Teismo praktikos rinkinys

GENERALINIO ADVOKATO
MANUEL CAMPOS SÁNCHEZ-BORDONA IŠVADA,
pateikta 2020 m. sausio 15 d.[1]

Sujungtos Bylos C-511/18 ir C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
prieš
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

(*Conseil d'État* (Valstybės Taryba, veikianti kaip Vyriausiasis administracinis teismas, Prancūzija)
prašymai priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas ir privataus gyvenimo apsauga elektroninių ryšių sektoriuje – Nacionalinio saugumo užtikrinimas ir kova su terorizmu – Direktyva 2002/58 EB – Taikymo sritis – 1 straipsnio 3 dalis – 15 straipsnio 3 dalis – ESS 4 straipsnio 2 dalis – Europos Sąjungos pagrindinių teisių chartija – 6, 7, 8, 11 ir 47 straipsniai ir 52 straipsnio 1 dalis – Bendras ir nediferencijuotas prisijungimo duomenų ir duomenų, leidžiančių nustatyti turinio kūrėjų tapatybę, saugojimas – Srauto ir vietos nustatymo duomenų rinkimas – Prieiga prie duomenų"

1. Pastaruosius kelerius metus Teisingumo Teismas laikėsi nuoseklaus požiūrio, formuodamas jurisprudenciją dėl asmens duomenų saugojimo ir prieigos prie jų; ją sudaro šie svarbiausi sprendimai:

– 2014 m. balandžio 8 d. Sprendimas *Digital Rights Ireland ir kt.*[2], kuriame Teisingumo Teismas pripažino, kad Direktyva 2006/24/EB[3] negalioja, nes dėl jos galėjo būti neproporcingai ribojamos Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7 ir 8 straipsniais pripažįstamos teisės,

– 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.*[4], kuriame Teisingumo Teismas išaiškino Direktyvos 2002/58/EB[5] 15 straipsnio 1 dalį,

– 2018 m. spalio 2 d. Sprendimas *Ministerio Fiscal*[6], kuriame Teisingumo Teismas patvirtino tos pačios Direktyvos 2002/58 nuostatos išaiškinimą.

1 Originalo kalba: ispanų.

2 Bylos C-293/12 ir C-594/12, EU:C:2014:238 (toliau – Sprendimas *Digital Rights*).

3 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB (OL L 105, 2006, p. 54).

4 Bylos C-203/15 ir C-698/15, EU:C:2016:970 (toliau – Sprendimas *Tele2 Sverige ir Watson ir kt.*).

5 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 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).

6 Byla C-207/16, EU:C:2018:788 (toliau – Sprendimas *Ministerio Fiscal*).

2. Šie sprendimai (visų pirma antrasis) kelia tam tikrų valstybių narių institucijų susirūpinimą, nes jos mano, kad taikant tuos sprendimus jos netenka priemonės, kurią laiko būtina siekiant apsaugoti nacionalinį saugumą ir kovoti su nusikalstamumu ir terorizmu. Tuo remdamosi kai kurios valstybės narės prašo pakeisti arba patikslinti tą jurisprudenciją.

3. Tam tikri valstybių narių teismai tokį patį susirūpinimą išreiškė keturiuose prašymuose priimti prejudicinį sprendimą [7]; išvadą dėl jų pateikiau tą pačią dieną.

4. Visų pirma keturiose bylose keliama problema dėl Direktyvos 2002/58 taikymo veiklai, susijusiai su nacionaliniu saugumu ir kova su terorizmu. Jeigu šiomis aplinkybėmis minėta direktyva būtų taikoma, reikia išsiaiškinti, kokiu mastu valstybės narės gali riboti direktyvos saugomas teises į privatumą. Galiausiai reikės išnagrinėti, kiek su šia sritimi susijusiuose įvairiuose nacionalinės teisės aktuose (Jungtinės Karalystės [8], Belgijos [9] ir Prancūzijos [10]) atsižvelgiama į Sąjungos teisę, kaip ją išaiškino Teisingumo Teismas.

I. Teisinis pagrindas

A. Sąjungos teisė

1. Direktyva 2002/58

5. 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 su asmens duomenų tvarkymu elektroninių ryšių sektoriuje ir užtikrinančių laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą Bendrijoje, suderinimas.

<…>

3. Ši direktyva netaikoma veiklos rūšims, kurios neįeina į Europos bendrijos steigimo sutarties 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. 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.“

7 Be šių dviejų bylų (C-511/18 ir C-512/18), Bylos *Privacy International* (C-623/17) ir *Ordre des barreaux francophones et germanophone ir kt.* (C-520/18).

8 Byla *Privacy International*, C-623/17.

9 Byla *Ordre des barreaux francophones et germanophone ir kt.*, C-520/18.

10 Bylos *La Quadrature du Net ir kt.*, C-511/18 ir C-512/18.

7. 5 straipsnio „Pranešimų konfidencialumas“ 1 dalyje įtvirtinta:

„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 [asmenims, kurie nėra naudotojai,] 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 [siekiant] perduoti pranešimą nepažeidžiant konfidencialumo principo.“

8. 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.“

9. 15 straipsnio „Kai kurių Direktyvos 95/46/EB[11] nuostatų taikymas“ 1 dalyje numatyta:

„Valstybės narės gali patvirtinti teisines priemones, ribojančias šios direktyvos 5 ir 6 straipsniuose, 8 straipsnio 1, 2, 3 ir 4 dalyse ir 9 straipsnyje nustatytų teisių ir pareigų taikymą, jeigu toks ribojimas yra būtina, tinkama ir adekvati [proporcinga] demokratinės visuomenės priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias [nusikalstamas] veikas ar neteisėtą elektroninių ryšių sistemos naudojimą [ir vykdant persekiojimą dėl jų], kaip nurodyta Direktyvos 95/46/EB 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 [įskaitant] nurodytus Europos Sąjungos [s]utarties 6 straipsnio 1 ir 2 dalyse.“

2. Direktyva 2000/31/EB[12]

10. 14 straipsnyje nustatyta:

„1. Kai teikiama informacinės visuomenės paslauga, kurią sudaro paslaugos gavėjo pateiktos informacijos perdavimas ryšio tinklu, valstybės narės užtikrina, kad paslaugų teikėjas nebūtų atsakingas už informaciją, kurią saugo paslaugos gavėjo prašymu, tik tada, jei:

<…>

3. Šis straipsnis neturi įtakos teismo arba administracinės institucijos galimybei vadovaujantis valstybių narių teisinėmis sistemomis reikalauti, kad paslaugų teikėjas nutrauktų pažeidimą arba užkirstų jam kelią, jis taip pat neturi įtakos valstybių narių galimybei nustatyti procedūras, reglamentuojančias informacijos panaikinimą arba galimybės ją pasiekti atėmimą.“

11 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 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).

