Teismo praktikos rinkinys

TEISINGUMO TEISMO (didžioji kolegija) SPRENDIMAS

2020 m. spalio 6 d.*

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas elektroninių ryšių sektoriuje – Elektroninių ryšių paslaugų teikėjas – Bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų perdavimas – Nacionalinio saugumo užtikrinimas – Direktyva 2002/58/EB – Taikymo sritis – 1 straipsnio 3 dalis ir 3 straipsnis – Elektroninių ryšių konfidencialumas – Apsauga – 5 straipsnis ir 15 straipsnio 1 dalis – Europos Sąjungos pagrindinių teisių chartija – 7, 8, 11 straipsniai bei 52 straipsnio 1 dalis – ESS 4 straipsnio 2 dalis“

Byloje C-623/17

dėl *Investigatory Powers Tribunal* (Bylų dėl tyrimų įgaliojimų teismas, Jungtinė Karalystė) 2017 m. spalio 18 d. sprendimu, kurį Teisingumo Teismas gavo 2017 m. spalio 31 d., pagal SESV 267 straipsnį pateikto prašymo priimti prejudicinį sprendimą byloje

Privacy International

prieš

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service

TEISINGUMO TEISMAS (didžioji kolegija),

kurį sudaro pirmininkas K. Lenaerts, pirmininko pavaduotoja R. Silva de Lapuerta, kolegijų pirmininkai J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb ir L. S. Rossi, teisėjai J. Malenovský, L. Bay Larsen, T. von Danwitz (pranešėjas), C. Toader, K. Jürimäe, C. Lycourgos ir N. Piçarra,

generalinis advokatas M. Campos Sánchez-Bordona,

posėdžio sekretorė C. Strömholm, administratorė,

atsižvelgęs į rašytinę proceso dalį ir įvykus 2019 m. rugsėjo 9 ir 10 d. posėdžiui,

* Proceso kalba: anglų.

išnagrinėjęs pastabas, pateiktas:

– *Privacy International*, atstovaujamos QC B. Jaffey ir T. de la Mare, solisitoriaus D. Cashman ir advokato H. Roy,

– Jungtinės Karalystės vyriausybės, atstovaujamos Z. Lavery, D. Guðmundsdóttir ir S. Brandon, padedamų QC G. Facenna ir D. Beard, baristerių C. Knight ir R. Palmer,

– Belgijos vyriausybės, atstovaujamos P. Cottin ir J.-C. Halleux, padedamų advokatų J. Vanpraet ir E. de Lophem,

– Čekijos vyriausybės, atstovaujamos M. Smolek, J. Vláčil ir O. Serdula,

– Vokietijos vyriausybės, iš pradžių atstovaujamos M. Hellmann, R. Kanitz, D. Klebs ir T. Henze, vėliau J. Möller, M. Hellmann, R. Kanitz ir D. Klebs,

– Estijos vyriausybės, atstovaujamos A. Kalbus,

– Airijos vyriausybės, atstovaujamos M. Browne, G. Hodge ir A. Joyce, padedamų baristerio D. Fennelly,

– Ispanijos vyriausybės, iš pradžių atstovaujamos L. Aguilera Ruiz ir M. J. García-Valdecasas Dorrego, vėliau L. Aguilera Ruiz,

– Prancūzijos vyriausybės, iš pradžių atstovaujamos E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas ir D. Dubois, vėliau E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune ir D. Dubois,

– Kipro vyriausybės, atstovaujamos E. Symeonidou ir E. Neofytou,

– Latvijos vyriausybės, iš pradžių atstovaujamos V. Soņeca ir I. Kucina, vėliau V. Soņeca,

– Vengrijos vyriausybės, iš pradžių atstovaujamos G. Koós, M. Z. Fehér, G. Tornyai ir Z. Wagner, vėliau G. Koós ir M. Z. Fehér,

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

– Lenkijos vyriausybės, atstovaujamos B. Majczyna, J. Sawicka ir M. Pawlicka,

– Portugalijos vyriausybės, atstovaujamos L. Inez Fernandes, M. Figueiredo ir F. Aragão Homem,

– Švedijos vyriausybės, iš pradžių atstovaujamos A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren ir A. Alriksson, vėliau H. Shev, C. Meyer-Seitz, L. Zettergren ir A. Alriksson,

– Norvegijos vyriausybės, atstovaujamos T. B. Leming, M. Emberland ir J. Vangsnes,

– Europos Komisijos, iš pradžių atstovaujamos H. Kranenborg, M. Wasmeier, D. Nardi ir P. Costa de Oliveira, vėliau H. Kranenborg, M. Wasmeier ir D. Nardi,

– Europos duomenų apsaugos priežiūros pareigūno, atstovaujamo T. Zerdick ir A. Buchta,

susipažinęs su 2020 m. sausio 15 d. posėdyje pateikta generalinio advokato išvada,

priima šį

Sprendimą

1 Prašymas priimti prejudicinį sprendimą pateiktas 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; klaidų ištaisymai OL L 241, 2013, p. 9 ir OL L 275, 2014, p. 8, toliau – Direktyva 2002/58), 1 straipsnio 3 dalies ir 15 straipsnio 1 dalies, siejamų su ESS 4 straipsnio 2 dalimi ir Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7, 8 straipsniais ir 52 straipsnio 1 dalimi, išaiškinimo.

2 Šis prašymas pateiktas nagrinėjant *Privacy International* ginčą su *Secretary of State for Foreign and Commonwealth Affairs* (Užsienio reikalų ir tautų sandraugos ministras, Jungtinė Karalystė), *Secretary of State for the Home Departement* (Vidaus reikalų ministras, Jungtinė Karalystė), *Government Communications Headquarters* (Vyriausybės ryšių centrinis biuras, Jungtinė Karalystė, toliau – GCHQ), *Security Service* (Saugumo tarnyba, Jungtinė Karalystė, toliau – MI5) ir su *Secret Intelligence Service* (Slaptoji žvalgybos tarnyba, Jungtinė Karalystė, toliau – MI6) dėl teisės aktų, kuriais saugumo ir žvalgybos tarnyboms leidžiama gauti ir naudoti masinius ryšio duomenis (*bulk communications data*), teisėtumo.

Teisinis pagrindas

Sąjungos teisė

Direktyva 95/46

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. buvo 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/EB (OL L 119, 2016, p. 1; klaidų ištaisymas OL L 127, 2018, p. 2). Šios direktyvos 3 straipsnis „Taikymo sritis“ buvo suformuluotas taip:

„1. Ši direktyva taikoma automatiniais būdais tvarkant asmens duomenis ištisai arba dalimis ir neautomatiniais būdais tvarkant asmens duomenis, kai tie duomenys sudaro arba yra skirti sudaryti rinkmenų sistemos dalį.

2. Ši direktyva netaikoma tvarkant asmens duomenis:

– kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, kaip antai veikla, kuri numatyta [ESS] 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

4 Direktyvos 2002/58 2, 6, 7, 11, 22, 26 ir 30 konstatuojamosiose dalyse nustatyta:

„(2) Šia direktyva siekiama gerbti pagrindines žmogaus teises ir laikomasi [Chartijos] principų; visų pirma šia direktyva siekiama užtikrinti visapusišką pagarbą minėtos Chartijos 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 [nauja] 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 pirma 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 [Sąjungos] 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.

<…>

(22) Draudimas saugoti pranešimus ir srauto duomenis kitiems nei naudotojai asmenims, taip pat saugoti juos be naudotojų sutikimo nėra skirtas uždrausti šios informacijos automatinį, tarpinį ir tranzitinį saugojimą, jeigu tai daroma tik siekiant perduoti pranešimą elektroninių ryšių tinklu, ir ne ilgiau, nei reikia perdavimui ir srautams valdyti, garantuojant konfidencialumą saugojimo metu. Tais atvejais, kai kitų paslaugų gavėjų pageidavimu būtina užtikrinti didesnį viešai prieinamos informacijos tolesnio perdavimo jiems efektyvumą, ši direktyva neturėtų drausti saugoti tokią informaciją ilgiau su sąlyga, kad ji yra bet kuriuo atveju prieinama visuomenei be jokių ribojimų, o duomenys apie atskirus abonentus ar naudotojus, kurie prašo tokios informacijos, sunaikinami.

