefonu. 99 straipsnio 2 dalies antras–septintas sakiniai taikomi *mutatis mutandis*.

<…>“

15 TKG 99 straipsnio 2 dalyje nurodytas bendravimas, į kurį daroma nuoroda TKG 113b straipsnio 6 dalyje, yra bendravimas su socialinės ar religinės srities asmenimis, valdžios institucijomis ir organizacijomis, kurie siūlo tik arba daugiausia pagalbos telefonu paslaugas skubios psichologinės ar socialinės situacijos atveju skambinantiems, iš principo liekantiems anonimais, ir kuriems patiems arba jų darbuotojams šiuo aspektu yra taikomos specialios konfidencialumo pareigos. TKG 99 straipsnio 2 dalies antrame ir ketvirtame sakiniuose numatyta išimtis taikoma, jeigu subjektai, kuriems skambinama, jų prašymu įtraukiami į Federalinės elektros energijos, dujų, telekomunikacijų, pašto ir geležinkelių tinklų tarnybos sudarytą sąrašą, telefono numerių savininkams nustačius savo misiją pateikiant viešosios teisės reglamentuojamos institucijos, įstaigos, organizacijos ar fondo pažymą.

16 TKG 113c straipsnio 1 ir 2 dalyje numatyta:

„1) Pagal 113b straipsnį saugomi duomenys gali būti:

1. perduodami teisėsaugos institucijai, kai ji paprašo juos perduoti, remdamasi teisės akto nuostata, leidžiančia rinkti 113b straipsnyje nurodytus duomenis siekiant vykdyti baudžiamąjį persekiojimą už labai sunkias nusikalstamas veikas;

2. perduodami federalinių žemių saugumo institucijai, jeigu ji prašo juos perduoti remdamasi teisės akto nuostata, leidžiančia rinkti 113b straipsnyje nurodytus duomenis siekiant užkirsti kelią konkrečiam pavojui asmens sveikatai, gyvybei ar laisvei arba federacinės valstybės ar federalinės žemės egzistavimui;

<…>

2) Subjektai, kuriems taikomi 113a straipsnio 1 dalyje nustatyti įpareigojimai, pagal 113b straipsnį saugomų duomenų negali naudoti kitais tikslais, nei numatyti 1 dalyje.“

17 TKG 113d straipsnyje nurodyta:

„Subjektai, kuriems taikomas 113a straipsnio 1 dalyje numatytas įpareigojimas, turi užtikrinti, kad pagal 113b straipsnio 1 dalį saugomi duomenys, laikantis saugojimo pareigos ir taikant technines bei organizacines priemones, atitinkančias naujausius pasiekimus technikos srityje, būtų apsaugoti nuo neteisėtos kontrolės ir naudojimo. Šios priemonės visų pirma apima:

1. itin saugios šifravimo procedūros naudojimą;

2. saugojimą atskiruose saugojimo infrastruktūros objektuose, atskirtuose nuo infrastruktūros, skirtos įprastoms operacinėms funkcijoms vykdyti;

3. saugojimą atjungtose informacinėse duomenų tvarkymo sistemose, užtikrinant aukšto lygio apsaugą nuo kibernetinių atakų;

4. prieigos prie duomenų tvarkymui naudojamų įrenginių suteikimą tik asmenims, turintiems specialų leidimą, suteiktą už įpareigojimo vykdymą atsakingo subjekto;

5. įpareigojimą užtikrinti, kad naudojantis prieiga prie duomenų dalyvautų bent du asmenys, turintys specialų leidimą, suteiktą už įpareigojimo vykdymą atsakingo subjekto.“

18 TKG 113e straipsnis suformuluotas taip:

„1) Subjektas, atsakingas už 113a straipsnio 1 dalyje numatyto įpareigojimo vykdymą, turi užtikrinti, kad siekiant kontroliuoti duomenų apsaugą būtų registruojama kiekviena prieiga prie duomenų, kurie pagal 113b straipsnio 1 dalį saugomi laikantis saugojimo pareigos, visų pirma jų skaitymo, kopijavimo, keitimo, ištrynimo ir uždarymo veiksmas. Turi būti registruojama:

1. prieigos laikas;

2. asmenys, pasinaudoję prieiga prie duomenų;

3. prieigos tikslas ir pobūdis.

2) Užregistruoti duomenys negali būti naudojami kitais nei duomenų apsaugos kontrolės tikslais.

3) Asmuo, atsakingas už 113a straipsnio 1 dalyje numatytą įpareigojimą, turi užtikrinti, kad užregistruoti duomenys būtų ištrinti praėjus vieniems metams.“

19 Siekiant užtikrinti ypač aukštą duomenų saugumo ir kokybės lygį, Federalinė elektros energijos, dujų, telekomunikacijų, pašto ir geležinkelių tinklų agentūra pagal TKG 113f straipsnio 1 dalį nustato visus reikalavimus, kurie pagal jo 113f straipsnio 2 dalį turi būti nuolat vertinami ir prireikus pritaikomi. Pagal TKG 113g straipsnį reikalaujama, kad specialios saugumo priemonės būtų įtrauktos į saugumo politikos aprašymą, kurį turi pateikti atsakingas subjektas.

StPO

20 *Strafprozessordnung* (Baudžiamojo proceso kodeksas, toliau – *StPO*) 100g straipsnio 2 dalies pirmas sakinys suformuluotas taip:

„Jeigu tam tikros faktinės aplinkybės leidžia įtarti, kad asmuo, kaip vykdytojas ar bendrininkas, padarė vieną iš antrame sakinyje nurodytų labai sunkių nusikalstamų veikų arba pasikėsino ją padaryti tuo atveju, kai yra baudžiama už pasikėsinimą padaryti nusikalstamą veiką, ir jeigu konkrečiu atveju nusikalstama veika taip pat yra labai sunki, srauto duomenys, saugomi pagal [TKG] 113b straipsnį, gali būti renkami, jei ištirti bylos aplinkybes arba nustatyti įtariamojo buvimo vietą kitais būdais būtų pernelyg sunku arba neįmanoma ir duomenų rinkimas yra proporcingas bylos reikšmei.“

21 *StPO* 101a straipsnio 1 dalyje nurodyta, kad rinkti srauto duomenis pagal *StPO* 100g straipsnį galima tik gavus teismo leidimą. Pagal *StPO* 101a straipsnio 2 dalį sprendimo motyvuose turi būti nurodyti esminiai argumentai, susiję su priemonės būtinumu ir tinkamumu konkrečiu atveju. *StPO* 101a straipsnio 6 dalyje numatyta pareiga informuoti atitinkamų telekomunikacijų dalyvius.

Pagrindinės bylos ir prejudicinis klausimas

22 *SpaceNet* ir *Telekom Deutschland* Vokietijoje teikia viešai prieinamas interneto prieigos paslaugas. Be to, antroji Vokietijoje dar teikia viešai prieinamas telefono ryšio paslaugas.

23 Šios paslaugų teikėjos *Verwaltungsgericht Köln* (Kelno administracinis teismas, Vokietija) ginčijo TKG 113a straipsnio 1 dalies ir 113b straipsnio nuostatomis joms nustatytą pareigą nuo 2017 m. liepos 1 d. saugoti jų klientų telekomunikacijų srauto ir vietos nustatymo duomenis.

24 2018 m. balandžio 20 d. sprendimais *Verwaltungsgericht Köln* (Kelno administracinis teismas) nusprendė, kad *SpaceNet* ir *Telekom Deutschland* neprivalo saugoti klientų, kuriems jos suteikia prieigą prie interneto, telekomunikacijų srauto duomenų, nurodytų TKG 113b straipsnio 3 dalyje, ir, be to, *Telekom Deutschland* neprivalo saugoti klientų, kuriems ji teikia prieigą prie viešai prieinamų telefonijos paslaugų, telekomunikacijų srauto duomenų, nurodytų TKG 113b straipsnio 2 dalies pirmame ir antrame sakiniuose. Atsižvelgęs į 2016 m. gruodžio 21 d. Sprendimą *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970) minėtas teismas nusprendė, kad tokia saugojimo pareiga prieštarauja Sąjungos teisei.

25 Vokietijos Federacinė Respublika dėl šių sprendimų pateikė kasacinius skundus *Bundesverwaltungsgericht* (Federalinis administracinis teismas, Vokietija), prašymą priimti prejudicinį sprendimą pateikusiam teismui.

26 Prašymą priimti prejudicinį sprendimą pateikęs teismas mano, kad klausimas, ar TKG 113a straipsnio 1 dalies ir 113b straipsnio nuostatomis nustatyta saugojimo pareiga prieštarauja Sąjungos teisei, priklauso nuo Direktyvos 2002/58 aiškinimo.

27 Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, jog Teisingumo Teismas 2016 m. gruodžio 21 d. Sprendime *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970) jau galutinai nusprendė, kad teisės aktai dėl srauto ir vietos nustatymo duomenų saugojimo ir nacionalinių valdžios institucijų prieigos prie šių duomenų iš esmės patenka į Direktyvos 2002/58 taikymo sritį.

28 Jis taip pat nurodo, kad pagrindinėje byloje nagrinėjama saugojimo pareiga, kiek ja ribojamos iš Direktyvos 2002/58 5 straipsnio 1 dalies, 6 straipsnio 1 dalies ir 9 straipsnio 1 dalies kylančios teisės, gali būti pateisinama tik remiantis šios direktyvos 15 straipsnio 1 dalimi.

29 Šiuo klausimu jis primena, kad, remiantis 2016 m. gruodžio 21 d. Sprendimu *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970), Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, kuriais numatyta siekiant kovoti su nusikalstamumu bendrai ir nediferencijuotai saugoti visų abonentų ir registruotų vartotojų visus srauto ir vietos nustatymo duomenis, susijusius su visomis elektroninio ryšio priemonėmis.

30 Vis dėlto, prašymą priimti prejudicinį sprendimą pateikusio teismo nuomone, kaip ir bylose, kuriose priimtas minėtas sprendimas, nagrinėtose teisės normose, pagal pagrindinėje byloje nagrinėjamas teisės normas nereikalaujama jokio pagrindo saugoti duomenis ar kokio nors ryšio tarp saugomų duomenų ir nusikalstamos veikos ar pavojaus visuomenės saugumui. Iš tiesų pagal šias nacionalinės teisės normas reikalaujama be priežasties, bendrai ir nediferencijuojant individualiai, laiko ir geografiniu požiūriais saugoti didžiąją dalį reikšmingų telekomunikacijų srauto duomenų.

31 Vis dėlto prašymą priimti prejudicinį sprendimą pateikęs teismas mano, kad neatmestina galimybė, jog pagrindinėje byloje nagrinėjama saugojimo pareiga gali būti pateisinama pagal Direktyvos 2002/58 15 straipsnio 1 dalį.

32 Pirma, jis pažymi, kad, priešingai nei pagal bylose, kuriose priimtas 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970), nagrinėtas nacionalinės teisės normas, pagal pagrindinėje byloje nagrinėjamas nacionalinės teisės normas nereikalaujama saugoti visų abonentų ir registruotų vartotojų visų telekomunikacijų srauto duomenų, susijusių su visomis elektroninio ryšio priemonėmis. Kaip matyti iš TKG 113b straipsnio 5 ir 6 dalių, saugojimo pareiga netaikoma ne tik pranešimų turiniui, bet negali būti saugomi ir duomenys, susiję su lankytomis interneto svetainėmis, elektroninio pašto paslaugų duomenys ir duomenys, kuriais grindžiami socialinio ar religinio pobūdžio pranešimai į kai kurias linijas arba iš jų.