12 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva) (OL L 178, 2000, p. 1; 2004 m. specialusis leidimas lietuvių k., 13 sk., 25 t., p. 399).

11. 15 straipsnyje numatyta:

„1. Valstybės narės nenustato [paslaugų] teikėjams nei bendros prievolės teikiant 12, 13 ir 14 straipsnių reglamentuojamas paslaugas stebėti informaciją, kurią jie perduoda arba saugo, nei bendros prievolės aktyviai domėtis faktais arba aplinkybėmis, rodančiomis nelegalią veiklą.

2. Valstybės narės gali nustatyti prievoles informacinės visuomenės paslaugų teikėjams nedelsiant informuoti kompetentingas viešąsias institucijas apie įtariamą nelegalią veiklą arba informaciją, kurią pateikia jų paslaugų gavėjai, arba prievolę pateikti kompetentingoms institucijoms, gavus jų prašymą, informaciją, leidžiančią nustatyti jų paslaugos gavėjų, su kuriais jie sudarę informacijos saugojimo sutartis, tapatybę.“

3. Reglamentas (ES) 2016/679[13]

12. 2 straipsnyje „Materialinė taikymo sritis“ įtvirtinta:

„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;

c) duomenis tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla;

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. 23 straipsnio „Apribojimai“ 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 pagrindinių teisių ir laisvių esmė ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

13 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016, p. 11, klaidų ištaisymas OL L 127, 2018 5 23, p. 2).

d) nusikalstamų veikų prevenciją, tyrimą, nustatymą ar patraukimą už jas baudžiamojon atsakomybėn arba baudžiamųjų sankcijų 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 proceso apsaugą;

g) reglamentuojamųjų profesijų etikos pažeidimų prevenciją, tyrimą, nustatymą ir patraukimą baudžiamojon 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.“

14. 95 straipsnyje „Ryšys su Direktyva 2002/58/EB“ įtvirtinta:

„Šiuo reglamentu fiziniams arba juridiniams asmenims nenustatoma papildomų prievolių, susijusių su duomenų tvarkymu Sąjungoje viešaisiais ryšių tinklais teikiant viešai prieinamas elektroninių ryšių paslaugas, kiek tai susiję su klausimais, kuriais jiems taikomos Direktyvoje 2002/58/EB nustatytos specialios prievolės, kuriomis siekiama to paties tikslo.“

B. Nacionalinė teisė

1. Code de la sécurité intérieure (Vidaus saugumo kodeksas)

15. L. 851-1 straipsnyje nustatyta:

„Šios knygos II antraštinės dalies 1 skyriuje numatytomis sąlygomis gali būti leidžiama iš elektroninių ryšių operatorių ir asmenų, nurodytų *Code des postes et des communications électroniques* (Pašto ir elektroninių ryšių kodeksas) L.34-1 straipsnyje, taip pat asmenų, nurodytų *Loi n.º 2004-575 <…> pour la confiance dans l'économie numériqu*e (Įstatymas Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika) 6 straipsnio I dalies 1 ir 2 punktuose, rinkti informaciją ar dokumentus, tvarkomus ar saugomus jų tinkluose arba jiems teikiant elektroninių ryšių paslaugas, įskaitant techninius duomenis, susijusius su abonento numerių identifikavimu ar prisijungimu prie elektroninių ryšių paslaugų, su visų nurodyto asmens prisijungimo ar abonento numerių rinkimu, naudotų galinių įrenginių vietos nustatymu ir abonento komunikacijomis, t. y. numeriais, kuriais skambinta ir iš kurių gauti skambučiai, ryšio trukme ir data. <…>“

16. L. 851-2 ir L. 851-4 straipsniuose, atsižvelgiant į skirtingus tikslus ir taikant skirtingas taisykles, reglamentuojama realiuoju laiku suteikiama administracinė prieiga prie tokia tvarka saugomų prisijungimo duomenų.

17. L. 851-2 straipsnyje išimtinai terorizmo prevencijos tikslais leidžiama iš tų pačių subjektų rinkti L. 851-1 straipsnyje nurodytą informaciją ar dokumentus. Šis duomenų rinkimas, susijęs tik su vienu ar keliais asmenimis, kurie prieš tai identifikuoti kaip keliantys terorizmo grėsmę, vyksta realiuoju laiku. Tas pats pasakytina apie L. 851-4 straipsnį, pagal kurį operatoriams leidžiama realiuoju laiku

perduoti tik techninius duomenis apie galinių įrenginių vietą [14].

18. L. 851-3 straipsnyje leidžiama elektroninių ryšių operatorius ir techninių paslaugų teikėjus įpareigoti „savo tinkluose automatizuotomis priemonėmis tvarkyti duomenis tam, kad atsižvelgiant į leidime apibrėžtus parametrus būtų nustatomi prisijungimai, galintys kelti terorizmo grėsmę“ [15].

19. L. 851-5 straipsnyje nustatyta, kad tam tikromis sąlygomis „gali būti leidžiama naudoti techninį prietaisą, kuris padėtų realiuoju laiku nustatyti asmens, transporto priemonės ar daikto buvimo vietą“.

20. Pagal L. 851-6 straipsnio I dalį tam tikromis sąlygomis galima „naudojantis *Code pénal* (Baudžiamasis kodeksas) 226-3 straipsnio 1 dalyje nurodytu aparatu ar techniniu prietaisu <…> tiesiogiai rinkti techninius prisijungimo duomenis, leidžiančius nustatyti galinį įrenginį arba jo naudotojo abonento numerį, taip pat duomenis, susijusius su naudojamų galinių įrenginių vieta“.

2. Pašto ir elektroninių ryšių kodeksas

21. Faktinėms aplinkybėms taikytinos versijos L. 34-1 straipsnyje nustatyta:

„I. Šis straipsnis taikomas asmens duomenų tvarkymui teikiant visuomenei elektroninių ryšių paslaugas; visų pirma jis taikomas tinklams, kuriuose naudojami identifikavimo ir duomenų rinkimo prietaisai.