<…>

(26) Su abonentais susiję duomenys, kurie yra tvarkomi elektroninių ryšių tinkluose sujungimų ir informacijos perdavimo tikslais, apima duomenis apie fizinių asmenų privatų gyvenimą ir susiję su jų teise į susirašinėjimo slaptumą arba susiję su teisėtais juridinių asmenų interesais. Tokie

duomenys saugotini tiek, kiek jie reikalingi [paslaugai teikti,] sąskaitoms pateikti ir sumokėti už tinklų sujungimus, ir tik ribotą laiko tarpą. <…> [Bet koks kitas tokių duomenų tvarkymas] leidžiama[s] tik abonentui sutikus, kuris apsisprendžia, remdamasis tikslia ir išsamia informacija iš šio teikėjo apie numatomus duomenų tolimesnio tvarkymo būdus, apie abonento teisę nesutikti arba panaikinti duotą sutikimą tvarkyti tokius duomenis. <…> sunaikinami arba padaromi anoniminiais tokioms paslaugoms [ryšių paslaugoms rinkodaros tikslais] reikalingi srauto duomenys. <…>

<…>

(30) Elektroninių ryšių tinklų ir paslaugų teikimo sistemos turi būti suprojektuotos taip, kad reikalingas asmens duomenų kiekis būtų griežtai apribotas iki minimumo. <…>“

5 Direktyvos 2002/58 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 [Europos Sąjungoje], suderinimas.

2. Šios direktyvos nuostatos smulkiau išaiškina [patikslina] 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 Europos Sąjungos steigimo [Europos Sąjungos] 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.“

6 Šios direktyvos 2 straipsnyje „Sąvokų apibrėžimai“ nurodyta:

„Jeigu toliau nepateikta 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;

<…>“

7 Minėtos direktyvos 3 straipsnyje „Paslaugos“ numatyta:

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

8 Direktyvos 2002/58 5 straipsnyje „Pranešimų konfidencialumas“: numatyta:

„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 [asmenims, kurie nėra naudotojai] 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 [abonentas ar naudotojas, gavęs pagal Direktyvą [95/46] išsamią informaciją, *inter alia*, apie tokio duomenų tvarkymo tikslus, su tuo sutiko]. Ši nuostata nedraudžia vykdyti techninį saugojimą ar naudotis duomenimis, jei siekiama tik atlikti pranešimo perdavimą elektroninių ryšių tinklu, taip pat [arba] būtinais atvejais, kad informacinės visuomenės paslaugų teikėjas galėtų teikti paslaugas, kurių aiškiai paprašo abonentas ar naudotojas.“

9 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.“

10 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. <…>“

11 Minėtos direktyvos 15 straipsnio „Kai kurių Direktyvos [95/46] nuostatų taikymas“ 1 dalyje nustatyta:

„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 nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, 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 [teisėkūros] priemones, leidžiančias ribotą laikotarpį saugoti duomenis, remiantis šioje dalyje nustatytais motyvais. Visos šioje dalyje nurodytos priemonės turi atitikti bendruosius [Sąjungos] teisės principus, tarp jų ir nurodytus Europos Sąjungos Sutarties 6 straipsnio 1 ir 2 dalyse.“

Reglamentas 2016/679

12 Reglamento 2016/679 2 straipsnyje nustatyta:

„1. Šis reglamentas taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis.

2. Šis reglamentas netaikomas asmens duomenų tvarkymui, kai:

a) duomenys tvarkomi vykdant veiklą, kuriai Sąjungos teisė netaikoma;

b) duomenis tvarko valstybės narės, vykdydamos veiklą, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius;

<…>

d) duomenis tvarko kompetentingos valdžios institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už jas, baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais.

<…>“

13 Šio reglamento 4 straipsnyje numatyta:

„Šiame reglamente:

<…>

2) duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;

<…>“

14 To paties reglamento 23 straipsnio 1 dalyje nustatyta:

„Sąjungos ar valstybės narės teise, kuri taikoma duomenų valdytojui arba duomenų tvarkytojui, teisėkūros priemone gali būti apribotos 12–22 straipsniuose ir 34 straipsnyje, taip pat 5 straipsnyje tiek, kiek jo nuostatos atitinka 12–22 straipsniuose numatytas teises ir prievoles, nustatytos prievolės ir teisės, kai tokiu apribojimu gerbiama [paisoma] pagrindinių teisių ir laisvių esmė[s] ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

d) nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar patraukimą už jas baudžiamojon atsakomybėn arba bausmių vykdymą, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją;

e) kitus Sąjungos ar valstybės narės svarbius tikslus, susijusius su bendrais viešaisiais interesais, visų pirma svarbiu ekonominiu ar finansiniu Sąjungos ar valstybės narės interesu, įskaitant pinigų, biudžeto bei mokesčių klausimus, visuomenės sveikatą ir socialinę apsaugą;

f) teismų nepriklausomumo ir teismo procesų apsaugą;

g) reglamentuojamųjų profesijų etikos pažeidimų prevenciją, tyrimą, nustatymą ir patraukimą baudžiamojon atsakomybėn [atsakomybėn] už juos;

h) stebėsenos, tikrinimo ar reguliavimo funkciją, kuri (net jeigu tik kartais) yra susijusi su viešosios valdžios funkcijų vykdymu a–e ir g punktuose nurodytais atvejais;

i) duomenų subjekto apsaugą arba kitų asmenų teisių ir laisvių apsaugą;

j) civilinių ieškinių vykdymo užtikrinimą.“

15 Reglamento 2016/679 94 straipsnio 2 dalyje nustatyta:

„Nuorodos į panaikintą direktyvą laikomos nuorodomis į šį reglamentą. Nuorodos į Direktyvos [95/46] 29 straipsniu įsteigtą Darbo grupę asmenų apsaugai tvarkant asmens duomenis laikomos nuorodomis į šiuo reglamentu įsteigtą Europos duomenų apsaugos valdybą.“

Jungtinės Karalystės teisė

16 Pagrindinės bylos faktinėms aplinkybėms taikytinos redakcijos *Telecommunications Act 1984* (1984 m. Telekomunikacijų įstatymas, toliau – 1984 m. įstatymas) 94 straipsnyje „Nurodymai nacionalinio saugumo sumetimais ir kt.“ nustatyta:

„(1) Ministras, pasikonsultavęs su asmeniu, kuriam taikomas šis straipsnis, gali duoti šiam asmeniui bendro pobūdžio nurodymus, kurie, ministro nuomone, yra būtini siekiant užtikrinti nacionalinį saugumą arba santykius su už Jungtinės Karalystės ribų esančios šalies ar teritorijos vyriausybe.

(2) Jeigu ministrui atrodo, kad nacionalinio saugumo ar santykių su už Jungtinės Karalystės ribų esančios šalies ar teritorijos vyriausybės interesais tai yra būtina, jis, pasikonsultavęs su asmeniu, kuriam taikomas šis straipsnis, gali duoti nurodymus šiam asmeniui, prašydamas (atsižvelgiant į bylos aplinkybes) atlikti arba neatlikti tam tikrą nurodymuose minimą veiksmą.

(2a) Ministras gali duoti nurodymus pagal šio straipsnio (1) arba (2) dalį tik tuo atveju, jei mano, kad veiksmai, kurių reikalaujama pagal nurodymus, yra proporcingi tikslui, kuris turi būti pasiektas tokiu elgesiu.

(3) Asmuo, kuriam taikomas šis straipsnis, turi vykdyti visus ministro jam pagal šį straipsnį duotus nurodymus, nepaisydamas jokių kitų pareigų, jam tenkančių pagal *Communications Act 2003* (2003 m. Ryšių įstatymas, Jungtinė Karalystė) 1 skyriaus 1 ar 2 dalis, o kai nurodymai duoti viešųjų elektroninių ryšių tinklų teikėjui, – net jei tokie nurodymai jam taikomi dėl kitos priežasties nei kaip prieigos prie tokio tinklo teikėjui.

(4) Ministras pateikia abiem Parlamento rūmams visų pagal šį straipsnį duotų nurodymų kopiją, nebent mano, kad šių nurodymų atskleidimas prieštarautų nacionalinio saugumo ar santykių su už Jungtinės Karalystės ribų esančios šalies ar teritorijos vyriausybe interesams arba asmens komerciniams interesams.

(5) Asmuo neatskleidžia ir iš jo negali būti reikalaujama pagal įstatymą ar kitą aktą atskleisti informacijos apie priemones, kurių imtasi pagal šį straipsnį, jei ministras jam pranešė, kad šios informacijos atskleidimas prieštarautų nacionalinio saugumo ar santykių su už Jungtinės Karalystės ribų esančios šalies ar teritorijos vyriausybe interesams arba kito asmens komerciniams interesams.