33 Antra, tas teismas nurodo, kad TKG 113b straipsnio 1 dalyje numatyta keturių savaičių vietos nustatymo duomenų ir dešimties savaičių srauto duomenų saugojimo trukmė, o 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvoje 2006/24/EB dėl duomenų, generuojamų arba

tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančioje Direktyvą 2002/58/EB (OL L 105, 2006, p. 54), kuria buvo grįsti nacionalinės teisės aktai, nagrinėti bylose, kuriose priimtas 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970), numatyta saugojimo trukmė apėmė saugojimą nuo šešių mėnesių iki dvejų metų.

34 Prašymą priimti prejudicinį sprendimą pateikusio teismo teigimu, jei tam tikrų ryšio priemonių ar duomenų kategorijų neįtraukimo ir saugojimo trukmės apribojimo nepakanka pašalinti bet kokią riziką, kad bus sudarytas išsamus atitinkamų asmenų profilis, ši rizika yra bent jau gerokai mažesnė įgyvendinant pagrindinėje byloje nagrinėjamus nacionalinės teisės aktus.

35 Trečia, šie teisės aktai apima griežtus saugomų duomenų apsaugos ir prieigos prie jų apribojimus. Taigi, viena vertus, jie užtikrina veiksmingą saugomų duomenų apsaugą nuo piktnaudžiavimo rizikos ir nuo bet kokios neteisėtos prieigos prie tokių duomenų. Kita vertus, saugomi duomenys gali būti naudojami tik kovojant su sunkiais nusikaltimais arba siekiant išvengti konkretaus pavojaus asmens sveikatai, gyvybei ar laisvei arba federacinės valstybės ar federalinės žemės egzistavimui.

36 Ketvirta, Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimas, kad bet koks duomenų saugojimas be priežasties apskritai neatitinka Sąjungos teisės, galėtų prieštarauti valstybių narių pareigai veikti, kylančiai iš Chartijos 6 straipsnyje įtvirtintos teisės į saugumą.

37 Penkta, prašymą priimti prejudicinį sprendimą pateikęs teismas mano, kad Direktyvos 2002/58 15 straipsnio aiškinimas, pagal kurį draudžiama bendrai saugoti duomenis, labai apribotų nacionalinio įstatymų leidėjo veiksmų laisvę baudimo už nusikaltimus ir visuomenės saugumo srityje, už kurią pagal ESS 4 straipsnio 2 dalį ir toliau būtų atsakinga tik kiekviena valstybė narė.

38 Šešta, prašymą priimti prejudicinį sprendimą pateikęs teismas mano, jog reikia atsižvelgti į Europos Žmogaus Teisių Teismo jurisprudenciją, ir pažymi, kad jis nusprendė, jog Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – EŽTK) 8 straipsnis neprieštarauja nacionalinės teisės nuostatoms, kuriomis numatytas masinis tarpvalstybinių duomenų srautų perėmimas, atsižvelgiant į grėsmes, su kuriomis šiuo metu susiduria daug valstybių, ir į technologines priemones, kuriomis dabar gali naudotis teroristai ir nusikaltėliai, vykdydami neteisėtus veiksmus.

39 Tokiomis aplinkybėmis *Bundesverwaltungsgericht* (Federalinis administracinis teismas) nutarė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šį prejudicinį klausimą:

„Ar, atsižvelgiant, pirma, į [Chartijos] 7, 8 ir 11 straipsnius bei 52 straipsnio 1 dalį ir, antra, į [šios Chartijos] 6 straipsnį ir [ESS] 4 straipsnį, Direktyvos [2002/58] 15 straipsnį reikia aiškinti taip, kad pagal jį draudžiama nacionalinės teisės norma, pagal kurią viešai prieinamų elektroninių ryšių paslaugų teikėjai įpareigojami saugoti tų paslaugų galutinių naudotojų srauto ir vietos nustatymo duomenis, jeigu:

1) šiam įpareigojimui netaikoma jokia konkreti vietos, laiko ar teritorijos sąlyga;

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

a) 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;
b) ryšio pradžios ir pabaigos datą ir laiką arba – trumposios, multimedijos ir pan. žinutės perdavimo atveju – žinutės išsiuntimo ir gavimo momentą, nurodant laiko juostą;
c) paslaugos, kuria naudojamasi, duomenis, jeigu telefonijos paslauga apima įvairių paslaugų galimybes;
d) be to, mobiliosios telefonijos paslaugų atveju:
   i) skambinančių abonentų ir abonentų, kuriems skambinama, tarptautinį identifikatorių;
   ii) galinio įrenginio, į kurį ir iš kurio skambinta, tarptautinį identifikatorių;
   iii) paslaugos pirmojo aktyvavimo datą ir laiką, nurodant laiko juostą, jeigu paslaugos buvo apmokėtos iš anksto;
   iv) ryšio prieigos taškų, kuriais skambinantysis abonentas ir abonentas, kuriam buvo skambinta, naudojosi ryšio pradžioje, pavadinimus;
e) internetinės telefonijos paslaugų atveju – ir skambinančiojo abonento bei abonento, kuriam buvo skambinta, IP (interneto protokolo) adresus ir priskirtus naudotojo identifikatorius;

3) pareiga saugoti duomenis teikiant viešai prieinamas interneto prieigos paslaugas apima šiuos duomenis:
   a) abonentui naudojimosi internetu tikslais priskirtą interneto protokolo adresą;
   b) unikalų interneto prieigos taško identifikatorių bei priskirtą naudotojo identifikatorių,
   c) interneto naudojimo per priskirtą interneto protokolo adresą pradžios ir pabaigos datą ir laiką, nurodant laiko juostą;
   d) mobilaus naudojimosi atveju – ryšio prieigos taško, kuriuo buvo naudojamasi interneto ryšio pradžioje, pavadinimą;

4) draudžiama saugoti šiuos duomenis:
   a) pranešimo turinį;
   b) duomenis apie aplankytas interneto svetaines;
   c) elektroninio pašto paslaugų duomenis;
   d) socialinei ar religinei sričiai priklausančių asmenų, institucijų ir organizacijų, su kuriomis susisiekiama arba kurie susisiekia, ryšių duomenis;

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

6) užtikrinama veiksminga saugomų duomenų apsauga nuo piktnaudžiavimo rizikos ir nuo neteisėtos prieigos; ir

7) saugomus duomenis leidžiama naudoti tik siekiant vykdyti persekiojimą už sunkias nusikalstamas veikas ir užkirsti kelią konkrečiam pavojui, kylančiam asmens sveikatai, gyvybei ar laisvei arba valstybės ar federalinės žemės saugumui, 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, taip pat vykdant žvalgybos uždavinius?“

Procesas Teisingumo Teisme

40 2019 m. gruodžio 3 d. Teisingumo Teismo pirmininko sprendimu bylos C-793/19 ir C-794/19 buvo sujungtos, kad būtų bendrai vykdoma rašytinė ir žodinė proceso dalys ir priimtas sprendimas.

41 2020 m. liepos 14 d. Teisingumo Teismo pirmininko sprendimu procesas sujungtose bylose C-793/19 ir C-794/19 buvo sustabdytas pagal Teisingumo Teismo procedūros reglamento 55 straipsnio 1 dalies b punktą, kol bus priimtas sprendimas byloje *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18).

42 2020 m. spalio 6 d. Teisingumo Teismui priėmus sprendimą byloje *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791), Teisingumo Teismo pirmininkas 2020 m. spalio 8 d. nurodė atnaujinti procesą sujungtose bylose C-793/19 ir C-794/19.

43 Prašymą priimti prejudicinį sprendimą pateikęs teismas, kuriam kanceliarija pranešė apie šį sprendimą, nurodė, kad neatsiima prašymo priimti prejudicinį sprendimą.

44 Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas visų pirma pažymėjo, kad pagrindinėje byloje nagrinėjamuose teisės aktuose numatyta saugojimo pareiga susijusi su mažesniu duomenų kiekiu ir trumpesne saugojimo trukme, nei numatyta nacionalinės teisės aktuose, nagrinėtuose bylose, kuriose priimtas 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). Šie ypatumai sumažina galimybę, kad iš saugomų duomenų būtų galima padaryti labai tikslias išvadas dėl asmenų, kurių duomenys buvo saugomi, privataus gyvenimo.

45 Be to, jis dar kartą nurodė, kad pagrindinėje byloje nagrinėjamais nacionalinės teisės aktais užtikrinama veiksminga saugomų duomenų apsauga nuo piktnaudžiavimo ir neteisėtos prieigos rizikos.

46 Galiausiai jis pabrėžė, kad išlieka abejonių dėl pagrindinėje byloje nagrinėjamuose nacionalinės teisės aktuose numatyto IP adresų saugojimo suderinamumo su Sąjungos teise dėl 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791) 155 ir 168 punktų nenuoseklumo. Taigi, prašymą priimti prejudicinį sprendimą pateikusio teismo nuomone, iš šio sprendimo neaišku, ar siekiant saugoti IP adresus Teisingumo Teismas reikalauja saugojimo motyvo, susijusio su tikslu užtikrinti nacionalinį saugumą, kovoti su sunkiais nusikaltimais arba užkirsti kelią didelėms grėsmėms visuomenės saugumui, kaip matyti iš minėto sprendimo 168 punkto, ar IP adresų saugojimas yra leidžiamas net nesant konkretaus motyvo, nes šiais tikslais ribojamas tik saugomų duomenų naudojimas, kaip matyti iš to paties sprendimo 155 punkto.

Dėl prejudicinio klausimo

47 Prejudiciniu klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 6–8 ir 11 straipsniais, taip pat 52 straipsnio 1 dalimi ir ESS 4 straipsnio 2 dalimi, turi būti aiškinama taip, kad pagal ją draudžiama nacionalinės teisės nuostata, pagal kurią, išskyrus tam tikras išimtis, viešai prieinamų elektroninių ryšių paslaugų teikėjams nustatoma pareiga šios direktyvos 15 straipsnio 1 dalyje nurodytais tikslais, visų pirma siekiant užtikrinti baudžiamąjį

persekiojimą už sunkias nusikalstamas veikas arba užkirsti kelią konkrečiam pavojui nacionaliniam saugumui, bendrai ir nediferencijuotai saugoti didžiąją dalį šių paslaugų galutinių vartotojų srauto ir vietos nustatymo duomenų, numatant kelių savaičių saugojimo laikotarpį, taip pat taisykles, kuriomis siekiama užtikrinti veiksmingą saugomų duomenų apsaugą nuo piktnaudžiavimo rizikos ir nuo bet kokios neteisėtos prieigos prie šių duomenų.

Dėl Direktyvos 2002/58 taikymo

48 Dėl Airijos, taip pat Prancūzijos, Nyderlandų, Lenkijos ir Švedijos vyriausybių argumentų, kad pagrindinėje byloje nagrinėjami nacionalinės teisės aktai, kiek jie buvo priimti siekiant užtikrinti nacionalinį saugumą, nepatenka į Direktyvos 2002/58 taikymo sritį, pakanka priminti, kad tokie nacionalinės teisės aktai, kaip nagrinėjami pagrindinėje byloje, pagal kuriuos elektroninių ryšių paslaugų teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis, siekdami apsaugoti nacionalinį saugumą ir kovoti su nusikalstamumu, patenka į Direktyvos 2002/58 taikymo sritį (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 104 punktas).