II. Elektroninių ryšių operatoriai, visų pirma asmenys, kurių veikla – teikti visuomenei ryšių paslaugas internetu, sunaikina arba nuasmenina visus srauto duomenis, nepažeisdami III, IV, V ir VI dalių nuostatų.

Subjektai, teikiantys visuomenei elektroninių ryšių paslaugas, laikydamiesi pirmesnės pastraipos nustato vidaus tvarką kompetentingų institucijų prašymams įvykdyti.

Subjektai, kurie, vykdydami pagrindinę arba papildomą profesinę veiklą, teikia visuomenei prisijungimo paslaugas, leidžiančias naudojantis prieiga prie interneto palaikyti ryšius internetu (net ir nemokamai), privalo vykdyti pagal šį straipsnį elektroninių ryšių operatoriams taikomas nuostatas.

III. Tam, kad būtų atskleistos ir ištirtos nusikalstamos veikos arba *Code de la propriété intellectuelle* (Intelektinės nuosavybės kodeksas) L. 336-3 straipsnyje nustatytos pareigos neįvykdymas ir dėl to būtų persekiojama, arba tam, kad būtų užkirstas kelias prieš duomenų tvarkymo automatizuotomis priemonėmis sistemas rengiamoms atakoms, numatytoms Baudžiamojo kodekso 323-1–323-3-1 straipsniuose, už kurias baudžiama pagal minėtus straipsnius, ir siekiant vienintelio tikslo – prireikus užtikrinti, kad teisminei institucijai arba Intelektinės nuosavybės kodekso L. 331-12 straipsnyje nurodytai viešajai institucijai, arba *Code de la défense* (Gynybos kodeksas) L. 2321-1 straipsnyje nurodytai nacionalinei informacinių sistemų saugumo institucijai būtų suteikta reikiamos informacijos, – operacijų, kuriomis siekiama sunaikinti arba nuasmeninti tam tikrų kategorijų techninius duomenis, vykdymas gali būti atidėtas ne ilgiau kaip vieniems metams. *Conseil d'État* (Valstybės Taryba) dekrete, priimtame pateikus *Commission nationale de l'informatique et des libertés* (Nacionalinė informatikos ir laisvių komisija) nuomonę, laikantis VI dalyje nurodytų

14 Kaip teigia prašymus priimti prejudicinį sprendimą pateikęs teismas, dėl šių būdų paslaugų teikėjams nenustatyta papildoma pareiga saugoti duomenis, palyginti su tuo, kas reikalinga sąskaitoms už jų paslaugas pateikti, šių paslaugų rinkodarai vykdyti ir pridėtinės vertės paslaugoms teikti.

15 Kaip teigia prašymą priimti prejudicinį sprendimą pateikęs teismas, šis būdas, kuris neapima bendro ir nediferencijuoto saugojimo, skirtas tik tam, kad ribotą laiką iš šių asmenų tvarkytų visų prisijungimo duomenų būtų atrenkami tie duomenys, kurie galėtų būti susiję su tokios rūšies sunkia nusikalstama veika.

apribojimų patikslinamos šios duomenų kategorijos ir duomenų saugojimo trukmė, atsižvelgiant į operatorių veiklą ir ryšių pobūdį, taip pat kompensavimo taisyklės, pagal kurias prireikus kompensuojamos papildomos konkrečios paslaugų, šiuo pagrindu operatorių teikiamų valstybės prašymu, išlaidos, kurias galima nustatyti.

<…>

VI. III, IV ir V dalyse nustatytomis sąlygomis saugomi ir tvarkomi duomenys susiję tik su operatorių teikiamų paslaugų naudotojų identifikavimu, techninėmis operatorių užtikrinamų ryšių savybėmis ir galinių įrenginių vieta.

Jokiais atvejais duomenys negali būti susiję su atitinkamos korespondencijos, kuria keičiamasi, turiniu ar informacija, su kuria susipažįstama kokia nors forma naudojantis tokiais elektroniniais ryšiais.

Duomenys saugomi ir tvarkomi laikantis 1978 m. sausio 6 d. *Loi no 78-17 relative à l'informatique, aux fichiers et aux libertés* (Informatikos, rinkmenų ir laisvių įstatymas Nr. 78-17) nuostatų.

Operatoriai imasi visų priemonių, siekdami neleisti šiais duomenimis naudotis kitais tikslais, nei numatyti šiame straipsnyje."

22. Pagal R. 10-13 straipsnio 1 dalį tam, kad būtų atskleistos ir ištirtos nusikalstamos veikos ir būtų vykdomas persekiojimas dėl jų, operatoriai turi saugoti tokius duomenis:

„a) informaciją, leidžiančią nustatyti naudotojo tapatybę;

b) duomenis apie naudojamus galinius ryšių įrenginius;

c) informaciją apie kiekvieno ryšio technines savybes, taip pat jo datą, laiką ir trukmę;

d) duomenis apie prašytas arba naudotas papildomas paslaugas ir jų teikėjus;

e) duomenis, leidžiančius nustatyti ryšių adresato (-ų) tapatybę."

23. Pagal tos pačios nuostatos II dalį tuo atveju, kai vykdoma telefonijos veikla, operatorius turi saugoti ne tik pirma nurodytus duomenis, bet ir duomenis, padedančius nustatyti ryšio šaltinį ir vietą.

24. Pagal to paties straipsnio III dalį nurodyti duomenys turi būti saugomi metus nuo jų įregistravimo dienos.

3. Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (2004 m. birželio 21 d. Įstatymas Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika)

25. Įstatymo Nr. 2004-575 6 straipsnio II dalies pirmoje pastraipoje numatyta, kad asmenys, kurių veikla yra teikti visuomenei ryšio paslaugas internetu, ir fiziniai ar juridiniai asmenys, kurie užtikrina, net ir nemokamai, internetu teikiant visuomenei ryšių paslaugas šių paslaugų gavėjų pateiktų signalų, rašytinės medžiagos, vaizdo, garso ar bet kokio pobūdžio pranešimų saugojimą, „laiko ir saugo duomenis, leidžiančius nustatyti asmenis, prisidėjusius kuriant paslaugų, kurias jie teikia, turinį".

26. Tos pačios nuostatos II dalies trečioje pastraipoje nustatyta, kad teisminė institucija gali pareikalauti iš šių asmenų perduoti pirmoje pastraipoje nurodytus duomenis.