<…>

(8) Šis straipsnis taikomas [Ryšių biurui (OFCOM)] ir viešųjų elektroninių ryšių tinklų teikėjams.“

17 *Regulation of Investigatory Powers Act 2000* (2000 m. Įstatymas dėl tyrimo įgaliojimų reglamentavimo, toliau – RIPA) 21 straipsnio 4 ir 6 dalyse nustatyta:

„(4) Šiame skyriuje „su pranešimais susiję duomenys“ – tai:

a) visi srauto duomenys, kurie (siuntėjo ar kitu būdu) pateikiami pranešime arba kaip pranešimo priedas, siekiant naudotis bet kuriomis pašto paslaugomis ar telekomunikacijų sistemomis, kurias pasitelkus šie duomenys yra ar gali būti perduodami;

b) bet kokia informacija, kuri neapima pranešimo turinio (išskyrus informaciją, patenkančią į a punkto taikymo sritį) ir yra susijusi su bet kurio asmens atliekamu naudojimusi:
   i) bet kokiomis pašto arba telekomunikacijų paslaugomis arba
   ii) bet kokia telekomunikacijų sistemos dalimi bet kuriam asmeniui teikiant telekomunikacijų paslaugas arba kai jomis naudojamasi;

c) bet kokia informacija, kuriai netaikomas a arba b punktas ir kurią turi arba gauna pašto arba telekomunikacijų paslaugas teikiantis asmuo, kiek tai susiję su asmenimis, kuriems tos paslaugos teikiamos.

<…>

(6) [S]ąvoka „srauto duomenys“, kiek tai susiję su bet kokiu pranešimu, apima:

a) visus duomenis, padedančius arba galinčius padėti nustatyti bet kurio asmens tapatybę, įrangą ar buvimo vietą, į kurią ar iš kurios yra arba gali būti perduotas pranešimas;

b) visus duomenis, padedančius arba galinčius padėti nustatyti ar atrinkti įrangą, kuria naudojantis yra arba gali būti perduotas pranešimas;

c) visus duomenis, apimančius įrangos, kuri ryšių sistemoje naudojama siekiant perduoti bet kokius pranešimus, įjungimo signalus, ir

d) visus duomenis, padedančius nustatyti konkrečiame pranešime arba šio pranešimo priede pateikiamus duomenis, arba kitus konkrečiame pranešime arba šio pranešimo priede pateikiamus duomenis.

<…>“

18 RIPA 65–69 straipsniuose nustatytos *Investigatory Powers Tribunal* (Bylų dėl tyrimų įgaliojimų teismas, Jungtinė Karalystė) veiklos ir jurisdikcijos taisyklės. Pagal šio įstatymo 65 straipsnį skundai šiam teismui gali būti pateikti, jei yra pagrindo manyti, kad duomenys buvo gauti netinkamai.

Pagrindinė byla ir prejudiciniai klausimai

19 2015 m. pradžioje apie įvairių Jungtinės Karalystės saugumo ir žvalgybos tarnybų, t. y. GCHQ, MI5 ir MI6, masinio ryšio duomenų rinkimo ir naudojimo praktiką buvo paskelbta, be kita ko, *Intelligence and Security Committee of Parliament* (Parlamento žvalgybos ir saugumo komitetas, Jungtinė Karalystė) ataskaitoje. 2015 m. birželio 5 d. *Investigatory Powers Tribunal* (Bylų dėl tyrimų įgaliojimų teismas) nevyriausybinė organizacija *Privacy International* pareiškė ieškinį užsienio reikalų ir tautų sandraugos ministrui, vidaus reikalų ministrui ir saugumo ir žvalgybos tarnyboms, ginčydama šios praktikos teisėtumą.

20 Prašymą priimti prejudicinį sprendimą pateikęs teismas išnagrinėjo šios praktikos teisėtumą, visų pirma atsižvelgdamas į vidaus teisę ir 1950 m. lapkričio 4 d. Romoje pasirašytos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – EŽTK) nuostatas, taip pat į Sąjungos teisę. 2016 m. spalio 17 d. sprendimu tas teismas konstatavo, kad atsakovai pagrindinėje byloje pripažino, jog minėtos saugumo ir žvalgybos tarnybos, vykdydamos savo veiklą, renka ir naudoja su fiziniais asmenimis susijusius duomenų rinkinius, priklausančius skirtingoms kategorijoms (*bulk personal data*), kaip antai biografinius ar su kelionėmis susijusius duomenis, finansinio ar komercinio pobūdžio duomenis, ryšio duomenis, galimai apimančius jautrius duomenis, kuriems taikoma profesinė paslaptis, arba žurnalistinę medžiagą. Šie įvairiais būdais, tam tikrais atvejais ir slaptais, gauti duomenys analizuojami juos sugrupuojant ir tvarkant automatizuotai ir gali būti atskleisti kitiems asmenims ir valdžios institucijoms, taip pat jais gali būti dalijamasi su užsienio partneriais. Saugumo ir žvalgybos tarnybos taip pat naudoja masinius ryšio duomenis, kurie yra renkami iš viešųjų elektroninių ryšių tinklų teikėjų, remiantis, be kita ko, ministro nurodymais, priimtais pagal 1984 m. įstatymo 94 straipsnį. GCHQ ir MI5 taip veikė atitinkamai nuo 2001 m. ir 2005 m.

21 Prašymą priimti prejudicinį sprendimą pateikęs teismas nusprendė, kad šios duomenų rinkimo ir naudojimo priemonės atitinka vidaus teisę, o nuo 2015 m. ir EŽTK 8 straipsnį, išskyrus dar nenagrinėtus klausimus, susijusius su šių priemonių proporcingumu ir duomenų perdavimu tretiesiems asmenims. Šiuo klausimu jis patikslino, kad jam buvo pateikti įrodymai dėl taikytinų garantijų, be kita ko, susiję su prieigos ir duomenų atskleidimo kitiems asmenims nei saugumo ir žvalgybos tarnybos procedūromis, duomenų saugojimo tvarka ir nepriklausomos kontrolės buvimu.

22 Dėl pagrindinėje byloje nagrinėjamų duomenų rinkimo ir naudojimo priemonių teisėtumo pagal Sąjungos teisę 2017 m. rugsėjo 8 d. sprendime prašymą priimti prejudicinį sprendimą pateikęs teismas nagrinėjo, ar šios priemonės patenka į Sąjungos teisės taikymo sritį, ir, jei taip, ar jos suderinamos su šia teise. Dėl masinių ryšio duomenų šis teismas konstatavo, kad pagal 1984 m. įstatymo 94 straipsnį tuo atveju, kai ministras duoda atitinkamus nurodymus, elektroninių ryšių tinklų teikėjai, vykdydami savo ekonominę veiklą, kuriai taikoma Sąjungos teisė, privalo pateikti saugumo ir žvalgybos tarnyboms surinktus duomenis. Vis dėlto taip nėra renkant kitus duomenis, kuriuos šios tarnybos renka nesinaudodamos tokiais privalomojo pobūdžio įgaliojimais. Remdamasis šia išvada tas teismas nusprendė, jog būtina kreiptis į Teisingumo Teismą, kad būtų nustatyta, ar tvarka, išplaukianti iš šio 94 straipsnio, patenka į Sąjungos teisės taikymo sritį, ir, jei taip, ar šiai tvarkai taikomi 2016 m. gruodžio 21 d. Sprendimu *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970, toliau – Sprendimas *Tele2*,) suformuotoje jurisprudencijoje nustatyti reikalavimai ir kokiu būdu.

23 Šiuo klausimu savo prašyme priimti prejudicinį sprendimą nacionalinis teismas nurodo, kad pagal minėtą 94 straipsnį ministras gali elektroninių ryšių paslaugų teikėjams duoti bendrus ar specialius nurodymus, kurie, jo manymu, yra būtini nacionaliniam saugumui ar santykiams su užsienio vyriausybe. Nurodydamas RIPA 21 straipsnio 4 ir 6 dalyse pateiktas apibrėžtis, tas teismas patikslina, kad atitinkami duomenys apima srauto duomenis ir informaciją apie naudojamas paslaugas, kaip tai suprantama pagal šią nuostatą, tik pranešimų turinys nepatenka į tokių duomenų apibrėžtį. Šie duomenys ir informacija, be kita ko, leidžia sužinoti su pranešimu susijusią informaciją „kas, kur, kada ir kaip“. Šie duomenys perduodami saugumo ir žvalgybos tarnyboms, kurios juos saugo savo veiklos tikslais.

24 Minėto teismo teigimu, pagrindinėje byloje nagrinėjama tvarka skiriasi nuo tvarkos, nustatytos *Data Retention and Investigatory Powers Act 2014* (2014 m. Duomenų saugojimo ir tyrimo įgaliojimų įstatymas, Jungtinė Karalystė), kuri buvo nagrinėjama byloje, kurioje priimtas 2016 m. gruodžio 21 d. Sprendimas *Tele2* (C-203/15 ir C-698/15, EU:C:2016:970), nes pagal pastarąją tvarką buvo numatyta, kad duomenis saugo elektroninių ryšių paslaugų teikėjai ir kad jie yra perduodami ne tik saugumo ir žvalgybos tarnyboms, siekiant užtikrinti nacionalinį saugumą, bet ir kitoms valdžios institucijoms, atsižvelgiant į jų poreikius. Be to, minėtas sprendimas susijęs su baudžiamuoju tyrimu, o ne su nacionaliniu saugumu.