Dėl Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo

Teisingumo Teismo jurisprudencijoje nustatytų principų priminimas

49 Pagal suformuotą jurisprudenciją aiškinant Sąjungos teisės nuostatą reikia remtis ne tik jos tekstu, bet ir jos kontekstu bei teisės akto, kuriame ji įtvirtinta, tikslais, taip pat, be kita ko, atsižvelgti į šių teisės aktų genezę (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 32 punktas ir jame nurodyta jurisprudencija).

50 Iš pačios Direktyvos 2002/58 15 straipsnio 1 dalies formuluotės matyti, kad šioje direktyvoje numatytomis teisėkūros priemonėmis, kurias valstybėms narėms leidžiama priimti tos direktyvos numatytomis sąlygomis, tik siekiama „riboti“ teisių ir pareigų, numatytų Direktyvos 2002/58 5, 6 ir 9 straipsniuose, „taikymą“ (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 33 punktas).

51 Kalbant apie šioje direktyvoje nustatytą sistemą, kurios dalis yra 15 straipsnio 1 dalis, reikia priminti, kad pagal šios direktyvos 5 straipsnio 1 dalies pirmą ir antrą sakinius valstybės narės užtikrina pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai prieinamas elektroninių ryšių paslaugas, konfidencialumą, taikydamos nacionalinės teisės aktus. Visų pirma jos draudžia asmenims, kurie nėra naudotojai, be atitinkamų naudotojų sutikimo klausyti, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus ir su jais susijusius srauto duomenis, išskyrus atvejus, kai naudotojas leido tai teisėtai daryti pagal tos pačios direktyvos 15 straipsnio 1 dalį (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 34 punktas).

52 Šiuo klausimu Teisingumo Teismas jau yra nusprendęs, kad
Direktyvos 2002/58 5 straipsnio 1 dalyje įtvirtintas elektroninių pranešimų ir su jais susijusių srauto duomenų konfidencialumo principas, be kita ko, reiškia, kad iš esmės bet kuriam asmeniui, išskyrus naudotoją, draudžiama saugoti šiuos pranešimus ir duomenis be jo sutikimo

(2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 107 punktas; taip pat 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 35 punktas).

53 Ši nuostata atspindi tikslą, kurio Sąjungos teisės aktų leidėjas siekė priimdamas Direktyvą 2002/58. Iš Europos Parlamento ir Tarybos direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje pasiūlymo [COM(2000) 385 *final*], kuriuo remiantis parengta Direktyva 2002/58, aiškinamojo memorandumo matyti, jog Sąjungos teisės aktų leidėjas siekė „užtikrinti, kad ir toliau būtų laikomasi asmens duomenų ir privataus gyvenimo aukšto lygio apsaugos visų elektroninių ryšių paslaugų atveju, nepaisant naudojamos technologijos“. Taigi minėta direktyva, kaip matyti, be kita ko, iš jos 6 ir 7 konstatuojamųjų dalių, siekiama apsaugoti elektroninių ryšių paslaugų naudotojus nuo pavojaus, kuris asmens duomenims ir privačiam gyvenimui kyla dėl naujų technologijų ir ypač dėl didėjančių automatizuoto duomenų kaupimo ir tvarkymo pajėgumų. Konkrečiai kalbant, kaip nurodyta tos pačios direktyvos 2 konstatuojamojoje dalyje, Sąjungos teisės aktų leidėjas siekia užtikrinti visapusišką Chartijos 7 ir 8 straipsniuose nurodytų teisių, susijusių atitinkamai su privatumo ir asmens duomenų apsauga, paisymą (šiuo klausimu žr. 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 36 punktą ir jame nurodytą jurisprudenciją).

54 Priimdamas Direktyvą 2002/58 Sąjungos teisės aktų leidėjas sukonkretino šias teises taip, kad elektroninių ryšių priemonių naudotojai iš esmės turi teisę tikėtis, kad be jų sutikimo jų pranešimai ir su jais susiję duomenys išliks anonimiški ir negalės būti įrašomi (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 109 punktas; taip pat 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 37 punktas).

55 Dėl elektroninių ryšių paslaugų teikėjų atliekamo su abonentais ir naudotojais susijusių srauto duomenų tvarkymo ir saugojimo Direktyvos 2002/58 6 straipsnio 1 dalyje numatyta, kad šie duomenys turi būti sunaikinti arba pakeisti taip, kad taptų anoniminiai, jeigu jie nebėra reikalingi pranešimui perduoti, o 2 dalyje patikslinta, kad srauto duomenys, kurių reikia abonentams pateikti sąskaitas ir atsiskaityti už tinklų sujungimą, gali būti tvarkomi tik tol, kol nepasibaigęs terminas, per kurį sąskaita gali būti teisėtai užginčyta ar išieškotas apmokėjimas. Dėl kitų nei srauto duomenys vietos nustatymo duomenų šios direktyvos 9 straipsnio 1 dalyje nurodyta, kad šie duomenys gali būti tvarkomi tik esant tam tikroms sąlygoms ir padarius juos anoniminius arba gavus naudotojų ar abonentų sutikimą.

56 Taigi Direktyvoje 2002/58 ne tik reglamentuojama prieiga prie tokių duomenų numatant priemones, kuriomis siekiama užkirsti kelią piktnaudžiavimui, bet visų pirma įtvirtintas draudimo tretiesiems asmenims juos saugoti principas (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 39 punktas).

57 Kadangi pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybėms narėms leidžiama priimti teisėkūros priemones, kuriomis „ribojamas“ šios direktyvos 5, 6 ir 9 straipsniuose numatytų teisių ir pareigų, kaip antai kylančių iš pranešimų konfidencialumo ir draudimo saugoti su jais susijusius duomenis principų, primintų šio sprendimo 52 punkte, taikymas, šioje nuostatoje įtvirtinta būtent tuose 5, 6 ir 9 straipsniuose numatytos bendros taisyklės išimtis, todėl, remiantis suformuota jurisprudencija, ji turi būti aiškinama siaurai. Tokia nuostata negali pateisinti to, kad nukrypimas nuo pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą ir ypač šios direktyvos 5 straipsnyje numatyto draudimo saugoti šiuos duomenis

taptų taisykle, nes taip būtų labai susiaurinta 5 straipsnio apimtis (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 40 punktas ir jame nurodyta jurisprudencija).

58 Dėl tikslų, galinčių pateisinti teisių ir pareigų, numatytų būtent Direktyvos 2002/58 5, 6 ir 9 straipsniuose, apribojimą, Teisingumo Teismas jau yra nusprendęs, kad šios direktyvos 15 straipsnio 1 dalies pirmame sakinyje pateiktas tikslų sąrašas yra baigtinis, todėl pagal šią nuostatą priimta teisėkūros priemonė turi iš tikrųjų griežtai atitikti vieną iš šių tikslų (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 41 punktas ir jame nurodyta jurisprudencija).

59 Be to, iš Direktyvos 2002/58 15 straipsnio 1 dalies trečio sakinio matyti, kad priemonės, kurių valstybės narės imasi pagal šią nuostatą, turi atitikti bendruosius Sąjungos teisės principus, įskaitant proporcingumo principą, ir užtikrinti Chartijoje garantuojamų pagrindinių teisių paisymą. Šiuo klausimu Teisingumo Teismas jau yra nusprendęs, kad dėl valstybės narės nacionalinės teisės aktuose nustatytos pareigos elektroninių ryšių paslaugų teikėjams saugoti srauto duomenis, kad prireikus jie būtų prieinami kompetentingoms nacionalinėms institucijoms, kyla klausimų ne tik dėl Chartijos 7 ir 8 straipsnių, bet ir Chartijos 11 straipsnio, susijusio su saviraiškos laisve, laikymosi, nes ši laisvė yra vienas iš esminių demokratinės ir pliuralistinės visuomenės pagrindų ir vertybių, kuriomis pagal ESS 2 straipsnį grindžiama Europos Sąjunga, dalis (šiuo klausimu žr. 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 42 ir 43 punktus ir juose nurodytą jurisprudenciją).

60 Šiuo klausimu reikia patikslinti, kad srauto ir vietos nustatymo duomenų saugojimas savaime yra, pirma, Direktyvos 2002/58 5 straipsnio 1 dalyje numatyto draudimo saugoti šiuos duomenis, taikomo bet kuriam asmeniui, kuris nėra naudotojas, išimtis ir, antra, Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių į privataus gyvenimo gerbimą ir asmens duomenų apsaugą suvaržymas, neatsižvelgiant į tai, ar atitinkama informacija, susijusi su privačiu gyvenimu, yra jautri, ar ne, ar suinteresuotieji asmenys patyrė nepatogumų dėl tokio suvaržymo, taip pat nepaisant to, ar saugomi duomenys vėliau naudojami, ar ne (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 44 punktas ir jame nurodyta jurisprudencija).

61 Ši išvada juo labiau pagrįsta dėl to, kad srauto ir vietos nustatymo duomenys gali atskleisti daug svarbių aspektų apie atitinkamų asmenų privatų gyvenimą, įskaitant jautrią informaciją, pavyzdžiui, seksualinę orientaciją, politines pažiūras, religinius, filosofinius, visuomeninius ar kitus įsitikinimus ir sveikatos būklę, nors tokiems duomenims, be to, Sąjungos teisėje taikoma ypatinga apsauga. Iš šių duomenų, vertinamų kaip visuma, gali būti daromos labai tikslios išvados apie asmenų, kurių duomenys saugomi, privatų gyvenimą, kaip antai kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ar kitokį judėjimą, vykdomą veiklą, šių asmenų socialinius ryšius ir jų lankomą socialinę aplinką. Visų pirma šie duomenys sudaro sąlygas atitinkamų asmenų profiliui nustatyti, o tai irgi yra tokia pati jautri informacija, kiek tai susiję su teise į privataus gyvenimo gerbimą, kaip ir pats pranešimų turinys (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 45 punktas ir jame nurodyta jurisprudencija).

62 Taigi, pirma, srauto ir vietos nustatymo duomenų saugojimu teisėsaugos tikslais gali būti pažeista Chartijos 7 straipsnyje įtvirtinta teisė į komunikacijos slaptumą, ir tai gali turėti atgrasomąjį poveikį elektroninių ryšių priemonių naudotojams įgyvendinti jos 11 straipsnyje garantuojamą jų saviraiškos laisvę; šis poveikis yra juo didesnis, juo didesnė saugomų duomenų apimtis ir įvairovė.

Antra, atsižvelgiant į didelį srauto ir vietos nustatymo duomenų, kurie gali būti nuolat saugomi taikant bendro ir nediferencijuoto saugojimo priemonę, kiekį ir į informacijos, kurią šie duomenys gali suteikti, jautrumą, vien elektroninių ryšių paslaugų teikėjų atliekamas šių duomenų saugojimas kelia piktnaudžiavimo ir neteisėtos prieigos pavojų (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 46 punktas ir jame nurodyta jurisprudencija).