27. II dalies paskutinėje pastraipoje numatyta, kad *Conseil d'État* (Valstybės Taryba) dekrete „apibrėžia pirmoje pastraipoje nurodytus duomenis ir nustato jų saugojimo trukmę ir tvarką“ [16].

II. Faktinės aplinkybės ir pateikti prejudiciniai klausimai

A. Byla C-511/18

28. *La Quadrature du Net*, *French Data Network*, *Igwan.net* ir *Fédération des fournisseurs d'accès à internet associatifs* (toliau – pareiškėjai) paprašė *Conseil d'État* (Valstybės Taryba) panaikinti kelis dekretus, kuriais įgyvendinamos tam tikros Vidaus saugumo kodekso nuostatos [17].

29. Pareiškėjai iš esmės teigė, kad tiek ginčijami dekretai, tiek šios Vidaus saugumo kodekso nuostatos pažeidžia teisę į privatų gyvenimą, teisę į asmens duomenų apsaugą ir teisę į veiksmingą teisinę gynybą, užtikrinamas atitinkamai pagal Chartijos 7, 8 ir 47 straipsnius.

30. Tokiomis aplinkybėmis *Conseil d'État* (Valstybės Taryba) pateikia Teisingumo Teismui šiuos klausimus:

„1. Ar tokiomis aplinkybėmis, kai nacionaliniam saugumui keliama rimta nuolatinė grėsmė, ypač susijusi su terorizmo pavojumi, pagal [Direktyvos 2002/58] 15 straipsnio 1 dalies leidžiančiąsias nuostatas paslaugų teikėjams numatyta pareiga bendrai ir nediferencijuojant saugoti duomenis turi būti laikoma teisių apribojimu, pateisinamu pagal [Chartijos] 6 straipsnį užtikrinama teise į saugumą ir nacionalinio saugumo reikalavimais, dėl kurių atsakomybė pagal [ESS] 4 straipsnį tenka tik valstybėms narėms?

2. Ar [Direktyva 2002/58], siejama su [Chartija], turi būti aiškinama taip, kad ja leidžiamos teisėkūros priemonės, kaip antai skirtos rinkti srauto ir konkrečių asmenų vietos nustatymo duomenims realiu laiku, kurios, nors ir daro poveikį elektroninių ryšių paslaugų teikėjų teisėms ir pareigoms, vis dėlto nenustato konkrečios jų duomenų saugojimo pareigos?

3. Ar [Direktyva 2002/58], siejama su [Chartija], turi būti aiškinama taip, jog tam, kad prisijungimo duomenų rinkimas būtų teisėtas, pagal ją visais atvejais taikomas reikalavimas apie tai informuoti duomenų subjektus, kai toks informavimas nebegali neigiamai paveikti kompetentingų institucijų atliekamų tyrimų ar kai toks rinkimas gali būti laikomas teisėtu atsižvelgiant į visas kitas egzistuojančias procedūrines garantijas, jeigu jomis užtikrinama teisė į veiksmingą teisinę gynybą?“

16 Tai ji padarė *Décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (2011 m. vasario 25 d. Dekretas Nr. 2011-219 dėl duomenų, leidžiančių nustatyti visų kuriant internete skelbiamą turinį prisidėjusių asmenų tapatybę, saugojimo ir perdavimo). Atsižvelgiant į šį dekretą galima išskirti: a) 1 straipsnio 1 dalį, pagal kurią subjektai, teikiantys ryšių paslaugas internetu, turi saugoti šiuos duomenis: prisijungimo identifikatorių, abonentui suteiktą identifikatorių, prisijungti naudojamo galinio įrenginio identifikatorių, prisijungimo pradžios ir pabaigos datą ir laiką, abonento linijos savybes; b) 1 straipsnio 2 dalį – pagal ją asmenys, kurie užtikrina, net ir nemokamai, internetu teikiant visuomenei ryšių paslaugas šių paslaugų gavėjų pateiktų signalų, rašytinės medžiagos, vaizdo, garso ar bet kokio pobūdžio pranešimų saugojimą, turi kiekvienos operacijos atveju saugoti šiuos duomenis: prisijungimo prie ryšio šaltinio identifikatorių, turiniui, dėl kurio vykdoma operacija, suteiktą identifikatorių, siekiant prisijungti prie paslaugos ir perduoti turinį naudojamų protokolų tipus, operacijos pobūdį, jos datą ir laiką, operacijos autoriaus naudojamą identifikatorių; c) galiausiai 1 straipsnio 3 dalį, kurioje nustatyta, kad dviejose pirmesnėse dalyse minimi asmenys turi saugoti toliau nurodytą informaciją, naudotojo pateiktą pasirašant sutartį ar sukuriant paskyrą: prisijungimo identifikatorių sukuriant paskyrą; pavardę ir vardą arba įmonės pavadinimą; susijusius pašto adresus, naudojamus slapyvardžius, susijusius el. pašto arba paskyros adresus, telefono numerius, atnaujintą slaptažodį ir duomenis, leidžiančius jį patikrinti arba pakeisti.

17 Ginčijami dekretai buvo šie: *Décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement* (2015 m. rugsėjo 28 d. Dekretas Nr. 2015-1185 dėl specialiųjų žvalgybos tarnybų paskyrimo); b) *Décret n.º 2015-1211 du 1er octubre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (2015 m. spalio 1 d. Dekretas Nr. 2015-1211 dėl ginčų, susijusių su žvalgybos būdų, kuriems reikalingas leidimas, ir valstybės saugumui svarbių rinkmenų sistemų įgyvendinimu); c) *Décret n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure* (2015 m. gruodžio 11 d. Dekretas Nr. 2015-1639 dėl kitų nei specializuotų žvalgybos tarnybų, kurios gali naudotis Vidaus saugumo kodekso VIII knygos V antraštinėje dalyje nurodytais duomenų rinkimo būdais, paskyrimo); d) *Décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement* (2016 m. sausio 29 d. Dekretas Nr. 2016-67 dėl informacijos rinkimo būdų).

B. Byla C-512/18

31. Pareiškėjai – ginčo, dėl kurio iškelta Byla C-511/18, šalys, išskyrus *Igwan.net*, taip pat prašė *Conseil d'État* (Valstybės Taryba) panaikinti (implicitinį) sprendimą atmesti jų prašymą panaikinti *Code des postes et des communications électroniques* (Pašto ir elektroninių ryšių kodeksas) R. 10-13 straipsnį ir 2011 m. vasario 25 d. Dekretą Nr. 2011-219.