25 Prašymą priimti prejudicinį sprendimą pateikęs teismas priduria, kad saugumo ir žvalgybos tarnybų sudarytos duomenų bazės tvarkomos masiškai, automatizuotai ir nespecifiškai, siekiant atskleisti galimas nežinomas grėsmes. Šiuo tikslu prašymą priimti prejudicinį sprendimą pateikęs teismas nurodo, kad taip sudarytų metaduomenų rinkiniai turėtų būti kuo išsamesni, kad „šieno kupetoje“ būtų galima rasti „adatą“, kuri ten slepiasi. Kiek tai susiję su minėtų tarnybų masinio duomenų rinkimo naudingumu ir prieigos prie šių duomenų būdais, minėtas teismas visų pirma remiasi 2016 m. rugpjūčio 19 d. *QC* David Anderson, kuris tuo metu buvo *United Kingdom Independent Reviewer of Terrorism Legislation* (Nepriklausomas Jungtinės Karalystės su terorizmu susijusių teisės aktų prižiūrėtojas), parengtos ataskaitos išvadomis; rengdamas šią ataskaitą jis rėmėsi žvalgybos specialistų grupės atliktu tyrimu ir saugumo bei žvalgybos tarnybų darbuotojų parodymais.

26 Prašymą priimti prejudicinį sprendimą pateikęs teismas taip pat patikslina, kad, *Privacy International* teigimu, pagrindinėje byloje nagrinėjama tvarka yra neteisėta pagal Sąjungos teisę, o atsakovai pagrindinėje byloje mano, kad pagal šią tvarką numatyta pareiga perduoti duomenis, prieiga prie šių duomenų ir jų naudojimas nepriklauso Sąjungos kompetencijai, visų pirma remiantis ESS 4 straipsnio 2 dalimi, pagal kurią kiekviena valstybė narė išlieka atsakinga už savo nacionalinį saugumą.

27 Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas, remdamasis 2006 m. gegužės 30 d. Sprendimu *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346, 56–59 punktai), susijusiu su PNR *(Passenger Name Record)* duomenų perdavimu visuomenės saugumo užtikrinimo tikslais, teigia, kad neatrodo, jog komercinių bendrovių veikla, tvarkant ir perduodant duomenis nacionalinio saugumo užtikrinimo tikslu, patenka į Sąjungos teisės taikymo sritį. Reikėtų išnagrinėti ne tai, ar nagrinėjama veikla yra duomenų tvarkymas, o tik tai, ar tokios veiklos esmė ir poveikis yra palaikyti esminę valstybės funkciją, kaip tai suprantama pagal ESS 4 straipsnio 2 dalį, taikant viešosios valdžios institucijų nustatytą visuomenės saugumo sistemą.

28 Tuo atveju, jei pagrindinėje byloje nagrinėjamos priemonės vis dėlto patektų į Sąjungos teisės taikymo sritį, prašymą priimti prejudicinį sprendimą pateikęs teismas teigia, kad 2016 m. gruodžio 21 d. Sprendimo *Tele2* (C-203/15 ir C-698/15, EU:C:2016:970) 119–125 punktuose nustatyti reikalavimai yra netinkami nacionalinio saugumo sričiai ir gali trukdyti saugumo ir žvalgybos tarnybų galimybei valdyti tam tikrą grėsmę nacionaliniam saugumui.

29 Šiomis aplinkybėmis *Investigatory Powers Tribunal* (Bylų dėl tyrimų įgaliojimų teismas) nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„Ar tokiomis aplinkybėmis, kai:

a) [saugumo ir žvalgybos tarnybų] galimybės naudoti joms pateikiamus [masinius ryšio duomenis] yra labai svarbios Jungtinės Karalystės nacionaliniam saugumui, įskaitant kovos su terorizmu, šnipinėjimu ir branduolinių ginklų platinimu sritis, užtikrinti;

b) iš esmės [saugumo ir žvalgybos tarnyboms] naudojant [masinius ryšio duomenis] siekiama atskleisti dar nežinomas grėsmes nacionaliniam saugumui, taikant netikslinius masinius metodus, pagrįstus [masinių ryšio duomenų] surinkimu į vieną vietą. Jų pagrindinė nauda yra ta, kad greitai nustatomas taikinys ir vykdomi parengiamieji darbai, taip pat suteikiamas pagrindas imtis veiksmų kilus neišvengiamai grėsmei;

c) elektroninių ryšių tinklų paslaugų teikėjai neprivalo saugoti [masinių ryšio] duomenų (ilgiau, nei to reikalaujama pagal įprastas veiklos taisykles), juos saugo tik valstybė ([saugumo ir žvalgybos tarnybos]);

d) nacionalinis teismas nustatė (išskyrus kai kuriuos nenagrinėtus klausimus), kad garantijos, susijusios su tuo, kaip [saugumo ir žvalgybos tarnybos] naudoja [masinius ryšio duomenis], atitinka EŽTK reikalavimus;

e) nacionalinis teismas pripažino, kad [2016 m. gruodžio 21 d. Sprendimo *Tele2* (C-203/15 ir C-698/15, EU:C:2016:970)] 119–125 punktuose sukonkretintų reikalavimų, jeigu jie būtų taikomi, nustatymas pakenktų priemonėms, kurių saugumo ir žvalgybos tarnybos ėmėsi nacionaliniam saugumui užtikrinti, ir taip kiltų grėsmė Jungtinės Karalystės nacionaliniam saugumui:

1. Ar, atsižvelgiant į ESS 4 straipsnį ir Direktyvos [2002/58] 1 straipsnio 3 dalį, ministro elektroninių ryšių tinklo teikėjui pateiktuose nurodymuose esantis įpareigojimas, kuriuo remdamasis jis turi teikti masinius ryšio duomenis valstybės narės saugumo ir žvalgybos tarnyboms, patenka į Sąjungos teisės ir Direktyvos [2002/58] taikymo sritį?

2. Jei atsakymas į pirmąjį klausimą yra teigiamas, ar tokiems ministro nurodymams taikomas kuris nors iš [2016 m. gruodžio 21 d. Sprendimo *Tele2* (C-203/15 ir C-698/15, EU:C:2016:970) 119–125 punktuose nurodytų reikalavimų, galiojančių saugomiems ryšių duomenims] arba bet kokie kiti reikalavimai, be nustatytųjų EŽTK? Jei taip, kaip ir kiek šie reikalavimai taikomi, atsižvelgiant į esminį saugumo ir žvalgybos tarnybų poreikį naudoti masinio duomenų gavimo ir automatizuoto tvarkymo metodus, norint apsaugoti nacionalinį saugumą, ir kiek tokioms galimybėms, jeigu jos atitinka EŽTK, galima iš esmės sukliudyti nustatant tokius reikalavimus?“

Dėl prejudicinių klausimų

Dėl pirmojo klausimo

30 Pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 2002/58 1 straipsnio 3 dalis, siejama su ESS 4 straipsnio 2 dalimi, turi būti aiškinama taip, kad į šios direktyvos taikymo sritį patenka nacionalinės teisės aktai, pagal kuriuos valstybės institucija gali įpareigoti elektroninių ryšių paslaugų teikėjus perduoti saugumo ir žvalgybos tarnyboms srauto ir vietos nustatymo duomenis, kad būtų užtikrintas nacionalinis saugumas.

31 Šiuo klausimu *Privacy International* iš esmės teigia, kad, atsižvelgiant į Teisingumo Teismo jurisprudencijoje suformuotas išvadas dėl Direktyvos 2002/58 taikymo srities, tiek saugumo ir žvalgybos tarnybų atliekamas duomenų rinkimas iš šių paslaugų teikėjų pagal 1984 m. įstatymo 94 straipsnį, tiek šių tarnybų atliekamas tokių duomenų naudojimas patenka į šios direktyvos taikymo sritį, neatsižvelgiant į tai, ar šie duomenys renkami juos perduodant realiuoju laiku, ar ne. Konkrečiai kalbant, tai, kad nacionalinio saugumo užtikrinimo tikslas aiškiai nurodytas minėtos direktyvos 15 straipsnio 1 dalyje, nereiškia, kad ši direktyva netaikoma tokioms situacijoms, o ESS 4 straipsnio 2 dalis neturi įtakos šiam vertinimui.