63 Taigi tiek, kiek valstybėms narėms leidžiama apriboti šio sprendimo 51–54 punktuose nurodytas teises ir pareigas, Direktyvos 2002/58 15 straipsnio 1 dalis atspindi tai, kad Chartijos 7, 8 ir 11 straipsniuose įtvirtintos teisės nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų visuomeninę paskirtį. Iš tiesų, kaip matyti iš Chartijos 52 straipsnio 1 dalies, ja leidžiama apriboti naudojimąsi tokiomis teisėmis, jei šie apribojimai numatyti įstatymo, nekeičia minėtų teisių esmės ir, remiantis proporcingumo principu, yra būtini ir tikrai atitinka Sąjungos pripažintus bendrojo intereso tikslus arba reikalingi kitų teisėms ir laisvėms apsaugoti. Taigi, aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį atsižvelgiant į Chartiją, taip pat reikia atsižvelgti į Chartijos 3, 4, 6 ir 7 straipsniuose įtvirtintų teisių ir nacionalinio saugumo apsaugos bei kovos su sunkiais nusikaltimais tikslų svarbą, prisidedant prie kitų asmenų teisių ir laisvių apsaugos (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 48 punktas ir jame nurodyta jurisprudencija).

64 Kiek tai konkrečiai susiję su kova su nusikalstamomis veikomis, kurių aukos yra visų pirma nepilnamečiai ir kiti pažeidžiami asmenys, reikia atsižvelgti į tai, kad pareigos veikti, tenkančios viešosios valdžios institucijoms, gali kilti iš Chartijos 7 straipsnio, siekiant priimti teisines priemones, kuriomis norima apsaugoti privatų ir šeimos gyvenimą. Tokios pareigos taip pat gali išplaukti iš minėto 7 straipsnio, kiek tai susiję su būsto neliečiamybe ir komunikacijos slaptumu, ir iš 3 ir 4 straipsnių, susijusių su asmenų fizinės ir psichinės sveikatos apsauga bei kankinimo, nežmoniško ir žeminamo elgesio draudimu (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 49 punktas ir jame nurodyta jurisprudencija).

65 Taigi, atsižvelgiant į šias įvairias pareigas veikti, reikia suderinti įvairius nagrinėjamus teisėtus interesus ir teises ir sukurti teisinę sistemą, leidžiančią tai suderinti (šiuo klausimu žr. 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 50 punktą ir jame nurodytą jurisprudenciją).

66 Tokiomis aplinkybėmis iš pačios Direktyvos 2002/58 15 straipsnio 1 dalies pirmo sakinio formuluotės matyti, kad valstybės narės gali priimti nuo šio sprendimo 52 punkte nurodyto konfidencialumo principo nukrypstančią priemonę, kai ji yra „būtina, tinkama ir adekvati [proporcinga] demokratinės visuomenės [demokratinėje visuomenėje]“; šios direktyvos 11 konstatuojamojoje dalyje patikslinta, kad tokio pobūdžio priemonė turi „griežtai“ atitikti siekiamą tikslą.

67 Šiuo klausimu reikia priminti, kad, remiantis suformuota Teisingumo Teismo jurisprudencija, dėl pagrindinės teisės į privataus gyvenimo gerbimą apsaugą reikalaujama, kad nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neviršytų to, kas yra griežtai būtina. Be to, bendrojo intereso tikslo negalima siekti neatsižvelgiant į tai, kad jis turi būti derinamas su pagrindinėmis teisėmis, kurioms taikoma priemonė, nustatant pusiausvyrą tarp, viena vertus, bendrojo intereso tikslo ir, kita vertus, nagrinėjamų teisių (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 52 punktas ir jame nurodyta jurisprudencija).

68 Konkrečiau kalbant, iš Teisingumo Teismo jurisprudencijos matyti, kad valstybių narių galimybė pateisinti teisių ir pareigų, numatytų būtent Direktyvos 2002/58 5, 6 ir 9 straipsniuose, apribojimą turi būti vertinama atsižvelgiant į suvaržymo, kurį lemia toks apribojimas, dydį ir tikrinant, ar šiuo apribojimu siekiamo bendrojo intereso tikslo svarba jį atitinka (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 53 punktas ir jame nurodyta jurisprudencija).

69 Tam, kad atitiktų proporcingumo reikalavimą, nacionalinės teisės aktuose turi būti numatytos aiškios ir tikslios taisyklės, reglamentuojančios nagrinėjamos priemonės apimtį ir taikymą bei nustatančios minimalius reikalavimus, kad asmenys, kurių asmens duomenys tvarkomi, turėtų pakankamai garantijų, leidžiančių veiksmingai apsaugoti šiuos duomenis nuo piktnaudžiavimo pavojų. Tokie teisės aktai turi būti teisiškai privalomi pagal nacionalinę teisę ir juose turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis gali būti imtasi tokių duomenų tvarkymą numatančios priemonės, taip užtikrinant, kad teisių suvaržymas neviršytų to, kas griežtai būtina. Būtinybė turėti tokias garantijas yra dar svarbesnė tais atvejais, kai asmens duomenys tvarkomi automatizuotai, visų pirma kai egzistuoja didelis neteisėtos prieigos prie šių duomenų pavojus. Šios išvados ypač taikytinos tais atvejais, kai susiduriama su šios ypatingos asmens duomenų kategorijos, kurią sudaro jautrūs duomenys, apsauga (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 54 punktas ir jame nurodyta jurisprudencija).

70 Taigi nacionalinės teisės aktai, kuriuose numatytas asmens duomenų saugojimas, visada turi atitikti objektyvius kriterijus, nustatančius saugotinų duomenų ir siekiamo tikslo ryšį (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 55 punktas ir jame nurodyta jurisprudencija).

71 Dėl bendrojo intereso tikslų, galinčių pateisinti priemonę, kurios imtasi pagal Direktyvos 2002/58 15 straipsnio 1 dalį, iš Teisingumo Teismo jurisprudencijos, visų pirma 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791), matyti, kad, remiantis proporcingumo principu, egzistuoja šių tikslų hierarchija, atsižvelgiant į jų atitinkamą svarbą, ir kad tokia priemone siekiamo tikslo svarba turi būti siejama su jos sukelto suvaržymo dydžiu (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 56 punktas).

72 Taigi, kalbant apie nacionalinio saugumo užtikrinimą, kurio svarba viršija kitų Direktyvos 2002/58 15 straipsnio 1 dalyje nurodytų tikslų svarbą, Teisingumo Teismas konstatavo, kad pagal šią nuostatą, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, nedraudžiamos teisėkūros priemonės, kuriomis, siekiant užtikrinti nacionalinį saugumą, leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis tais atvejais, kai atitinkama valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra, esama arba numatoma, o sprendimui, kuriame numatytas toks įpareigojimas, gali būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi sąlygų ir garantijų, kurios turi būti numatytos; toks įpareigojimas gali būti nustatytas tik tam tikru laikotarpiu, neviršijančiu to, kas griežtai būtina, bet kurį galima pratęsti, jeigu ši grėsmė išlieka (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 58 punktas ir jame nurodyta jurisprudencija).

73 Kiek tai susiję su nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo už jas tikslu, Teisingumo Teismas pažymėjo, kad pagal proporcingumo principą tik kova su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencija gali pateisinti didelius Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymus, kaip antai susijusius su srauto ir vietos nustatymo duomenų saugojimu. Taigi tik nedideli minėtų pagrindinių teisių suvaržymai gali būti pateisinami tikslu užtikrinti nusikalstamų veikų prevenciją, tyrimą, nustatymą ir baudžiamąjį persekiojimą už jas apskritai (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 59 punktas ir jame nurodyta jurisprudencija).

74 Dėl kovos su sunkiais nusikaltimais tikslo Teisingumo Teismas yra nusprendęs, kad nacionalinės teisės aktai, numatantys bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, viršija tai, kas griežtai būtina, ir negali būti laikomi pateisinamais demokratinėje visuomenėje. Atsižvelgiant į informacijos, kurią gali suteikti srauto ir vietos nustatymo duomenys, jautrumą, šios informacijos konfidencialumas yra esminis, užtikrinant teisę į privataus gyvenimo gerbimą. Taigi, atsižvelgiant, pirma, į atgrasomąjį poveikį Chartijos 7 ir 11 straipsniuose įtvirtintoms pagrindinėms teisėms, nurodytoms šio sprendimo 62 punkte, įgyvendinti, kurį gali sukelti šių duomenų saugojimas, ir, antra, į suvaržymo, kurį lemia toks saugojimas, dydį, svarbu, kad demokratinėje visuomenėje, kaip numatyta Direktyvoje 2002/58 nustatytoje sistemoje, šis saugojimas būtų išimtis, o ne taisyklė, ir kad šie duomenys nebūtų sistemingai ir nuolat saugomi. Ši išvada darytina net ir dėl kovos su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencijos tikslų bei dėl jiems teiktinos svarbos (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 65 punktas ir jame nurodyta jurisprudencija).

75 Vis dėlto Teisingumo Teismas nurodė, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais, taip pat 52 straipsnio 1 dalimi, neprieštarauja teisėkūros priemonėms, 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 atitinkamų asmenų kategorijas arba geografinius kriterijus laikotarpiu, neviršijančiu to, kas griežtai būtina, tačiau kurį galima pratęsti,

– bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas laikotarpiu, neviršijančiu to, kas griežtai būtina,

– bendras ir nediferencijuotas duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas ir

– leidžiama kompetentingos institucijos sprendimu, kuriam taikoma veiksminga teisminė kontrolė, įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų, kuriuos turi šie paslaugų teikėjai, saugojimą (anglų k. *quick freeze*),

jeigu šios priemonės aiškiomis ir tiksliomis taisyklėmis užtikrina, kad nagrinėjamų duomenų saugojimas priklauso nuo materialinių ir procedūrinių su tuo susijusių sąlygų laikymosi ir atitinkami asmenys turi veiksmingas garantijas nuo piktnaudžiavimo rizikos (2020 m. spalio 6 d.

Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 168 punktas; taip pat 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 67 punktas).

Dėl priemonės, kuria kelių savaičių laikotarpiu numatytas bendras ir nediferencijuotas didžiosios dalies srauto ir vietos nustatymo duomenų saugojimas

76 Atsižvelgiant į šiuos principinius svarstymus reikia nagrinėti pagrindinėje byloje nagrinėjamų nacionalinės teisės aktų ypatybes, kurias pabrėžė prašymą priimti prejudicinį sprendimą pateikęs teismas.

77 Pirma, kiek tai susiję su saugomų duomenų apimtimi, iš nutarties dėl prašymo priimti prejudicinį sprendimą matyti, kad teikiant telefonijos paslaugas šiuose teisės aktuose nustatyta saugojimo pareiga apima, be kita ko, duomenis, reikalingus ryšio šaltiniui ir jo paskirties vietai, ryšio pradžios ir pabaigos datai ir laikui arba – SMS, multimedijos ar panašios žinutės atveju – žinutės išsiuntimo ir gavimo momentui, taip pat mobilaus naudojimosi atveju – ryšio prieigos taškų, kuriais skambinantysis abonentas ir abonentas, kuriam buvo skambinta, naudojosi ryšio pradžioje, pavadinimui nustatyti. Teikiant interneto prieigos paslaugas pareiga saugoti, be kita ko, apima abonentui priskirtą IP adresą, interneto naudojimo iš priskirto IP adreso pradžios ir pabaigos datą ir laiką, o mobilaus naudojimo atveju – interneto ryšio pradžioje naudotų ryšio prieigos taškų pavadinimą. Taip pat saugomi duomenys, leidžiantys sužinoti atitinkamą ryšio prieigos tašką aptarnaujančių antenų geografinę padėtį ir didžiausios spinduliuotės kryptis.