32. Šie pareiškėjai mano, kad ginčijamose teisės normose yra nustatyta pareiga saugoti srauto, vietos nustatymo ir prisijungimo duomenis ir dėl šios pareigos, atsižvelgiant į jos bendrą pobūdį, neproporcingai ribojama teisė į privatų ir šeimos gyvenimą, teisė į asmens duomenų apsaugą ir teisė į saviraiškos laisvę (šios teisės užtikrinamos Chartijos 7, 8 ir 11 straipsniuose), taip pažeidžiant Direktyvos 2002/58 15 straipsnio 1 dalį.

33. Nagrinėdama šį skundą *Conseil d'État* (Valstybės Taryba) suformulavo tokius prejudicinius klausimus:

„1. Ar pagal [Direktyvos 2002/58] 15 straipsnio 1 dalies leidžiančiąsias nuostatas paslaugų teikėjams numatyta pareiga bendrai ir nediferencijuojant saugoti duomenis turi būti laikoma, ypač atsižvelgiant į garantijas ir kontrolę, kurios vėliau taikytinos šių prisijungimo duomenų rinkimui ir jų naudojimui, teisių apribojimu, pateisinamu pagal [Chartijos] 6 straipsnį užtikrinama teise į saugumą ir nacionalinio saugumo reikalavimais, dėl kurių atsakomybė pagal [ESS] 4 straipsnį tenka tik valstybėms narėms?

2. Ar Direktyvos 2000/31 nuostatos, atsižvelgiant į [Chartijos] 6, 7, 8 ir 11 straipsnius bei 52 straipsnio 1 dalį, turi būti aiškinamos taip, kad jomis leidžiama valstybei narei nustatyti nacionalinį reglamentavimą, pagal kurį asmenys, kurių veikla yra teikti visuomenei ryšio paslaugas internetu, ir fiziniai ar juridiniai asmenys, kurie užtikrina, net ir nemokamai, teikiant visuomenei ryšių paslaugas internetu šių paslaugų gavėjų pateiktų signalų, rašytinės medžiagos, vaizdo, garso ar bet kokio pobūdžio pranešimų saugojimą, būtų įpareigoti saugoti duomenis, leidžiančius nustatyti asmenis, dalyvavusius kuriant jų teikiamų paslaugų turinį, kad prireikus teisminė institucija galėtų iš jų pareikalauti perduoti šiuos duomenis, siekdama užtikrinti, kad būtų laikomasi civilinę ar baudžiamąją atsakomybę reglamentuojančių nuostatų?“

III. Procesas Teisingumo Teisme ir šalių pozicijos

34. Prašymai priimti prejudicinį sprendimą Teisingumo Teismo kanceliarijoje užregistruoti 2018 m. rugpjūčio 3 d.

35. Rašytines pastabas pateikė *La Quadrature du Net*, *la Fédération des fournisseurs d'accès à Internet associatifs*, *French Data Network*, Vokietijos, Belgijos, Jungtinės Karalystės, Čekijos, Kipro, Danijos, Ispanijos, Estijos, Prancūzijos, Vengrijos, Airijos, Lenkijos ir Švedijos vyriausybės, taip pat Komisija.

36. 2019 m. rugsėjo 9 d. buvo surengtas viešas teismo posėdis (kartu su teismo posėdžiais bylose *Privacy International*, C-623/17, ir *Ordre des barreaux francophones et germanophone ir kt.*, C-520/18); jame dalyvavo keturių prašymų priimti prejudicinį sprendimą šalys, minėtų vyriausybių ir Nyderlandų, Norvegijos vyriausybių bei Komisijos atstovai, taip pat Europos asmens duomenų apsaugos priežiūros pareigūnas.

IV. Analizė

37. *Conseil d'État* (Valstybės Taryba) klausimus galima suskirstyti į tris grupes:

– pirma, ar Sąjungos teisę atitinka nacionalinės teisės normos, kuriose elektroninių ryšių paslaugų teikėjams nustatyta pareiga bendrai ir nediferencijuojant saugoti prisijungimo duomenis (pirmasis klausimas bylose C-511/18 ir C-512/18), visų pirma duomenis, leidžiančius nustatyti turinio, kurį siūlo šių paslaugų teikėjai, kūrėjų tapatybę (antrasis klausimas byloje C-512/18),

– antra, ar tam, kad prisijungimo duomenų rinkimo procedūros būtų teisėtos, visais atvejais turi būti informuojami duomenų subjektai, jeigu nekyla pavojus atliekamiems tyrimams (trečiasis klausimas byloje C-511/18),

– trečia, ar srauto ir vietos nustatymo duomenų rinkimas realiuoju laiku, neprivalant jų saugoti, atitinka (ir kokiomis sąlygomis) Direktyvą 2002/58 (antrasis klausimas byloje C-511/18).

38. Galiausiai reikia nustatyti, ar Sąjungos teisę atitinka nacionalinės teisės normos, kuriose elektroninių ryšių paslaugų teikėjams nustatytos dviejų rūšių pareigos: a) pirma, *rinkti* tam tikrus duomenis, tačiau jų nesaugoti; b) antra, *saugoti* prisijungimo duomenis ir duomenis, padedančius nustatyti paslaugų, teikiamų tokių paslaugų teikėjų, turinio kūrėjų tapatybę.

39. Visų pirma reikės išnagrinėti, ar Direktyva 2002/58 yra taikytina, būtent atsižvelgiant į aplinkybes [18], kuriomis šios nacionalinės teisės normos priimtos (t. y. aplinkybes, kurioms susiklosčius gali kilti pavojus nacionaliniam saugumui).

A. Dėl Direktyvos 2002/58 taikytinumo

40. Prašymus priimti prejudicinį sprendimą pateikęs teismas laikosi nuomonės, kad teisės normos, dėl kurių kilo ginčas, patenka į Direktyvos 2002/58 taikymo sritį. Jis mano, kad tokia išvada darytina remiantis jurisprudencija, suformuota Sprendime *Tele2 Sverige ir Watson* ir patvirtinta Sprendime *Ministerio Fiscal*.