32 Priešingai, Jungtinės Karalystės, Čekijos ir Estijos vyriausybės, Airija, Prancūzijos, Kipro, Vengrijos, Lenkijos ir Švedijos vyriausybės iš esmės teigia, kad Direktyva 2002/58 netaikytina pagrindinėje byloje nagrinėjamiems nacionalinės teisės aktams, nes jais siekiama užtikrinti nacionalinį saugumą. Saugumo ir žvalgybos tarnybų veikla priskirtina prie esminių valstybių narių funkcijų, susijusių su viešosios tvarkos palaikymu ir vidaus saugumo bei teritorinio vientisumo užtikrinimu, todėl ši veikla priklauso išimtinei valstybių narių kompetencijai, kaip tai matyti, be kita ko, iš ESS 4 straipsnio 2 dalies trečio sakinio.

33 Taigi šių vyriausybių teigimu, Direktyva 2002/58 negali būti aiškinama taip, kad nacionalinės priemonės, skirtos nacionaliniam saugumui užtikrinti, patenka į jos taikymo sritį. Šios direktyvos 1 straipsnio 3 dalyje ši taikymo sritis apribojama ir, kaip jau buvo numatyta Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje, į ją nepatenka su visuomenės saugumu, gynyba ir valstybės saugumu susijusios veiklos rūšys. Šios nuostatos atspindi ESS 4 straipsnio 2 dalyje numatytą kompetencijos pasidalijimą ir būtų neveiksmingos, jei nacionalinio saugumo sričiai priklausančioms priemonėms būtų taikomi Direktyvos 2002/58 reikalavimai. Be to, Teisingumo Teismo jurisprudencija, suformuota 2006 m. gegužės 30 d. Sprendime *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346) dėl Direktyvos 95/46 3 straipsnio 2 dalies pirmos įtraukos, taikytina ir Direktyvos 2002/58 1 straipsnio 3 daliai.

34 Reikia pažymėti, kad Direktyvos 2002/58 1 straipsnio 1 dalyje nurodyta, kad šioje direktyvoje, be kita ko, numatytas valstybių narių nuostatų, užtikrinančių vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatų gyvenimą ir konfidencialumą, apsaugą, kiek tai susiję su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, suderinimas.

35 Šios direktyvos 1 straipsnio 3 dalyje numatyta, kad ji netaikoma „valstybės veiksmams“ joje nurodytose srityse, įskaitant valstybės veiksmus baudžiamosios teisės srityje ir veiksmus, susijusius su visuomenės saugumu, gynyba, valstybės saugumu, įskaitant valstybės ekonominę gerovę, kai atitinkami veiksmai susiję su valstybės saugumo klausimais. Kaip pavyzdžiai nurodyta veikla visais atvejais yra pačių valstybių ar valstybės valdžios institucijų veikla, kuri nėra privačių asmenų veikla (2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 32 punktas ir jame nurodyta jurisprudencija).

36 Be to, Direktyvos 2002/58 3 straipsnyje numatyta, kad ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su visuomenei prieinamų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais Sąjungoje, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius (toliau – elektroninių ryšių paslaugos). Taigi, reikia manyti, kad ši direktyva reglamentuoja tokių paslaugų teikėjų veiklą (2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 33 punktas ir jame nurodyta jurisprudencija).

37 Esant šioms aplinkybėms, pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybėms narėms leidžiama, laikantis joje nustatytų sąlygų, patvirtinti „[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“ (2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 71 punktas).

38 Direktyvos 2002/58 15 straipsnio 1 dalis neišvengiamai paremta prielaida, kad joje numatytos nacionalinės teisėkūros priemonės patenka į jos taikymo sritį, nes joje aiškiai nustatyta, kad valstybės narės gali jas patvirtinti, tik jeigu laikosi joje numatytų sąlygų. Be to, tokiomis priemonėmis šioje nuostatoje nurodytais tikslais reglamentuojama elektroninių ryšių paslaugų teikėjų veikla (2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 34 punktas ir jame nurodyta jurisprudencija).

39 Būtent atsižvelgdamas į šiuos argumentus Teisingumo Teismas nusprendė, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su jos 3 straipsniu, turi būti aiškinama taip, kad į šios direktyvos taikymo sritį patenka ne tik teisėkūros priemonė, kuria elektroninių ryšių paslaugų teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis, bet ir teisėkūros priemonė, pagal kurią jie įpareigojami kompetentingoms nacionalinėms institucijoms suteikti prieigą prie šių duomenų. Iš tiesų tokios teisėkūros priemonės neišvengiamai reiškia, kad minėti paslaugų teikėjai tvarko minėtus duomenis, ir jų negalima, kiek jomis reglamentuojama tų pačių teikėjų veikla, prilyginti pačių valstybių veiklai, numatytai minėtos direktyvos 1 straipsnio 3 dalyje (šiuo klausimu žr. 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 35 ir 37 punktus ir juose nurodytą jurisprudenciją).

40 Kalbant apie teisinę priemonę, kaip antai 1984 m. įstatymo 94 straipsnį, kuria remdamasi kompetentinga institucija gali elektroninių ryšių paslaugų teikėjams nurodyti perduoti masinius duomenis saugumo ir žvalgybos tarnyboms, reikia pažymėti, kad pagal Reglamento 2016/679 4 straipsnio 2 punkte pateiktą apibrėžtį, kuri yra taikytina pagal Direktyvos 2002/58 2 straipsnį, siejamą su šio reglamento 94 straipsnio 2 dalimi, sąvoka „asmens duomenų tvarkymas“ apima „bet kokią automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekamą operaciją ar operacijų seką, kaip antai rinkimą, <…>, saugojimą <…>, susipažinimą, naudojimą, atskleidimą persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis <…>“.

41 Iš to matyti, kad asmens duomenų atskleidimas perduodant, taip pat duomenų saugojimas arba bet kokia kita jų suteikimo naudotis forma yra duomenų tvarkymas, kaip tai suprantama pagal Direktyvos 2002/58 3 straipsnį, todėl patenka į šios direktyvos taikymo sritį (šiuo klausimu žr. 2008 m. sausio 29 d. Sprendimo *Promusicae*, C-275/06, EU:C:2008:54, 45 punktą).

42 Be to, atsižvelgiant į tai, kas išdėstyta šio sprendimo 38 punkte, ir į Direktyvos 2002/58 bendrą struktūrą, šios direktyvos aiškinimas, pagal kurį jos 15 straipsnio 1 dalyje nurodytos teisėkūros priemonės nepatenka į šios direktyvos taikymo sritį, nes tikslai, kuriems turi būti taikomos tokios priemonės, iš esmės sutampa su tikslais, kurių siekiama tos pačios direktyvos 1 straipsnio 3 dalyje nurodyta veikla, panaikintų bet kokį šios direktyvos 15 straipsnio 1 dalies veiksmingumą (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 72 ir 73 punktus).

43 Taigi Direktyvos 2002/58 1 straipsnio 3 dalyje vartojama sąvoka „veiklos rūšys“, kaip iš esmės pažymėjo generalinis advokatas savo išvados sujungtose bylose *La Quadrature du Net ir kt.* (C-511/18 ir C-512/18, EU:C:2020:6) 75 punkte, kurį jis nurodė savo išvados šioje byloje 24 punkte, neturi būti aiškinama kaip apimanti šios direktyvos 15 straipsnio 1 dalyje nurodytas teisėkūros priemones.

44 Šios išvados negali paneigti ESS 4 straipsnio 2 dalies nuostatos, kuriomis remiasi šio sprendimo 32 punkte minėtos vyriausybės. Remiantis Teisingumo Teismo suformuota jurisprudencija, nors valstybės narės turi nustatyti savo esminius saugumo interesus ir imtis priemonių vidaus ir išorės saugumui užtikrinti, tik ta aplinkybė, kad buvo imtasi nacionalinės priemonės, siekiant užtikrinti nacionalinį saugumą, nereiškia, jog Sąjungos teisė netaikoma ir kad valstybės narės neturi jos laikytis, kaip reikalaujama (šiuo klausimu žr. 2013 m. birželio 4 d. Sprendimo *ZZ* C-300/11, EU:C:2013:363, 38 punktą ir jame nurodytą jurisprudenciją; 2018 m. kovo 20 d. Sprendimo *Komisija / Austrija (Valstybinė spaustuvė)*, C-187/16, EU:C:2018:194, 75 ir 76 punktus; taip pat 2020 m. balandžio 2 d. Sprendimo *Komisija / Lenkija, Vengrija ir Čekijos Respublika (Laikinas tarptautinės apsaugos prašytojų perkėlimo mechanizmas)*, C-715/17, C-718/17 ir C-719/17, EU:C:2020:257, 143 ir 170 punktus).

45 Tiesa, kad 2006 m. gegužės 30 d. Sprendime *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346, 56–59 punktai) Teisingumo Teismas nusprendė, kad oro transporto bendrovių atliekamas asmens duomenų perdavimas trečiosios valstybės valdžios institucijoms, siekiant užkirsti kelią terorizmui ir kitoms sunkioms nusikalstamoms veikoms, remiantis Direktyvos 95/46 3 straipsnio 2 dalies pirma įtrauka, nepatenka į šios direktyvos taikymo sritį, nes šis perdavimas patenka į viešosios valdžios institucijų nustatytą sritį, susijusią su visuomenės saugumu.