78 Nors pagal pagrindinėje byloje nagrinėjamus nacionalinės teisės aktus saugojimo pareiga netaikoma pranešimo turiniui ir duomenims, susijusiems su lankytomis interneto svetainėmis, ir nustatyta, kad ryšio prieigos taško identifikatorius saugomas tik ryšio pradžioje, reikia pažymėti, kad iš esmės tas pats pasakytina apie Direktyvą 2006/24 perkeliančius nacionalinės teisės aktus, kurie buvo nagrinėjami bylose, kuriose priimtas 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). Tačiau, nepaisant šių apribojimų, Teisingumo Teismas tame sprendime nusprendė, kad pagal minėtą direktyvą ir šiuos nacionalinės teisės aktus saugomų duomenų kategorijos gali leisti daryti labai tikslias išvadas apie atitinkamų asmenų privatų gyvenimą, kaip antai kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ar kitokį judėjimą, vykdomą veiklą, šių asmenų socialinius ryšius ir jų lankomą socialinę aplinką, ir būtent suteikia priemones šių asmenų profiliui nustatyti.

79 Be to, svarbu pažymėti, kad nors pagrindinėje byloje nagrinėjami teisės aktai neapima duomenų, susijusių su lankytomis interneto svetainėmis, vis dėlto juose numatytas IP adresų saugojimas. Tačiau, kadangi šie adresai gali būti naudojami būtent išsamiai interneto vartotojo naršymo keliams, taigi, ir jo veiklai internete, atsekti, šie duomenys leidžia nustatyti išsamų šio vartotojo profilį. Taigi tokiam atsekimui reikalingų minėtų IP adresų saugojimas ir analizė yra didelis pagrindinių interneto vartotojo teisių, įtvirtintų Chartijos 7 ir 8 straipsniuose, suvaržymas (šiuo klausimu žr. 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 153 punktą).

80 Be to, kaip savo rašytinėse pastabose pažymėjo *SpaceNet*, su elektroninio pašto paslaugomis susiję duomenys, nors jiems netaikoma pagrindinėje byloje nagrinėjamuose teisės aktuose numatyta saugojimo pareiga, yra tik labai maža nagrinėjamų duomenų dalis.

81 Taigi, kaip išvados 60 punkte iš esmės pažymėjo generalinis advokatas, pagrindinėje byloje nagrinėjamuose nacionalinės teisės aktuose numatyta saugojimo pareiga apima labai plačią srauto ir vietos nustatymo duomenų visumą, kuri iš esmės atitinka duomenis, dėl kurių priimta šio sprendimo 78 punkte priminta suformuota jurisprudencija.

82 Be to, atsakydama į per posėdį pateiktą klausimą Vokietijos vyriausybė patikslino, kad tik 1 300 subjektų buvo įtraukti į socialinio ar religinio pobūdžio asmenų, institucijų ar organizacijų, kurių elektroninių ryšių duomenys nėra saugomi pagal TKG 99 straipsnio 2 dalį ir 113b straipsnio 6 dalį, sąrašą, o tai akivaizdžiai sudaro nedidelę visų telekomunikacijų paslaugų vartotojų Vokietijoje, kurių duomenims taikoma pagrindinėje byloje nagrinėjamuose nacionalinės teisės aktuose numatyta saugojimo pareiga, dalį. Taigi saugomi, be kita ko, naudotojų, kuriems taikoma profesinė paslaptis, kaip antai advokatų, gydytojų ir žurnalistų, duomenys.

83 Taigi iš nutarties dėl prašymo priimti prejudicinį sprendimą matyti, kad šiuose nacionalinės teisės aktuose numatytas srauto ir vietos nustatymo duomenų saugojimas apima beveik visus gyventojus, nors jų padėtis net netiesiogiai negali lemti baudžiamojo persekiojimo. Be to, pagal juos reikalaujama be priežasties bendrai ir nediferencijuojant asmeniniu, laiko ir geografiniu požiūriais saugoti didžiąją dalį srauto ir vietos nustatymo duomenų, kurių apimtis iš esmės atitinka bylose, kuriose buvo suformuota šio sprendimo 78 punkte nurodyta jurisprudencija, saugomų duomenų apimtį.

84 Taigi, atsižvelgiant į šio sprendimo 75 punkte nurodytą jurisprudenciją, tokia pareiga saugoti duomenis, kaip nagrinėjama pagrindinėje byloje, negali būti laikoma tiksliniu duomenų saugojimu, priešingai, nei teigia Vokietijos vyriausybė.

85 Antra, kiek tai susiję su duomenų saugojimo trukme, iš Direktyvos 2002/58 15 straipsnio 1 dalies antro sakinio matyti, kad nacionalinėje priemonėje, kurioje nustatoma bendro ir nediferencijuoto saugojimo pareiga, numatytas saugojimo laikotarpis yra reikšmingas veiksnys, be kita ko, siekiant nustatyti, ar pagal Sąjungos teisę draudžiama tokia priemonė, nes pagal minėtą sakinį reikalaujama, kad šis terminas būtų „ribotas“.

86 Šiuo atveju tiesa, kad tokie terminai, kurie pagal TKG 113b straipsnio 1 dalį yra keturios savaitės vietos nustatymo duomenims ir dešimt savaičių kitiems duomenims, yra gerokai trumpesni, nei numatyti nacionalinės teisės aktuose, kuriuose nustatyta bendro ir nediferencijuoto saugojimo pareiga ir kuriuos nagrinėjo Teisingumo Teismas 2016 m. gruodžio 21 d. Sprendime *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970), 2020 m. spalio 6 d. Sprendime *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791), taip pat 2022 m. balandžio 5 d. Sprendime *Commissioner of An Garda Síochána ir kt.* (C-140/20, EU:C:2022:258).

87 Vis dėlto, kaip matyti iš šio sprendimo 61 punkte nurodytos jurisprudencijos, suvaržymo rimtumas kyla dėl pavojaus, ypač atsižvelgiant į jų skaičių ir įvairovę, kad visi saugomi duomenys leidžia daryti labai tikslias išvadas apie asmens ar asmenų, kurių duomenys saugomi, privatų gyvenimą ir visų pirma gali padėti nustatyti atitinkamo asmens ar asmenų profilį, kuris yra tokia pati jautri informacija, atsižvelgiant į teisę į privataus gyvenimo gerbimą, kaip ir pats pranešimų turinys.

88 Taigi srauto ar vietos nustatymo duomenų, galinčių suteikti informacijos apie elektroninių ryšių priemonės naudotojo pranešimus arba apie jo naudojamų galinių įrenginių buvimo vietą, saugojimas bet kuriuo atveju yra rimto pobūdžio, neatsižvelgiant į saugojimo laikotarpio trukmę, saugomų duomenų kiekį ar jų esmę, jeigu visi šie duomenys gali leisti padaryti labai tikslias išvadas

apie atitinkamo asmens ar asmenų privatų gyvenimą (žr., kiek tai susiję su prieiga prie tokių duomenų, 2021 m. kovo 2 d. Sprendimo *Prokuratuur (Prieigos prie elektroninių ryšių duomenų sąlygos)*, C-746/18, EU:C:2021:152, 39 punktą).

89 Šiuo klausimu pažymėtina, kad net nedidelio kiekio srauto ar vietos nustatymo duomenų saugojimas arba šių duomenų saugojimas trumpu laikotarpiu gali suteikti labai tikslios informacijos apie elektroninių ryšių priemonės naudotojo privatų gyvenimą. Be to, turimų duomenų kiekis ir iš jų gaunama labai konkreti informacija apie atitinkamo asmens privatų gyvenimą yra aplinkybės, kurias galima įvertinti tik susipažinus su minėtais duomenimis. Tačiau suvaržymas, kylantis dėl minėtų duomenų saugojimo, neišvengiamai atsiranda prieš tai, kai galima susipažinti su duomenis ir iš jų gaunama informacija. Taigi suvaržymo, kurį reiškia saugojimas, dydis turi būti vertinamas atsižvelgiant į atitinkamų asmenų privačiam gyvenimui keliamą pavojų, bendrai susijusį su saugomų duomenų kategorija; be to, nesvarbu, ar iš jų gaunama informacija apie privatų gyvenimą konkrečiai yra jautri (šiuo klausimu žr. 2021 m. kovo 2 d. Sprendimo *Prokuratuur (Prieigos prie elektroninių ryšių duomenų sąlygos)*, C-746/18, EU:C:2021:152, 40 punktą).

90 Nagrinėjamu atveju, kaip matyti iš šio sprendimo 77 punkto ir kaip buvo patvirtinta per teismo posėdį, iš visų srauto ir vietos nustatymo duomenų, saugomų atitinkamai dešimt ir keturias savaites, gali būti daromos labai tikslios išvados dėl asmenų, kurių duomenys saugomi, privataus gyvenimo, kaip antai kasdienio gyvenimo įpročių, nuolatinių ar laikinų gyvenamųjų vietų, kasdienių ar kitokių kelionių, vykdomos veiklos, šių asmenų socialinių ryšių ir jų lankomos socialinės aplinkos, ir būtent nustatomas šių asmenų profilis.

91 Trečia, kiek tai susiję su pagrindinėje byloje nagrinėjamuose nacionalinės teisės aktuose numatytomis garantijomis, kuriomis siekiama apsaugoti saugomus duomenis nuo piktnaudžiavimo rizikos ir bet kokios neteisėtos prieigos, reikia pažymėti, kad, kaip matyti iš šio sprendimo 60 punkte primintos jurisprudencijos, šių duomenų saugojimas ir prieiga prie jų yra skirtingi Chartijos 7 ir 11 straipsniuose įtvirtintų pagrindinių teisių suvaržymai, kuriuos būtina pateisinti atskirai pagal Chartijos 52 straipsnio 1 dalį. Iš to matyti, kad dėl nacionalinės teisės aktų, kuriais užtikrinamas visiškas iš jurisprudencijos, kuria išaiškinta Direktyva 2002/58 dėl prieigos prie saugomų duomenų, kylančių sąlygų laikymasis, pobūdžio negali būti nei apribotas, nei ištaisytas didelis šios direktyvos 5 ir 6 straipsniuose įtvirtintų teisių ir pagrindinių teisių, kurias šie straipsniai sukonkretina, suvaržymas, atsirandantis dėl šiuose nacionalinės teisės aktuose numatyto bendro šių duomenų saugojimo (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 47 punktas).

92 Galiausiai, ketvirta, dėl Europos Komisijos argumento, kad itin sunkūs nusikaltimai gali būti prilyginami grėsmei nacionaliniam saugumui, Teisingumo Teismas jau yra nusprendęs, kad nacionalinio saugumo užtikrinimo tikslas atitinka pagrindinį interesą apsaugoti esmines valstybės funkcijas ir pagrindinius visuomenės interesus ir apima veiklos, galinčios rimtai destabilizuoti pagrindines valstybės konstitucines, politines, ekonomines ar socialines struktūras, visų pirma keliančios tiesioginį pavojų visuomenei, gyventojams ar pačiai valstybei, pavyzdžiui, teroristinės veiklos, prevenciją ir baudžiamąjį persekiojimą už ją (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 61 punktas ir jame nurodyta jurisprudencija).

93 Skirtingai nei nusikalstamumas, net ypač sunkūs nusikaltimai, grėsmė nacionaliniam saugumui turi būti tikra, esama ar bent jau numatoma, o tai reiškia, kad turi būti pakankamai konkrečių aplinkybių, kad būtų galima pateisinti bendro ir nediferencijuoto srauto ir vietos nustatymo

duomenų saugojimo priemonę ribotą laikotarpį. Taigi tokia grėsmė savo pobūdžiu, rimtumu ir ją sudarančių aplinkybių specifika skiriasi nuo bendros ir nuolatinės rizikos, susijusios su įtampa ar net dideliais sunkumais visuomenės saugumui arba sunkiomis baudžiamosiomis veikomis (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 62 punktas ir jame nurodyta jurisprudencija).