41. Priešingai, kai kurios į bylą įstojusios vyriausybės teigia, kad nagrinėjamos teisės normos į šios direktyvos taikymo sritį nepatenka. Savo pozicijai apginti jos, be kitų argumentų, nurodo 2006 m. gegužės 30 d. Sprendimą *Parlamentas / Taryba ir Komisija* [19].

42. Sutinku su *Conseil d'État* (Valstybės Taryba), kad Sprendime *Tele2 Sverige ir Watson* ši ginčo dalis išspręsta patvirtinus, jog Direktyva 2002/58 iš esmės taikoma, kai elektroninių paslaugų teikėjai įstatymo yra įpareigoti saugoti savo abonentų duomenis ir leisti valdžios institucijoms su jais susipažinti. Šio argumento nepakeičia tai, kad nacionalinio saugumo sumetimais paslaugų teikėjams yra nustatytos tam tikros pareigos.

43. Jau dabar turiu pažymėti, kad jeigu būtų kokių nors Sprendimo *Tele2 Sverige ir Watson* ir ankstesnių sprendimų neatitikimų, pirmenybę reikėtų teikti pirmajam, nes jis vėlesnis ir dar kartą patvirtintas Sprendimu *Ministerio Fiscal*. Vis dėlto manau, kad neatitikimų nėra, ir pabandysiu tai paaiškinti.

18 Kaip nurodyta pirmajame klausime byloje C-511/18, „aplinkyb[es], kai nacionaliniam saugumui keliama rimta nuolatinė grėsmė, ypač susijusi su terorizmo pavojumi“.

19 Bylos C-317/04 ir C-318/04, EU:C:2006:346 (toliau – Sprendimas *Parlamentas / Taryba ir Komisija*).

1. Sprendimas „Parlamentas / Taryba ir Komisija“

44. Sprendime *Parlamentas / Taryba ir Komisija* išnagrinėti klausimai susiję su:

– Europos bendrijos ir Jungtinių Amerikos Valstijų susitarimu dėl oro vežėjų PNR [Passenger Name Records (keleivių duomenų įrašų)] duomenų tvarkymo ir perdavimo Jungtinių Amerikos Valstijų institucijoms [20],

– toms institucijoms perduodamų asmens duomenų, nurodytų keleivio duomenų įrašuose, apsaugos tinkamumu [21].

45. Teisingumo Teismas padarė išvadą, kad šių duomenų perdavimas yra tvarkymo operacija, susijusi su visuomenės saugumu ir su valstybės veiksmais baudžiamosios teisės srityje. Pagal Direktyvos 95/46 3 straipsnio 2 dalies pirmą įtrauką abu nagrinėjami sprendimai nepateko į Direktyvos 95/46 taikymo sritį.

46. Iš pradžių duomenis rinko oro vežėjai, vykdydami į Sąjungos teisės taikymo sritį patenkančią veiklą (parduodami bilietus). Vis dėlto, kaip nurodyta nagrinėjamame sprendime, tvarkyti šiuos duomenis „[reikia ne siekiant] suteikti paslaugas, bet [norint] apginti visuomenės saugumą ir nubaudimo tikslais“ [22].

47. Taigi Teisingumo Teismas laikėsi teleologinio požiūrio, atsižvelgdamas į tikslą, kurio siekiama tvarkant duomenis: kadangi siekiama užtikrinti visuomenės saugumo apsaugą, duomenų tvarkymas turėjo būti laikomas nepatenkančiu į Direktyvos 95/46 taikymo sritį. Vis dėlto šis tikslas nebuvo vienintelis lemiamas kriterijus [23], todėl sprendime pabrėžiama, kad „perdavimas vyksta pagal valstybės institucijų nustatytą tvarką, susijusią su visuomenės saugumu“ [24].

48. Taigi remiantis Sprendimu *Parlamentas / Taryba ir Komisija* galima įvertinti, kuo skiriasi Direktyvoje 95/46 įtvirtintos apribojimo sąlygos (analogiškos numatytoms Direktyvoje 2002/58) ir išimties sąlyga. Iš tikrųjų ir vienos, ir kitos sąlygos vis dėlto yra susijusios su panašiais bendrojo intereso tikslais, todėl atsiranda tam tikros painiavos dėl atitinkamos jų taikymo srities, kaip anuomet įspėjo generalinis advokatas Y. Bot [25].

20 2004 m. gegužės 17 d. Tarybos sprendimas 2004/496/EB dėl Europos bendrijos ir Jungtinių Amerikos Valstijų susitarimo dėl oro vežėjų PNR duomenų tvarkymo ir perdavimo Jungtinių Valstijų vidaus saugumo departamento Muitinių ir sienos apsaugos biurui sudarymo (OL L 183, 2004, p. 83; klaidų ištaisymas OL L 255, 2005, p. 168) (byla C-317/04).

21 2004 m. gegužės 14 d. Komisijos sprendimas 2004/535/EB dėl Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnybai perduodamų oro keleivių asmens duomenų, nurodytų Keleivio duomenų įraše (*Passenger Name Record*), tinkamos apsaugos (OL L 235, 2004, p. 11) (byla C-318/04).

22 Sprendimo *Parlamentas / Taryba ir Komisija* 57 punktas. 58 punkte pabrėžiama, jog „dėl to, kad <…> duomenys komerciniais tikslais buvo surinkti privačių subjektų, organizuojančių jų perdavimą į trečiąją valstybę“, šis perdavimas nėra vienas iš Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje nurodytų atvejų, kuriais ši direktyva netaikoma, nes „nagrinėjamas perdavimas nepatenka į šios nuostatos taikymo sritį. Iš tikro šis perdavimas vyksta pagal valstybės institucijų nustatytą tvarką, susijusią su visuomenės saugumu“.

23 Vėliau savo išvadoje byloje *Airija / Parlamentas ir Taryba* (C-301/06, EU:C:2008:558) tai pažymėjo buvęs generalinis advokatas Y. Bot. Jis teigė, kad Sprendimas *Parlamentas / Taryba ir Komisija* „nereiškia, jog tik asmens duomenų tvarkymo tikslo nagrinėjimas yra svarbus siekiant priskirti šį tvarkymą prie Direktyva 95/46 įdiegtos duomenų apsaugos sistemos ar atvirkščiai. Taip pat svarbu patikrinti, kokią veiklą vykdant šie duomenys yra tvarkomi. Tik jei šis tvarkymas atliekamas vykdant valstybės ar valstybės institucijų veiklą, o ne privačių subjektų veiklą, jam, remiantis Direktyvos 95/46 3 straipsnio 2 dalies pirmąja įtrauka, nėra taikoma šioje direktyvoje numatyta Bendrijos asmens duomenų apsaugos sistema“ (122 punktas).