46 Vis dėlto atsižvelgiant į šio sprendimo 36, 38 ir 39 punktuose nurodytus argumentus, šios jurisprudencijos negalima taikyti aiškinant Direktyvos 2002/58 1 straipsnio 3 dalį. Kaip iš esmės savo išvados sujungtose bylose *La Quadrature du Net ir kt.* (C-511/18 ir C-512/18, EU:C:2020:6) 70–72 punktuose nurodė generalinis advokatas, remiantis Direktyvos 95/46 3 straipsnio 2 dalies pirma įtrauka, su kuria susijusi minėta jurisprudencija, šios direktyvos taikymo sritis apskritai neapima „tvarkymo operacij[ų], susijusi[ų] su visuomenės saugumu, gynyba, valstybės saugumu“, neatsižvelgiant į tai, kas yra atitinkamų duomenų tvarkymo autorius. Tačiau aiškinant Direktyvos 2002/58 1 straipsnio 3 dalį atsižvelgti į tokį diferencijavimą būtina. Iš tiesų, kaip matyti iš šio sprendimo 37–39 ir 42 punktų, bet koks elektroninių ryšių paslaugų teikėjų atliekamas asmens duomenų tvarkymas patenka į šios direktyvos taikymo sritį, įskaitant tvarkymą, kylantį iš valstybės valdžios institucijų jiems nustatytų įpareigojimų, nors tokiam tvarkymui prireikus gali būti taikoma Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje numatyta išimtis, atsižvelgiant į platesnę šios nuostatos formuluotę, apimančią bet kokį tvarkymą, nepriklausomai nuo autoriaus, kurio tikslas visuomenės saugumas, gynyba arba valstybės saugumas.

47 Be to, reikia pažymėti, kad Direktyva 95/46, nagrinėta byloje, kurioje priimtas 2006 m. gegužės 30 d. Sprendimas *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346), pagal Reglamento 2016/679 94 straipsnio 1 dalį nuo 2018 m. gegužės 25 d. buvo panaikinta ir pakeista šiuo reglamentu. Nors minėto reglamento 2 straipsnio 2 dalies d punkte nurodyta, kad jis netaikomas, kai duomenis tvarko „kompetentingos valdžios institucijos“, siekdamos užkirsti kelią nusikalstamoms veikoms ir jas nustatyti, įskaitant apsaugą nuo grėsmės visuomenės saugumui ir tokios grėsmės prevenciją, iš to paties reglamento 23 straipsnio 1 dalies d ir h punktų matyti, kad asmens duomenų tvarkymas, kurį tuo pačiu tikslu atlieka privatūs asmenys, patenka į šio reglamento taikymo sritį.

Darytina išvada, kad prieš tai pateiktas Direktyvos 2002/58 1 straipsnio 3 dalies, 3 straipsnio ir 15 straipsnio 1 dalies aiškinimas atitinka Reglamento 2016/679 taikymo srities apibrėžimą, kurį papildo ir patikslina ši direktyva.

48 Vis dėlto kai valstybės narės tiesiogiai įgyvendina priemones, nukrypstančias nuo elektroninių ryšių konfidencialumo, nenustatydamos tokių ryšių paslaugų teikėjams pareigos tvarkyti duomenis, duomenų subjektų duomenų apsaugai taikoma ne Direktyva 2002/58, o tik nacionalinė teisė, išskyrus atvejus, kai taikoma 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89; klaidų ištaisymas OL L 127, 2018, p. 6), todėl nagrinėjamos priemonės turi visų pirma atitikti konstitucinio lygio nacionalinę teisę ir EŽTK reikalavimus.

49 Atsižvelgiant į tai, kas išdėstyta, į pirmąjį klausimą reikia atsakyti, kad Direktyvos 2002/58 1 straipsnio 3 dalį, 3 straipsnį ir 15 straipsnio 1 dalį, siejamus su ESS 4 straipsnio 2 dalimi, reikia aiškinti taip, kad į šios direktyvos taikymo sritį patenka nacionalinės teisės aktai, pagal kuriuos valstybės institucija gali įpareigoti elektroninių ryšių paslaugų teikėjus perduoti saugumo ir žvalgybos tarnyboms srauto ir vietos nustatymo duomenis, kad būtų užtikrintas nacionalinis saugumas.

Dėl antrojo klausimo

50 Antruoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su ESS 4 straipsnio 2 dalimi bei Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, kuriais valstybės institucija, siekdama užtikrinti nacionalinį saugumą, gali įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant perduoti srauto ir vietos nustatymo duomenis saugumo ir žvalgybos tarnyboms.

51 Pirmiausia reikia priminti, kad, remiantis prašyme priimti prejudicinį sprendimą pateikta informacija, pagal 1984 m. įstatymo 94 straipsnį ministrui leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus, jeigu jis mano, kad tai būtina nacionaliniam saugumui ar santykiams su užsienio vyriausybe, perduoti saugumo ir žvalgybos tarnyboms masinius ryšio duomenis, įskaitant srauto ir vietos nustatymo duomenis bei informaciją apie naudotas paslaugas, kaip tai suprantama pagal RIPA 21 straipsnio 4 ir 6 dalis. Ši nuostata, be kita ko, apima duomenis, reikalingus ryšio šaltiniui ir paskirčiai, pranešimo datai, laikui, trukmei ir tipui nustatyti, naudojamai įrangai identifikuoti, taip pat nustatyti galinių įrenginių ir ryšių vietą, tarp kurių, be kita ko, yra naudotojo asmenvardis ir adresas, telefono numeris, skambinančiojo telefono numeris, ryšio šaltinio ir gavėjo IP adresai ir aplankytų interneto svetainių adresai.

52 Toks duomenų atskleidimas juos perduodant susijęs su visais elektroninių ryšių priemonių naudotojais, nepatikslinant, ar toks perdavimas turi vykti realiuoju laiku, ar ne. Perdavus šiuos duomenis, remiantis prašyme priimti prejudicinį sprendimą pateikta informacija, saugumo ir žvalgybos tarnybos saugo juos ir gali jais naudotis savo veiklos tikslais, kaip ir kitomis šių tarnybų turimomis duomenų bazėmis. Konkrečiai kalbant, taip surinkti duomenys, kurie yra masiškai bei automatizuotai tvarkomi ir tiriami, gali būti sujungiami su kitomis duomenų bazėmis, kuriose saugomi įvairių kategorijų masiniai duomenys, arba jie gali būti atskleidžiami kitiems asmenims nei šios tarnybos ir perduodami į trečiąsias šalis. Galiausiai tokiems tarnybų veiksmams neturi būti duotas išankstinis teismo ar nepriklausomos administracinės institucijos leidimas ir apie juos nėra informuojami duomenų subjektai.

53 Direktyva 2002/58, 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 naujųjų technologijų ir ypač dėl didėjančių automatizuoto duomenų kaupimo ir

tvarkymo pajėgumų. Visų pirma minėta direktyva, kaip nurodyta jos 2 konstatuojamojoje dalyje, siekiama užtikrinti visapusišką pagarbą Chartijos 7 ir 8 straipsniuose išdėstytoms teisėms. Šiuo klausimu pažymėtina, kad 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“.

54 Šiuo tikslu Direktyvos 2002/58 5 straipsnio 1 dalyje nurodyta, kad „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“. Šioje nuostatoje taip pat pabrėžiama, kad „[v]isų pirma [valstybės narės] draudžia [asmenims, kurie nėra naudotojai] 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“, taip pat nurodoma, kad „[š]ios dalies nuostatos nedraudžia techninio saugojimo, būtino perduoti pranešim[ui] nepažeidžiant konfidencialumo principo“.

55 Taigi šioje 5 straipsnio 1 dalyje įtvirtintas tiek elektroninių pranešimų, tiek su jais susijusių srauto duomenų konfidencialumo principas, be kita ko, reiškia, kad iš principo bet kuriam kitam asmeniui nei naudotojai, draudžiama saugoti šiuos pranešimus ir duomenis be jų sutikimo. Atsižvelgiant į bendrą šios nuostatos formuluotę, ji neišvengiamai apima bet kokią operaciją, leidžiančią tretiesiems asmenims susipažinti su pranešimais ir su jais susijusiais duomenimis kitais nei pranešimo pristatymo tikslais.