94 Taigi nusikalstamumas, net ypač sunkūs nusikaltimai, negali būti prilyginti grėsmei nacionaliniam saugumui. Toks prilyginimas galėtų sukurti tarpinę nacionalinio saugumo ir visuomenės saugumo kategoriją, siekiant visuomenės saugumui taikyti nacionaliniam saugumui būdingus reikalavimus (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 63 punktas).

Dėl priemonių, kuriomis numatytas tikslinis saugojimas, IP adresų saugojimas arba operatyvus saugojimas

95 Kelios vyriausybės, tarp jų ir Prancūzijos vyriausybė, pažymi, kad tik bendras ir nediferencijuotas saugojimas leidžia veiksmingai pasiekti saugojimo priemonėmis siekiamų tikslų, o Vokietijos vyriausybė iš esmės nurodo, kad tokios išvados nepaneigia aplinkybė, jog valstybės narės gali imtis šio sprendimo 75 punkte nurodytų tikslinio ir operatyvaus saugojimo priemonių.

96 Šiuo klausimu reikia pažymėti, pirma, kad baudžiamojo persekiojimo veiksmingumas paprastai priklauso ne nuo vienos, bet nuo visų tyrimo priemonių, kurias šiuo tikslu gali taikyti kompetentingos nacionalinės valdžios institucijos (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 69 punktas).

97 Antra, pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, kaip ji išaiškinta šio sprendimo 75 punkte primintoje jurisprudencijoje, valstybės narės, siekdamos kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui, gali priimti ne tik priemones, kuriomis nustatomas tikslinis ir operatyvus saugojimas, bet ir priemones, numatančias bendrą ir nediferencijuotą saugojimą, pirma, duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, ir, antra, ryšio šaltinio IP adresų (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 70 punktas).

98 Šiuo klausimu neginčijama, kad duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas gali prisidėti prie kovos su sunkiais nusikaltimais, jeigu šie duomenys leidžia nustatyti asmenis, kurie naudojosi tokiomis priemonėmis, rengdami arba vykdydami sunkius nusikaltimus (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 71 punktas).

99 Taigi pagal Direktyvą 2002/58 nedraudžiama bendrai saugoti su civiline tapatybe susijusių duomenų, siekiant kovoti su nusikalstamumu apskritai. Šiomis aplinkybėmis reikia patikslinti, kad nei pagal šią direktyvą, nei pagal kokį nors kitą Sąjungos teisės aktą nedraudžiami nacionalinės teisės aktai, kuriais siekiama kovoti su sunkiais nusikaltimais ir pagal kuriuos tokios elektroninių ryšių priemonės, kaip iš anksto apmokėtos SIM kortelės, įsigijimas siejamas su sąlyga, kad patikrinami oficialūs dokumentai, patvirtinantys pirkėjo tapatybę, ir kad pardavėjas registruoja juose esančią informaciją, nes pardavėjas prireikus privalo suteikti kompetentingoms nacionalinėms institucijoms prieigą prie tokios informacijos (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 72 punktas).

100 Be to, reikia priminti, kad bendras ryšio šaltinio IP adresų saugojimas yra didelis Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymas, nes šie IP adresai gali leisti daryti tikslias išvadas apie atitinkamos elektroninių ryšių priemonės naudotojo privatų gyvenimą ir turėti atgrasomąjį poveikį naudojimuisi Chartijos 11 straipsnyje užtikrinama saviraiškos laisve. Vis dėlto, kiek tai susiję su tokiu saugojimu, Teisingumo Teismas yra konstatavęs, kad siekiant suderinti atitinkamas teises ir teisėtus interesus, kaip to reikalaujama pagal šio sprendimo 65–68 punktuose nurodytą jurisprudenciją, reikia atsižvelgti į tai, kad tuo atveju, kai nusikaltimas padaromas internete, visų pirma vaikų pornografijos, kaip tai suprantama pagal 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvos 2011/93/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL L 335, 2011, p. 1; klaidų ištaisymas OL L 18, 2012, p. 7), 2 straipsnio c punktą, įsigijimo, sklaidos, perdavimo arba pateikimo internetu atveju, IP adresas gali būti vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam toks adresas buvo suteiktas šios nusikalstamos veikos padarymo momentu (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 73 punktas).

101 Šiomis aplinkybėmis tiesa, kad teisėkūros priemonė, kurioje numatyta saugoti visų fizinių asmenų, turinčių galinį įrenginį, iš kurio gali būti suteikta prieiga prie interneto, IP adresus, apima asmenis, kurie iš pirmo žvilgsnio nėra susiję, kaip tai suprantama pagal šio sprendimo 70 punkte nurodytą jurisprudenciją, su siekiamais tikslais, ir kad interneto vartotojai, atsižvelgiant į tai, kas konstatuota šio sprendimo 54 punkte, turi teisę pagal Chartijos 7 ir 8 straipsnius tikėtis, kad jų tapatybė iš principo nebus atskleista, tačiau teisėkūros priemonė, numatanti vien bendrą ir nediferencijuotą prisijungimo šaltinio IP adresų saugojimą, iš esmės nėra prieštaraujanti Direktyvos 2002/58 15 straipsnio 1 daliai, siejamai su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, jeigu ši galimybė taikoma griežtai laikantis materialinių ir procedūrinių sąlygų, reglamentuojančių šių duomenų naudojimą (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 155 punktas).

102 Atsižvelgiant į Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymo, kurį sudaro šis saugojimas, dydį, šį suvaržymą gali pateisinti tik kova su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencija, kaip ir siekis užtikrinti nacionalinį saugumą. Be to, duomenų saugojimo trukmė negali viršyti to, kas griežtai būtina atsižvelgiant į siekiamą tikslą. Galiausiai tokio pobūdžio priemonėje turi būti numatytos griežtos šių duomenų naudojimo sąlygos ir garantijos, susijusios, be kita ko, su atitinkamų asmenų pranešimų ir vykdomos veiklos internete sekimu (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 156 punktas).

103 Taigi, priešingai, nei pažymėjo prašymą priimti prejudicinį sprendimą pateikęs teismas, nėra prieštaravimo tarp 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791) 155 ir 168 punktų. Kaip išvados 81 ir 82 punktuose iš esmės pažymėjo generalinis advokatas, iš šio sprendimo 155 punkto, siejamo su 156 ir 168 punktais, aiškiai matyti, kad tik kova su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencija, kaip ir nacionalinio saugumo užtikrinimas, gali pateisinti bendrą prisijungimo šaltinio IP adresų saugojimą, neatsižvelgiant į tai, ar atitinkami asmenys gali būti bent netiesiogiai susiję su siekiamais tikslais.

104 Trečia, kalbant apie teisėkūros priemones, kuriomis numatytas tikslinis ir operatyvus srauto ir vietos nustatymo duomenų saugojimas, pažymėtina, kad tam tikri valstybių narių nurodyti svarstymai dėl tokių priemonių rodo siauresnį šių priemonių apimties supratimą, nei nustatytas šio sprendimo 75 punkte nurodytoje jurisprudencijoje. Iš tiesų, nors remiantis tuo, kas priminta

šio sprendimo 57 punkte, šios saugojimo priemonės turi būti išimtys Direktyva 2002/58 nustatytoje sistemoje, pagal šią direktyvą, siejamą su Chartijos 7, 8 ir 11 straipsniuose ir 52 straipsnio 1 dalyje įtvirtintomis pagrindinėmis teisėmis, galimybė nustatyti įpareigojimą, kuriuo numatomas tikslinis saugojimas, nesiejama su sąlyga, kad vietos, kuriose gali būti įvykdyti sunkūs nusikaltimai, ar asmenys, įtariami dalyvavę vykdant tokį nusikaltimą, turi būti žinomi iš anksto. Be to, minėtoje direktyvoje nereikalaujama, kad įpareigojimas, kuriuo nustatomas operatyvus saugojimas, būtų taikomas tik įtariamiesiems, identifikuotiems iki nustatant tokį įpareigojimą (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 75 punktas).

105 Pirma, dėl tikslinio saugojimo Teisingumo Teismas nusprendė, kad pagal Direktyvos 2002/58 15 straipsnio 1 dalį nedraudžiami nacionalinės teisės aktai, grindžiami objektyviais kriterijais, leidžiančiais nustatyti asmenis, kurių srauto ir vietos nustatymo duomenys gali bent netiesiogiai atskleisti ryšį su sunkiais nusikaltimais, prisidėti prie kovos su jais arba užkirsti kelią dideliam pavojui visuomenės ar nacionaliniam saugumui (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 76 punktas ir jame nurodyta jurisprudencija).

106 Šiuo klausimu Teisingumo Teismas patikslino, kad nors šie objektyvūs veiksniai gali skirtis atsižvelgiant į priemones, kurių imamasi sunkių nusikaltimų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslais, tokie asmenys gali būti, be kita ko, tie, kurie per taikomas nacionalines procedūras ir remiantis objektyviais ir nediskriminaciniais kriterijais iš anksto buvo nustatyti kaip keliantys grėsmę visuomenės saugumui arba atitinkamos valstybės narės nacionaliniam saugumui (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 77 punktas).

107 Taigi valstybės narės turi galimybę nustatyti saugojimo priemones asmenims, dėl kurių remiantis tokiu identifikavimu atliekamas tyrimas ar taikomos kitos aktualios stebėjimo priemonės ar kurių nacionaliniame nuosprendžių registre yra įrašas apie ankstesnius teistumus už sunkius nusikaltimus, dėl ko gali kilti didelė pakartotinio nusikaltimo rizika. Kai toks identifikavimas grindžiamas objektyviais ir nediskriminaciniais kriterijais, apibrėžtais nacionalinėje teisėje, tikslinis saugojimas, taikomas taip identifikuotiems asmenims, yra pateisinamas (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 78 punktas).

108 Antra, tikslinį srauto ir vietos nustatymo duomenų saugojimą numatanti priemonė, remiantis nacionalinio įstatymų leidėjo pasirinkimu ir griežtai laikantis proporcingumo principo, taip pat gali būti grindžiama geografiniu kriterijumi, kai kompetentingos nacionalinės institucijos, remdamosi objektyviais ir nediskriminaciniais veiksniais, mano, kad vienoje ar keliose geografinėse teritorijose yra didelė rizika, kad bus rengiami ar vykdomi sunkūs nusikaltimai. Tokios zonos gali būti, be kita ko, vietos, kuriose įvykdoma daug sunkių nusikalstamų veikų, vietos, kuriose ypač susiduriama su sunkių nusikalstamų veikų vykdymo grėsme, pavyzdžiui, vietos ar infrastruktūra, kurias reguliariai lanko labai daug asmenų, arba strateginės vietos, pavyzdžiui, oro uostai, stotys, jūrų uostai ar rinkliavų zonos (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 79 punktas ir jame nurodyta jurisprudencija).