24 Sprendimo *Parlamentas / Taryba ir Komisija* 58 punktas. Susitarimo pagrindinis tikslas buvo reikalauti, kad oro vežėjai, teikiantys keleivių skraidinimo iš Sąjungos į JAV ir atgal paslaugas, suteiktų JAV institucijoms elektroninę prieigą prie PNR įrašuose pateiktų duomenų, esančių jų kompiuterinėse užsakymų ir išvykimo kontrolės sistemose. Taigi jame buvo nustatyta tarptautinio Sąjungos ir JAV bendradarbiavimo forma, siekiant kovoti su terorizmu ir kitais sunkiais nusikaltimais, ir stengiamasi šį tikslą suderinti su tikslu apsaugoti keleivių asmens duomenis. Šiomis aplinkybėmis vežėjams nustatyta pareiga nelabai skyrėsi nuo tiesioginio valdžios institucijų keitimosi duomenimis.

25 Generalinio advokato Y. Bot išvados byloje *Airija / Parlamentas ir Taryba* (C-301/06, EU:C:2008:558) 127 punktas.

49. Gali būti, kad dėl šios painiavos valstybės narės pateikė argumentą, jog šiomis aplinkybėmis Direktyva 2002/58 yra netaikytina. Jos mano, kad nacionalinio saugumo interesai užtikrinami tik taikant Direktyvos 2002/58 1 straipsnio 3 dalyje įtvirtintą išimtį. Vis dėlto akivaizdu, kad šiuos interesus taip pat padeda užtikrinti apribojimai, kuriuos leidžiama taikyti pagal minėtos direktyvos 15 straipsnio 1 dalį, įskaitant su nacionaliniu saugumu susijusį apribojimą. Pastaroji nuostata būtų nereikalinga, jeigu Direktyva 2002/58 būtų netaikytina tuo atveju, kai remiamasi nacionaliniu saugumu.

2. Sprendimas „Tele2 Sverige ir Watson“

50. Sprendime *Tele2 Sverige ir Watson* buvo nagrinėjamas klausimas, ar Sąjungos teisę atitinka tam tikros nacionalinės sistemos, pagal kurias visuomenei prieinamų elektroninių ryšių paslaugų teikėjams nustatyta bendra pareiga saugoti duomenis, susijusius su tokiais ryšiais. Taigi atvejai iš esmės buvo tapatūs tiems atvejams, kurie nagrinėjami šiuose prašymuose priimti prejudicinį sprendimą.

51. Dar kartą pateikus klausimą dėl Sąjungos teisės taikytinumo (tada jau pagal Direktyvą 2002/58), Teisingumo Teismas iš pradžių nurodė, kad „Direktyvos 2002/58 taikymo srities aprėptį reikia aiškinti atsižvelgiant, be kita ko, į jos bendrą sistemą“ [26].

52. Šiuo požiūriu Teisingumo Teismas pažymėjo, kad „iš tiesų Direktyvos 2002/58 15 straipsnio 1 dalyje numatytos teisinės priemonės susijusios su pačių valstybių ar valstybės valdžios institucijų veikla, kuri nėra privačių asmenų veikla <…>. Be to, tikslai, kuriems įgyvendinti turi būti skirtos tokios priemonės, konkrečiu atveju – nacionalinio saugumo apsauga <…>, iš esmės sutampa su tikslais, kurių siekiama šios direktyvos 1 straipsnio 3 dalyje nurodytomis veiklos rūšimis“ [27].

53. Taigi priemonių, kurias pagal Direktyvos 2002/58 15 straipsnio 1 dalį gali priimti valstybės narės, siekdamos apriboti teisę į privatumą, tikslas šiuo klausimu sutampa su tikslu, pateisinančiu direktyvoje numatytos sistemos netaikymą tam tikrų rūšių valstybės veiklai pagal direktyvos 1 straipsnio 3 dalį.

54. Vis dėlto Teisingumo Teismas nusprendė, kad „atsižvelgiant į bendrą Direktyvos 2002/58 sistemą“ dėl tokios aplinkybės negalima „daryti išvados, kad Direktyvos 2002/58 15 straipsnio 1 dalyje nurodytos teisinės priemonės nepatenka į šios direktyvos taikymo sritį, nes kitu atveju ši nuostata prarastų bet kokį veiksmingumą. Iš tikrųjų minėta nuostata neišvengiamai paremta prielaida, kad joje numatytos nacionalinės priemonės <…> patenka į šios direktyvos taikymo sritį, nes joje aiškiai numatyta, kad valstybės narės gali jas patvirtinti, tik jeigu laikosi joje numatytų sąlygų“ [28].

55. Teisingumo Teismas pridūrė, kad Direktyvos 2002/58 15 straipsnio 1 dalyje leidžiami apribojimai, „siekiant joje numatytų tikslų, reglamentuoja elektroninių ryšių paslaugų teikėjų veiklą“. Vadinasi, šią nuostatą, siejamą su direktyvos 3 straipsniu, „reikia aiškinti taip, kad minėtos teisinės priemonės patenka į šios direktyvos taikymo sritį“ [29].

56. Taigi Teisingumo Teismas pažymėjo, kad į Direktyvos 2002/58 taikymo sritį patenka tiek teisinė priemonė, kuria paslaugų teikėjams nustatoma „pareiga saugoti srauto ir vietos nustatymo duomenis, nes tokia veikla neišvengiamai apima šių teikėjų atliekamą asmens duomenų tvarkymą“ [30], tiek teisinė priemonė, reglamentuojanti valdžios institucijų prieigą prie šių paslaugų teikėjų saugomų duomenų [31].

26 Sprendimo *Tele2 Sverige ir Watson* 67 punktas.

27 Ten pat, 72 punktas.

28 Ten pat, 73 punktas.

29 Ten pat, 74 punktas.

30 Ten pat, 75 punktas.

31 Ten pat, 76 punktas.

57. Sprendime *Tele2 Sverige ir Watson* Teisingumo Teismo pateiktas Direktyvos 2002/58 išaiškinimas pakartotas Sprendime *Ministerio Fiscal*.