56 Taigi Direktyvos 2002/58 5 straipsnio 1 dalyje įtvirtintas draudimas perimti pranešimus ir su jais susijusius duomenis apima bet kokį elektroninių ryšių paslaugų teikėjų atliekamą srauto ir vietos nustatymo duomenų pateikimą valdžios institucijoms, kaip antai saugumo ir žvalgybos tarnyboms, ir šių institucijų atliekamą šių duomenų saugojimą, neatsižvelgiant į tai, kaip jie bus naudojami vėliau.

57 Taigi priimdamas šią direktyvą Sąjungos teisės aktų leidėjas sukonkretino Chartijos 7 ir 8 straipsniuose įtvirtintas teises taip, kad elektroninių ryšių priemonių naudotojai iš esmės turi teisę tikėtis, jog be jų sutikimo jų pranešimai ir su jais susiję duomenys išliks anonimiški ir negalės būti registruojami (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, 109 punktas).

58 Vis dėlto pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybėms narėms leidžiama nustatyti šios direktyvos 5 straipsnio 1 dalyje įtvirtintos pagrindinės pareigos užtikrinti asmens duomenų konfidencialumą ir susijusių pareigų, nurodytų, be kita ko, šios direktyvos 6 ir 9 straipsniuose, išimtis, jeigu toks ribojimas yra demokratinėje visuomenėje būtina, tinkama ir proporcinga priemonė, skirta apsaugoti nacionaliniam ir visuomenės saugumui bei gynybai arba užtikrinti nusikalstamų veikų ar neteisėto elektroninių ryšių sistemos naudojimo prevencijai, tyrimui, atskleidimui ar baudžiamajam persekiojimui už jas. Šiuo tikslu valstybės narės gali, *inter alia*, patvirtinti teisėkūros priemones, leidžiančias ribotą laikotarpį saugoti duomenis, kai tai pateisinama viena iš nurodytų priežasčių.

59 Atsižvelgiant į tai, galimybė nukrypti nuo Direktyvos 2002/58 5, 6 ir 9 straipsniuose numatytų teisių ir pareigų negali pateisinti to, kad pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą ir ypač šios direktyvos 5 straipsnyje aiškiai numatyto draudimo saugoti šiuos duomenis išimtis taptų taisykle (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 89 ir 104 punktus; taip pat 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, 111 punktą).

60 Be to, iš Direktyvos 2002/58 15 straipsnio 1 dalies trečio sakinio matyti, kad valstybėms narėms leidžiama imtis teisėkūros priemonių, kuriomis siekiama apriboti šios direktyvos 5, 6 ir 9 straipsniuose nurodytų teisių ir pareigų apimtį, tik laikantis bendrųjų Sąjungos teisės principų, įskaitant

proporcingumo principą, ir Chartijoje garantuojamų pagrindinių teisių. Šiuo klausimu Teisingumo Teismas jau yra nusprendęs, kad elektroninių ryšių paslaugų teikėjams valstybės narės nacionalinės teisės aktuose nustatyta pareiga saugoti srauto duomenis, kad prireikus jie būtų prieinami kompetentingoms nacionalinėms institucijoms, kelia klausimų ne tik dėl Chartijos 7 ir 8 straipsnių, susijusių atitinkamai su privataus gyvenimo ir asmens duomenų apsaugos užtikrinimu, bet ir dėl Chartijos 11 straipsnyje garantuojamos saviraiškos laisvės paisymo (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 25 ir 70 punktus; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 91 ir 92 punktus bei juose nurodytą jurisprudenciją).

61 Tokie pat klausimai kyla dėl kitų rūšių duomenų tvarkymo, kaip antai dėl jų perdavimo kitiems asmenims nei naudotojai arba dėl prieigos prie šių duomenų naudojimo tikslais (pagal analogiją žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 122 ir 123 punktus ir juose nurodytą jurisprudenciją).

62 Taigi, aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį, reikia atsižvelgti tiek į Chartijos 7 straipsnyje įtvirtintos teisės į privataus gyvenimą gerbimą, tiek į jos 8 straipsnyje įtvirtintos teisės į asmens duomenų apsaugą svarbą, kaip matyti iš Teisingumo Teismo jurisprudencijos, taip pat į saviraiškos laisvę, t. y. Chartijos 11 straipsnyje garantuojamą pagrindinę teisę, kuri yra vienas iš pagrindinių demokratinės ir pliuralistinės visuomenės pagrindų – vertybių, kuriomis pagal ESS 2 straipsnį grindžiama Sąjunga, dalis (šiuo klausimu žr. 2001 m. kovo 6 d. Sprendimo *Connolly / Komisija*, C-274/99 P, EU:C:2001:127, 39 punktą; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 93 punktą ir jame nurodytą jurisprudenciją).

63 Vis dėlto Chartijos 7, 8 ir 11 straipsniuose įtvirtintos teisės nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų visuomeninę paskirtį (šiuo klausimu žr. 2020 m. liepos 16 d. Sprendimo *Facebook Ireland ir Schrems*, C-311/18, EU:C:2020:559, 172 punktą ir jame nurodytą jurisprudenciją).

64 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 bendruosius interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

65 Reikia pridurti, jog reikalavimas, kad visi šios teisės įgyvendinimo apribojimai būtų numatyti įstatyme, reiškia, kad pačiame teisiniame pagrinde, kuriuo leidžiamas šių teisių suvaržymas, turi būti apibrėžta atitinkamos teisės įgyvendinimo apribojimo apimtis (2020 m. liepos 16 d. Sprendimo *Facebook Ireland ir Schrems*, C-311/18, EU:C:2020:559, 175 punktas).

66 Dėl proporcingumo principo paisymo reikia pabrėžti, kad Direktyvos 2002/58 15 straipsnio 1 dalies pirmame sakinyje numatyta, kad valstybės narės gali nustatyti nuo pranešimų ir su jais susijusių srauto duomenų konfidencialumo pareigos nukrypstančią priemonę, kai ji yra „būtina, tinkama ir adekvati [proporcinga] demokratinė[je] visuomenė[je]“ atsižvelgiant į šia nuostata siekiamus tikslus. Minėtos direktyvos 11 konstatuojamojoje dalyje patikslinama, kad tokio pobūdžio priemonė turi „griežtai“ atitikti siekiamą tikslą.

67 Šiuo klausimu reikia priminti, kad pagrindinės teisės į privataus gyvenimo gerbimą apsauga reikalauja, remiantis suformuota Teisingumo Teismo jurisprudencija, 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 (šiuo klausimu žr. 2008 m. gruodžio 16 d. Sprendimo *Satakunnan Markkinapörssi ir Satamedia*, C-73/07, EU:C:2008:727, 56 punktą; 2010 m. lapkričio 9 d. Sprendimo *Volker und*

Markus Schecke ir Eifert, C-92/09 ir C-93/09, EU:C:2010:662, 76, 77 ir 86 punktus; 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 52 punktą ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 140 punktą).

68 Tam, kad atitiktų proporcingumo reikalavimą, 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, visų pirma juose turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis gali būti imtasi tokios 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, kokią sudaro jautrūs duomenys, apsaugos klausimu (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 54 ir 55 punktus; 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 117 punktą ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 141 punktą).

69 Dėl klausimo, ar nacionalinės teisės aktai, kaip antai nagrinėjami pagrindinėje byloje, atitinka Direktyvos 2002/58 15 straipsnio 1 dalies, siejamos su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, reikalavimus, reikia pažymėti, kad perduodant srauto ir vietos nustatymo duomenis kitiems asmenims nei naudotojai, kaip antai saugumo ir žvalgybos tarnyboms, nukrypstama nuo konfidencialumo principo. Kadangi ši operacija vykdoma, kaip šiuo atveju, bendrai ir nediferencijuotai, nukrypimas nuo pagrindinės pareigos užtikrinti duomenų konfidencialumą tampa taisykle, nors pagal Direktyva 2002/58 nustatytą sistemą reikalaujama, kad toks nukrypimas būtų išimtis.

70 Be to, pagal suformuotą Teisingumo Teismo jurisprudenciją srauto ir vietos nustatymo duomenų perdavimas tretiesiems asmenims yra Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymas, neatsižvelgiant į vėlesnį šių duomenų panaudojimą. Šiuo klausimu nesvarbu tai, ar atitinkama informacija, susijusi su privačiu gyvenimu, yra jautri, ar ne, ir ar suinteresuotieji asmenys patyrė nepatogumų dėl tokio suvaržymo (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 124 ir 126 punktus bei juose nurodytą jurisprudenciją; taip pat 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* C-511/18, C-512/18 ir C-520/18 115 ir 116 punktus).