109 Reikia pabrėžti, kad pagal šią jurisprudenciją pirmesniame šio sprendimo punkte nurodytoms teritorijoms kompetentingos nacionalinės valdžios institucijos gali taikyti tikslinio saugojimo priemonę, pagrįstą geografiniu kriterijumi, kaip antai vidutiniu nusikalstamumo lygiu geografinėje

zonoje, ir nebūtinai turi turėti konkrečių įrodymų dėl sunkių nusikaltimų rengimo ar vykdymo atitinkamose teritorijose. Tokiu kriterijumi grindžiamas tikslinis duomenų saugojimas, atsižvelgiant į nurodytus sunkius nusikaltimus ir atitinkamų valstybių narių padėtį, gali paveikti tiek vietas, kuriose įvykdoma daug sunkių nusikaltimų, tiek vietas, kuriose tokių veikų padarymo tikimybė didelė, tad jis iš esmės taip pat negali lemti diskriminacijos, nes vidutinio sunkių nusikaltimų lygio kriterijus pats savaime neturi jokio ryšio su potencialiai diskriminuojančiais elementais (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 80 punktas).

110 Be to, visų pirma tikslinio saugojimo priemonė, susijusi su vietomis ar infrastruktūra, kuriose reguliariai lankosi labai daug asmenų, ar su tokiomis strateginėmis vietomis, kaip oro uostai, stotys, jūrų uostai ar rinkliavų zonos, leidžia kompetentingoms institucijoms rinkti srauto duomenis, ir būtent visų asmenų, kurie tam tikru momentu naudojasi elektroninių ryšių priemone vienoje iš šių vietų, vietos nustatymo duomenis. Taigi tokia tikslinio saugojimo priemonė gali leisti šioms valdžios institucijoms, turinčioms prieigą prie taip saugomų duomenų, gauti informacijos apie šių asmenų buvimą šios priemonės taikymo vietose ar geografinėse teritorijose ir apie jų judėjimą tarp jų arba jų viduje, taip pat, siekiant kovoti su sunkiais nusikaltimais, daryti išvadas dėl jų buvimo ir veiklos šiose vietose ar geografinėse teritorijose tam tikru saugojimo laikotarpio momentu (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 81 punktas).

111 Taip pat reikia pažymėti, kad geografinės teritorijos, kurioms taikomas toks tikslinis saugojimas, gali, o prireikus – turi būti pakeistos, atsižvelgiant į jų atranką pateisinusių sąlygų raidą, kad būtų galima reaguoti į kovos su sunkiais nusikaltimais pokyčius. Teisingumo Teismas jau yra nusprendęs, kad šio sprendimo 105–110 punktuose aprašytos tikslinio saugojimo priemonės negali viršyti to, kas griežtai būtina atsižvelgiant į siekiamą tikslą ir jas pateisinančias aplinkybes, nedarant poveikio galimam pratęsimui, kai išlieka būtinybė užtikrinti tokį saugojimą (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 151 punktas; taip pat 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 82 punktas).

112 Kalbant apie galimybę numatyti kitus nei asmeninio ar geografinio ryšio skiriamuosius kriterijus, pažymėtina, kad, siekiant taikyti tikslinį srauto ir vietos nustatymo duomenų saugojimą, negalima atmesti galimybės, kad į kitus objektyvius ir nediskriminacinius kriterijus gali būti atsižvelgta norint užtikrinti, kad tikslinio saugojimo apimtis neviršytų to, kas griežtai būtina, ir nustatyti bent jau netiesioginį sunkių nusikaltimų ir asmenų, kurių duomenys saugomi, ryšį. Šiuo aspektu, kadangi Direktyvos 2002/58 15 straipsnio 1 dalis susijusi su valstybių narių teisėkūros priemonėmis, būtent valstybės narės, o ne Teisingumo Teismas, turi nustatyti tokius kriterijus, turint omenyje, kad taip negalima vėl nustatyti bendro ir nediferencijuoto srauto ir vietos nustatymo duomenų saugojimo (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 83 punktas).

113 Bet kuriuo atveju, kaip išvados 50 punkte pažymėjo generalinis advokatas, galimi sunkumai tiksliai apibrėžiant atvejus ir sąlygas, kuriomis galima vykdyti tikslinį saugojimą, negali pateisinti to, kad valstybės narės, išimtį padarydamos taisykle, numato bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 84 punktas).

114 Antra, dėl operatyvaus srauto ir vietos nustatymo duomenų, kuriuos elektroninių ryšių paslaugų teikėjai tvarko ir saugo, remdamiesi Direktyvos 2002/58 5, 6 ir 9 straipsniais arba teisėkūros priemonėmis, priimtomis pagal šios direktyvos 15 straipsnio 1 dalį, saugojimo reikia priminti, kad šie duomenys, atsižvelgiant į konkretų atvejį, iš principo turi būti ištrinti arba padaryti anoniminiai pasibaigus teisės aktuose nustatytiems terminams, per kuriuos jie turi būti tvarkomi ir saugomi pagal minėtą direktyvą perkeliančias nacionalinės teisės nuostatas. Vis dėlto Teisingumo Teismas nusprendė, kad atliekant tokį tvarkymą ir saugojimą gali susiklostyti situacijos, kai kyla būtinybė saugoti šiuos duomenis ilgiau, nei numatyti terminai, siekiant išaiškinti sunkias nusikalstamas veikas arba nacionalinio saugumo pažeidimus; taip gali būti tiek tuo atveju, kai šios nusikalstamos veikos ar pažeidimai jau yra nustatyti, tiek tuo atveju, kai, objektyviai išnagrinėjus visas svarbias aplinkybes, gali būti pagrįstai įtariamas jų egzistavimas (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 85 punktas).

115 Esant tokiai situacijai, valstybės narės, atsižvelgdamos į šio sprendimo 65–68 punktuose nurodytą būtinybę suderinti nagrinėjamus teises ir teisėtus interesus, gali pagal Direktyvos 2002/58 15 straipsnio 1 dalį priimtuose teisės aktuose numatyti galimybę kompetentingos institucijos sprendimu, kuriam taikoma veiksminga teisminė kontrolė, įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų jų turimų srauto ir vietos nustatymo duomenų saugojimą (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 163 punktas; taip pat 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 86 punktas).

116 Jeigu tokio operatyvaus saugojimo tikslas nebeatitinka tikslų, dėl kurių duomenys buvo surinkti ir saugomi iš pradžių, o bet koks duomenų tvarkymas pagal Chartijos 8 straipsnio 2 dalį turi atitikti apibrėžtus tikslus, teisės aktuose valstybės narės turi nurodyti tikslą, dėl kurio galima operatyviai saugoti duomenis. Atsižvelgiant į Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymo, kurį gali sukelti toks saugojimas, dydį, šį suvaržymą galima pateisinti tik kova su sunkiais nusikaltimais ir *a fortiori* nacionalinio saugumo užtikrinimu, su sąlyga, kad šia priemone ir prieiga prie taip saugomų duomenų laikomasi to, kas griežtai būtina, ribų, kaip nurodyta 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791) 164–167 punktuose (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 87 punktas).

117 Teisingumo Teismas patikslino, kad tokia saugojimo priemonė neturi apsiriboti tik asmenų, iš anksto pripažintų keliančiais grėsmę atitinkamos valstybės narės visuomenės ar nacionaliniam saugumui, arba asmenų, kurie konkrečiai įtariami padarę sunkų nusikaltimą ar pasikėsinę į nacionalinį saugumą, duomenimis. Teisingumo Teismo teigimu, laikantis Direktyvos 2002/58 15 straipsnio 1 dalyje, siejamoje su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, nustatytos sistemos ir remiantis tuo, kas išdėstyta šio sprendimo 70 punkte, tokia priemonė, atsižvelgiant į nacionalinio įstatymų leidėjo pasirinkimą ir laikantis to, kas griežtai būtina, gali apimti kitų asmenų nei tie, kurie įtariami planavę arba padarę sunkią nusikalstamą veiką ar nacionalinio saugumo pažeidimą, srauto ir vietos nustatymo duomenis, jeigu tie duomenys, remiantis objektyviais ir nediskriminaciniais veiksniais, gali padėti išaiškinti tokią nusikalstamą veiką ar nacionalinio saugumo pažeidimą; tai gali būti, pavyzdžiui, aukos, jos socialinės ar profesinės aplinkos duomenys (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 165 punktas; taip pat 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 88 punktas).

118 Taigi teisėkūros priemone gali būti leidžiama taikyti įpareigojimą elektroninių ryšių paslaugų teikėjams operatyviai saugoti srauto ir vietos nustatymo duomenis, visų pirma asmenų, su kuriais prieš kylant didelei grėsmei visuomenės saugumui arba įvykdant sunkų nusikaltimą naudodamasi savo elektroninių ryšių priemonėmis susisiekė auka (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 89 punktas).

119 Pagal šio sprendimo 117 punkte primintą Teisingumo Teismo jurisprudenciją ir laikantys sąlygų, nurodytų tame punkte, toks operatyvus saugojimas taip pat gali būti taikomas tam tikroms geografinėms zonoms, pavyzdžiui, atitinkamos nusikalstamos veikos ar nacionalinio saugumo pažeidimo rengimo ar vykdymo vietoms. Reikia patikslinti, kad tokia priemonė taip pat gali būti taikoma srauto ir vietos nustatymo duomenims, susijusiems su vieta, kurioje dingo asmuo, potencialiai nukentėjęs nuo sunkios nusikalstamos veikos, su sąlyga, kad ši priemonė ir prieiga prie taip saugomų duomenų neviršytų to, kas griežtai būtina siekiant kovoti su sunkiais nusikaltimais ar užtikrinant nacionalinį saugumą, kaip nurodyta 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791) 164–167 punktuose (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 90 punktas).

120 Be to, svarbu pažymėti, kad pagal Direktyvos 2002/58 15 straipsnio 1 dalį kompetentingoms nacionalinėms institucijoms nedraudžiama taikyti operatyvaus saugojimo priemonės nuo pat pirmojo tyrimo, susijusio su didele grėsme visuomenės saugumui arba galimu sunkiu nusikaltimu, etapo, t. y. nuo momento, kai šios institucijos pagal atitinkamas nacionalinės teisės nuostatas gali pradėti tokį tyrimą (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 91 punktas).

121 Dėl šio sprendimo 75 punkte nurodytų įvairių srauto ir vietos nustatymo duomenų saugojimo priemonių reikia pažymėti, kad atsižvelgiant į nacionalinio įstatymų leidėjo pasirinkimą ir laikantis to, kas griežtai būtina, šios skirtingos priemonės gali būti taikomos kartu. Šiomis aplinkybėmis pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, kaip ji išaiškinta 2020 m. spalio 6 d. Sprendime *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791), nedraudžiamas šių priemonių derinys (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 92 punktas).

122 Ketvirta, galiausiai reikia pažymėti, kad pagal Teisingumo Teismo suformuotą jurisprudenciją, apibendrintą 2020 m. spalio 6 d. Sprendime *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791), pagal Direktyvos 2002/58 15 straipsnio 1 dalį priimtų priemonių proporcingumas reikalauja paisyti ne tik tinkamumo ir būtinumo reikalavimų, bet ir reikalavimų, susijusių su šių priemonių proporcingumu siekiamam tikslui (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 93 punktas).

123 Šiomis aplinkybėmis reikia priminti, kad 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.* (C-293/12 ir C-594/12, EU:C:2014:238) 51 punkte Teisingumo Teismas nusprendė, kad nors kova su sunkiais nusikaltimais yra pirmaeilės svarbos užtikrinant visuomenės saugumą, o jos veiksmingumas gali labai priklausyti nuo pažangių tyrimo technikų panaudojimo, vien toks bendrojo intereso tikslas, kad ir koks fundamentalus būtų, negali pateisinti to, kad tokia bendro ir nediferencijuoto srauto ir vietos nustatymo duomenų saugojimo priemonė, kaip įtvirtintina Direktyvoje 2006/24, būtų laikoma būtina (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 94 punktas).

124 Kartu 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791) 145 punkte Teisingumo Teismas patikslino, kad net valstybių narių pareigomis veikti, kurios tam tikrais atvejais gali kilti iš Chartijos 3, 4 ir 7 straipsnių ir kurios, kaip pažymėta to sprendimo 64 punkte, susijusios su taisyklių, leidžiančių veiksmingai kovoti su nusikalstamomis veikomis, nustatymu, negalima pateisinti tokių didelių Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių beveik visų gyventojų teisių suvaržymų, kokie nustatyti nacionalinės teisės aktuose, numatančiuose srauto ir vietos nustatymo duomenų saugojimą, kai atitinkamų asmenų duomenys negali atskleisti bent netiesioginio ryšio su siekiamu tikslu (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 95 punktas).

125 Be to, 2021 m. gegužės 25 d. EŽTT sprendimu *Big Brother Watch ir kt. prieš Jungtinę Karalystę* (CE:ECHR:2021:0525JUD 005817013) ir 2021 m. gegužės 25 d. Sprendimu *Centrum för Rättvisa prieš Švediją* (CE:ECHR:2021:0525JUD 003525208), kuriais per posėdį rėmėsi kai kurios vyriausybės, teigdamos, kad pagal EŽTK nedraudžiami nacionalinės teisės aktai, kuriuose iš esmės numatytas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas, negalima paneigti pirma nurodyto Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo. Tuose sprendimuose buvo nagrinėjamas masinis tarptautinių ryšių duomenų perėmimas. Taigi, kaip per posėdį pažymėjo Komisija, minėtuose sprendimuose Europos Žmogaus Teisių Teismas neišreiškė nuomonės dėl bendro ir nediferencijuoto srauto ir vietos nustatymo duomenų saugojimo nacionalinėje teritorijoje suderinamumo su EŽTK ar dėl didelio masto šių duomenų perėmimo siekiant užkirsti kelią, atskleisti ir tirti sunkias nusikalstamas veikas. Bet kuriuo atveju reikia priminti, kad pagal Chartijos 52 straipsnio 3 dalį siekiama užtikrinti būtiną joje įtvirtintų teisių ir atitinkamų EŽTK garantuojamų teisių darną, nedarant poveikio Sąjungos teisės ir Europos Sąjungos Teisingumo Teismo autonomijai, todėl aiškinant Chartiją į atitinkamas EŽTK teises reikia atsižvelgti tik kaip į minimalios apsaugos ribą (2020 m. gruodžio 17 d. Sprendimo *Centraal Israëlitisch Consistorie van België ir kt.*, C-336/19, EU:C:2020:1031, 56 punktas).

Dėl prieigos prie bendrai ir nediferencijuojant saugomų duomenų

126 Per posėdį Danijos vyriausybė teigė, kad kompetentingos nacionalinės institucijos, siekdamos kovoti su sunkiais nusikaltimais, turėtų turėti prieigą prie srauto ir vietos nustatymo duomenų, kurie buvo saugomi bendrai ir nediferencijuojant, remiantis 2020 m. spalio 6 d. Sprendime *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, 135–139 punktai) suformuota jurisprudencija, kad pašalintų rimtą grėsmę nacionaliniam saugumui, kuri yra reali, esama arba numatoma.

127 Pirmiausia reikia pažymėti, kad suteikiant galimybę kovos su sunkiais nusikaltimais tikslais naudotis srauto ir vietos nustatymo duomenimis, kurie buvo saugomi bendrai ir nediferencijuojant, tokia prieiga priklausytų nuo aplinkybių, nesusijusių su tuo tikslu, atsižvelgiant į tai, ar atitinkamoje valstybėje narėje egzistuoja didelė grėsmė nacionaliniam saugumui, kaip nurodyta pirmesniame punkte; nors vien tikslas kovoti su sunkiais nusikaltimais turėtų pateisinti tokių duomenų saugojimą ir prieigą prie jų, niekas nepateisina nevienodo požiūrio, ypač tarp valstybių narių (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 97 punktas).

128 Kaip Teisingumo Teismas jau yra nusprendęs, prieiga prie srauto ir vietos nustatymo duomenų, kuriuos elektroninių ryšių paslaugų teikėjai saugo taikydami pagal Direktyvos 2002/58 15 straipsnio 1 dalį numatytą priemonę – tokia prieiga turi būti suteikta laikantis sąlygų, nustatytų šią direktyvą aiškinančioje jurisprudencijoje, – iš principo gali būti

pateisinama tik bendrojo intereso tikslu, dėl kurio šiems teikėjams nustatytas toks įpareigojimas saugoti duomenis. Kitaip yra tik tuo atveju, jei prieigos tikslo svarba viršija saugojimą pateisinančio tikslo svarbą (žr. 2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 98 punktas).

129 Vis dėlto Danijos vyriausybės argumentai susiję su situacija, kai numatomo prašymo suteikti prieigą tikslas, t. y. kova su sunkiais nusikaltimais, bendrojo intereso tikslų hierarchijoje yra ne toks svarbus nei duomenų saugojimą pateisinantis tikslas, t. y. nacionalinio saugumo užtikrinimas. Tokiu atveju prieigos prie saugomų duomenų suteikimas prieštarautų šiai bendrojo intereso tikslų hierarchijai, primintai šio sprendimo pirmesniame punkte ir 68, 71, 72 ir 73 punktuose (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 99 punktas).

130 Be to, visų pirma remiantis šio sprendimo 74 punkte priminta jurisprudencija, srauto ir vietos nustatymo duomenys negali būti bendrai ir nediferencijuotai saugomi kovos su sunkiais nusikaltimais tikslais, todėl prieigos prie šių duomenų negalima pateisinti tais pačiais tikslais. Tačiau jeigu šie duomenys išimties tvarka buvo saugomi bendrai ir nediferencijuotai siekiant užtikrinti nacionalinį saugumą nuo grėsmės, kuri yra tikra, esama arba numatoma, laikantis šio sprendimo 71 punkte nurodytų sąlygų, nacionalinės teisėsaugos institucijos negali susipažinti su šiais duomenimis vykstant baudžiamajam persekiojimui, nes priešingu atveju minėtame 74 punkte primintas draudimas saugoti tokius duomenis, siekiant kovoti su sunkiais nusikaltimais, taptų visiškai neveiksmingas (2022 m. balandžio 5 d. Sprendimo *Commissioner of An Garda Síochána ir kt.*, C-140/20, EU:C:2022:258, 100 punktas).

131 Atsižvelgiant į visa tai, kas išdėstyta, į prejudicinį klausimą reikia atsakyti: Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiamos nacionalinės teisėkūros priemonės, kuriomis siekiant kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui prevenciškai numatomas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas. Vis dėlto minėto 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją nedraudžiamos tokios nacionalinės teisėkūros priemonės:

– pagal kurias, siekiant užtikrinti nacionalinį saugumą, leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant saugoti srauto ir vietos nustatymo duomenis tais atvejais, kai atitinkama valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra, esama arba numatoma, o sprendimui, kuriame nustatytas toks įpareigojimas, gali būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi sąlygų ir garantijų, kurios turi būti numatytos; toks įpareigojimas gali būti nustatytas tik laikotarpiu, neviršijančiu to, kas griežtai būtina, bet kurį galima pratęsti, jeigu tokia grėsmė išlieka,

– pagal kurias, siekiant užtikrinti nacionalinį saugumą, 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, atsižvelgiant į atitinkamų asmenų kategorijas arba geografinį kriterijų, būtų apribotas laikotarpio, neviršijančio to, kas griežtai būtina, tačiau kurį galima pratęsti,

– pagal kurias, siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui, numatomas bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas laikotarpiu, neviršijančiu to, kas griežtai būtina,

– pagal kurias, siekiant užtikrinti nacionalinį saugumą, kovoti su nusikalstamumu ir užtikrinti visuomenės saugumą, numatomas bendras ir nediferencijuotas duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas, ir

– pagal kurias, siekiant kovoti su sunkiais nusikaltimais ir *a fortiori* užtikrinti nacionalinį saugumą, leidžiama kompetentingos institucijos sprendimu, kuriam taikoma veiksminga teisminė kontrolė, įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų, kuriuos turi šie paslaugų teikėjai, saugojimą,

kai šiomis priemonėmis taikant aiškias ir tikslias taisykles užtikrinama, kad atitinkami duomenys būtų saugomi laikantis taikomų materialinių ir procedūrinių sąlygų ir kad atitinkami asmenys turėtų veiksmingas garantijas nuo piktnaudžiavimo rizikos.

Dėl bylinėjimosi išlaidų

132 Kadangi šis procesas pagrindinės bylos šalims yra vienas iš etapų prašymą priimti prejudicinį sprendimą pateikusio teismo nagrinėjamoje byloje, bylinėjimosi išlaidų klausimą turi spręsti šis teismas. Išlaidos, susijusios su pastabų pateikimu Teisingumo Teismui, išskyrus tas, kurias patyrė minėtos šalys, nėra atlygintinos.

Remdamasis šiais motyvais, Teisingumo Teismas (didžioji kolegija) nusprendžia:

2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), iš dalies pakeistos 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, 15 straipsnio 1 dalis, siejama su Europos Sąjungos pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi,

turi būti aiškinama taip:

pagal ją draudžiamos nacionalinės teisėkūros priemonės, kuriomis siekiant kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui prevenciškai numatomas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas;

pagal ją nedraudžiamos tokios nacionalinės teisėkūros priemonės:

– **pagal kurias, siekiant užtikrinti nacionalinį saugumą, leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant saugoti srauto ir vietos nustatymo duomenis tais atvejais, kai atitinkama valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra, esama arba numatoma, o sprendimui, kuriame nustatytas toks įpareigojimas, gali būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi sąlygų ir garantijų,**

kurios turi būti numatytos; toks įpareigojimas gali būti nustatytas tik laikotarpiu, neviršijančiu to, kas griežtai būtina, bet kurį galima pratęsti, jeigu tokia grėsmė išlieka,

– **pagal kurias, siekiant užtikrinti nacionalinį saugumą, 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, atsižvelgiant į atitinkamų asmenų kategorijas arba geografinį kriterijų, būtų apribotas laikotarpio, neviršijančio to, kas griežtai būtina, tačiau kurį galima pratęsti,**

– **pagal kurias, siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui, numatomas bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas laikotarpiu, neviršijančiu to, kas griežtai būtina,**

– **pagal kurias, siekiant užtikrinti nacionalinį saugumą, kovoti su nusikalstamumu ir užtikrinti visuomenės saugumą, numatomas bendras ir nediferencijuotas duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas, ir**

– **pagal kurias, siekiant kovoti su sunkiais nusikaltimais ir *a fortiori* užtikrinti nacionalinį saugumą, leidžiama kompetentingos institucijos sprendimu, kuriam taikoma veiksminga teisminė kontrolė, įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų, kuriuos turi šie paslaugų teikėjai, saugojimą,**

kai šiomis priemonėmis taikant aiškias ir tikslias taisykles užtikrinama, kad atitinkami duomenys būtų saugomi laikantis taikomų materialinių ir procedūrinių sąlygų ir kad atitinkami asmenys turėtų veiksmingas garantijas nuo piktnaudžiavimo rizikos.

Parašai.