71 Chartijos 7 straipsnyje įtvirtintos teisės suvaržymas, kurį lemia srauto ir vietos nustatymo duomenų perdavimas saugumo ir žvalgybos tarnyboms, turi būti laikomas ypač dideliu, atsižvelgiant, be kita ko, į informacijos, kurią gali atskleisti šie duomenys, jautrumą ir, be kita ko, į galimybę remiantis šiais duomenimis nustatyti duomenų subjektų profilį, nes tokia informacija yra tokia pat jautri kaip ir pats pranešimų turinys. Be to, toks suvaržymas duomenų subjektams gali sudaryti įspūdį, kad jų privatus gyvenimas yra nuolat stebimas (pagal analogiją žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 27 ir 37 punktus ir 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 99 ir 100 punktus).

72 Taip pat reikia pažymėti, kad perduodant srauto ir vietos nustatymo duomenis saugumo tikslais gali būti savaime pažeista Chartijos 7 straipsnyje įtvirtinta teisė į komunikacijos slaptumą ir tai gali turėti atgrasomąjį poveikį elektroninių ryšių priemonių naudotojams įgyvendinti Chartijos 11 straipsnyje garantuojamą jų saviraiškos laisvę. Toks atgrasomasis poveikis gali daryti poveikį visų pirma asmenims, kurių komunikacijai pagal nacionalines taisykles taikoma profesinės paslapties apsauga, ir pranešėjams, kurių veikla saugoma 2019 m. spalio 23 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/1937 dėl asmenų, pranešančių apie Sąjungos teisės pažeidimus, apsaugos (OL L 305, 2019, p. 17). Be to, šis poveikis yra tuo didesnis, kuo didesnė duomenų apimtis ir jų įvairovė (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.* C-293/12 ir C-594/12, EU:C:2014:238,

28 punktą; 2016 m. gruodžio 21 d. Sprendimo *Tele2* C-203/15 ir C-698/15, EU:C:2016:970, 101 punktą; taip pat 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* C-511/18, C-512/18 ir C-520/18, 118 punktą).

73 Galiausiai atsižvelgiant į didelį srauto ir vietos nustatymo duomenų, kurie gali būti nuolat saugomi taikant bendrą ir nediferencijuotą 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.

74 Kalbant apie tikslus, galinčius pateisinti tokius suvaržymus, konkrečiai apie pagrindinėje byloje nagrinėjamą nacionalinio saugumo užtikrinimo tikslą, pirmiausia reikia pažymėti, kad ESS 4 straipsnio 2 dalyje nustatyta, jog kiekviena valstybė narė išimtinai išlieka atsakinga už savo nacionalinį saugumą. Ši atsakomybė 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 pačiai visuomenei, gyventojams ar valstybei, pavyzdžiui, teroristinės veiklos, prevenciją ir baudžiamąjį persekiojimą už ją (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, 135 punktas).

75 Nacionalinio saugumo užtikrinimo tikslo, siejamo su ESS 4 straipsnio 2 dalimi, svarba viršija kitų Direktyvos 2002/58 15 straipsnio 1 dalyje nurodytų tikslų, be kita ko, kovos su nusikalstamumu apskritai, net ir su sunkiais nusikaltimais, ir visuomenės saugumo užtikrinimo tikslų svarbą. Iš tiesų pirmesniame punkte nurodytos grėsmės savo pobūdžiu ir ypatingu sunkumu skiriasi nuo bendros įtampos ar sutrikimų, net didelių, rizikos visuomenės saugumui. Taigi su sąlyga, kad bus laikomasi kitų Chartijos 52 straipsnio 1 dalyje numatytų reikalavimų, nacionalinio saugumo užtikrinimo tikslas gali pateisinti priemones, numatančias didesnį pagrindinių teisių suvaržymą nei tas, kurį būtų galima pateisinti kitais tikslais (2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-520/18 ir C-512/18, 136 punktas).

76 Vis dėlto tam, kad būtų įvykdytas šio sprendimo 67 punkte primintas proporcingumo reikalavimas, pagal kurį nuo asmens duomenų apsaugos leidžiančios nukrypti nuostatos ir tokios apsaugos apribojimai turi neviršyti to, kas griežtai būtina, nacionalinės teisės aktai, kuriais suvaržomos Chartijos 7 ir 8 straipsniuose įtvirtintos pagrindinės teisės, turi atitikti reikalavimus, kylančius iš šio sprendimo 65, 67 ir 68 punktuose nurodytos jurisprudencijos.

77 Konkrečiai kalbant, tokiuose teisės aktuose negali būti apsiribojama reikalavimu, kad valdžios institucijų prieiga prie duomenų atitiktų šiuo teisės aktu siekiamą tikslą, bet juose taip pat turi būti numatytos tokį naudojimą reglamentuojančios materialinės ir procesinės sąlygos (pagal analogiją žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 192 punktą ir jame nurodytą jurisprudenciją).

78 Taigi, nors bendra prieiga prie visų saugomų duomenų, kai nėra jokio, net netiesioginio, ryšio su siekiamu tikslu, negali būti laikoma apribota tuo, kas griežtai būtina, nacionalinės teisės aktai, reglamentuojantys prieigą prie srauto ir vietos nustatymo duomenų, turi būti pagrįsti objektyviais kriterijais, kad būtų nustatytos aplinkybės ir sąlygos, kurioms esant kompetentingoms nacionalinėms institucijoms būtų suteikta prieiga prie nagrinėjamų duomenų (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 119 punktą ir jame nurodytą jurisprudenciją).

79 Šie reikalavimai *a fortiori* taikomi teisėkūros priemonei, kaip antai nagrinėjamai pagrindinėje byloje, kuria remdamasi kompetentinga nacionalinė institucija gali įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant atskleisti srauto ir vietos nustatymo duomenis, juos perduodant

saugumo ir žvalgybos tarnyboms. Iš tiesų tokiu perdavimu šie duomenys padaromi prieinami viešosios valdžios institucijoms (pagal analogiją žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 212 punktą).

80 Kadangi srauto ir vietos nustatymo duomenys perduodami bendrai ir nediferencijuojant, toks perdavimas turi poveikį apskritai visiems asmenims, kurie naudojasi elektroninių ryšių paslaugomis. Taigi toks perdavimas taikomas net asmenims, dėl kurių neegzistuoja jokių požymių, leidžiančių manyti, kad jų elgesys gali turėti bent netiesioginį ar tolimą ryšį su tikslu užtikrinti nacionalinį saugumą, visų pirma nenustačius ryšio tarp duomenų, kuriuos numatyta perduoti, ir grėsmės visuomenės saugumui (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 57 ir 58 punktus; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2* C-203/15 ir C-698/15, EU:C:2016:970, 105 punktą). Atsižvelgiant į tai, kad, remiantis tuo, kas nustatyta šio sprendimo 79 punkte, tokių duomenų perdavimas viešosios valdžios institucijoms prilygsta prieigai prie jų, darytina išvada, kad nacionalinės teisės aktai, leidžiantys bendrai ir nediferencijuojant perduoti duomenis viešosios valdžios institucijoms, reiškia bendros prieigos suteikimą.

81 Iš to matyti, kad nacionalinės teisės aktai, įpareigojantys elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant atskleisti srauto ir vietos nustatymo duomenis, juos perduodant saugumo ir žvalgybos tarnyboms, viršija tai, kas griežtai būtina, ir negali būti laikomi pateisinamais demokratinėje visuomenėje, kaip to reikalaujama pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su ESS 4 straipsnio 2 dalimi ir Chartijos 7, 8, 11 straipsniais bei 52 straipsnio 1 dalimi.

82 Atsižvelgiant į visa tai, kas išdėstyta, į antrąjį klausimą reikia atsakyti, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su ESS 4 straipsnio 2 dalimi bei Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad ja draudžiami nacionalinės teisės aktai, pagal kuriuos valstybės institucija, siekdama užtikrinti nacionalinį saugumą, gali įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant perduoti srauto ir vietos nustatymo duomenis saugumo ir žvalgybos tarnyboms.

Dėl bylinėjimosi išlaidų

83 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:

1. **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, 1 straipsnio 3 dalis, 3 straipsnis ir 15 straipsnio 1 dalis, siejami su ESS 4 straipsnio 2 dalimi, turi būti aiškinami taip, kad į šios direktyvos taikymo sritį patenka nacionalinės teisės aktai, pagal kuriuos valstybės institucija gali įpareigoti elektroninių ryšių paslaugų teikėjus perduoti saugumo ir žvalgybos tarnyboms srauto ir vietos nustatymo duomenis, kad būtų užtikrintas nacionalinis saugumas.**

2. **Direktyvos 2002/58, iš dalies pakeistos Direktyva 2009/136, 15 straipsnio 1 dalis, siejama su ESS 4 straipsnio 2 dalimi ir Europos Sąjungos pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad ja draudžiami**

nacionalinės teisės aktai, pagal kuriuos valstybės institucija, siekdama užtikrinti nacionalinį saugumą, gali įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant perduoti srauto ir vietos nustatymo duomenis saugumo ir žvalgybos tarnyboms.

Parašai.