58. Ar galima teigti, kad Sprendime *Tele2 Sverige ir Watson* daugiau ar mažiau netiesiogiai nukrypstama nuo Sprendime *Parlamentas / Taryba ir Komisija* įtvirtintos jurisprudencijos? Taip mano, pavyzdžiui, Airijos vyriausybė: ji laikosi nuomonės, kad tik Sprendimas *Parlamentas / Taryba ir Komisija* atitinka Direktyvos 2002/58 teisinį pagrindą ir ESS 4 straipsnio 2 dalį [32].

59. Prancūzijos vyriausybė savo ruožtu mano, kad prieštaravimą būtų galima išspręsti pripažinus, jog Sprendime *Tele2 Sverige ir Watson* įtvirtintoje jurisprudencijoje yra nurodyta valstybių narių veikla baudžiamosios teisės srityje, o Sprendime *Parlamentas / Taryba ir Komisija* suformuota jurisprudencija susijusi su valstybės saugumu ir gynyba. Taigi Sprendime *Tele2 Sverige ir Watson* įtvirtinta jurisprudencija nebūtų taikoma dabar nagrinėjamam atvejui ir šioje byloje reikėtų remtis Sprendimu *Parlamentas / Taryba ir Komisija* [33].

60. Kaip nurodžiau, manau, kad galima rasti būdą darniai taikyti abu sprendimus (kitokį, nei siūlo Prancūzijos vyriausybė). Nepritariu Prancūzijos vyriausybei, nes manau, kad Sprendime *Tele2 Sverige ir Watson* įtvirtintas išvadas, aiškiai susijusias su kova su terorizmu [34], galima plačiai taikyti bet kokiai nacionaliniam saugumui kylančiai grėsmei (terorizmas yra viena iš tokių grėsmių).

3. Galimybė darniai aiškinti Sprendimą „Parlamentas / Taryba ir Komisija“ ir Sprendimą „Tele2 Sverige ir Watson“

61. Manau, kad sprendimuose *Tele2 Sverige ir Watson* ir *Ministerio Fiscal* Teisingumo Teismas atsižvelgė į priežastį, dėl kurios nustatytos išimties ir apribojimo sąlygos, taip pat į sisteminį abiejų rūšių sąlygų santykį.

62. Nors byloje *Parlamentas / Taryba ir Komisija* Teisingumo Teismas tvirtino, kad duomenų tvarkymas nepatenka į Direktyvos 95/46 taikymo sritį, jis taip teigė dėl to, kad, kaip jau minėjau, tipiško tarptautinio Europos Sąjungos ir JAV bendradarbiavimo aplinkybėmis pirmenybę reikėjo teikti nacionaliniam veiklos mastui atsižvelgiant į tai, kad duomenų tvarkymas taip pat apima komercinį ar privatumo aspektą. Vienas iš tuo metu nagrinėtų klausimų būtent buvo tinkamas teisinis nagrinėjamo sprendimo pagrindas.

63. Priešingai, dėl sprendimuose *Tele2 Sverige ir Watson* ir *Ministerio Fiscal* nagrinėjamų nacionalinių priemonių pažymėtina, kad Teisingumo Teismas pirmiausia atsižvelgė į duomenų tvarkymą nacionaliniu mastu: teisės aktai, pagal kuriuos tvarkyti duomenys, buvo vien nacionaliniai, taigi nesusiję su išorės aspektu, kuris būdingas Sprendimo *Parlamentas / Taryba ir Komisija* dalykui.

64. Kadangi duomenų tvarkymo tarptautinio ir nacionalinio aspektų (komercinis ir privatumo aspektai) reikšmė skiriasi, pirmojoje byloje Sąjungos teisėje įtvirtinta išimties sąlyga taikyta kaip tinkamesnė siekiant apsaugoti bendrąjį interesą, t. y. nacionalinį saugumą. Priešingai, antrojoje byloje tą patį interesą buvo galima veiksmingai užtikrinti taikant apribojimo sąlygą, numatytą Direktyvos 2002/58 15 straipsnio 1 dalyje.

65. Reikėtų įvertinti dar ir kitą skirtumą, susijusį su nevienodomis reguliavimo aplinkybėmis: kiekviename iš šių sprendimų daugiausia dėmesio skiriama dviejų nuostatų, kurios skiriasi ne vien išoriniu savo aspektu, aiškinimui.

32 Airijos vyriausybės rašytinių pastabų 15 ir 16 punktai.

33 Prancūzijos vyriausybės rašytinių pastabų 34–50 punktai.

34 Sprendimo *Tele2 Sverige ir Watson* 103 ir 119 punktai.

66. Taigi Sprendime *Parlamentas / Taryba ir Komisija* nuspręsta dėl Direktyvos 95/46 3 straipsnio 2 dalies išaiškinimo, o Sprendimas *Tele2 Sverige ir Watson* priimtas dėl Direktyvos 2002/58 1 straipsnio 3 dalies. Atidžiai skaitant šias nuostatas akivaizdu, kad jos gana skirtingos, siekiant pagrįsti Teisingumo Teismo sprendimų abiejose bylose reikšmę.

67. Direktyvos 95/46 3 straipsnio 2 dalyje numatyta, kad „[š]i direktyva *netaikoma tvarkant asmens duomenis* <…> kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, <…> 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“ [35].

68. Savo ruožtu Direktyvos 2002/58 1 straipsnio 3 dalyje nustatyta, kad ši direktyva „*netaikoma veiklos rūšims*, kurios neįeina į Europos bendrijos steigimo sutarties taikymo sritį, <…> 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“ [36].

69. Direktyvos 95/46 3 straipsnio 2 dalyje nustatyta, kad direktyva netaikoma *duomenų tvarkymui*, susijusiam su valstybės saugumu (kiek tai svarbu nagrinėjamu atveju), o Direktyvos 2002/58 1 straipsnio 3 dalyje numatyta, kad direktyva netaikoma *veiklos rūšims*, kuriomis siekiama apsaugoti valstybės saugumą (kiek tai taip pat svarbu nagrinėjamu atveju).

70. Skirtumas yra nemažas. Direktyvoje 95/46 nustatyta, kad ji netaikoma veiklai („asmens duomenų tvarkymas“), kurią gali vykdyti bet kas. Joje konkrečiai numatyta, kad ši veikla neapima tvarkymo, susijusio, be kita ko, su valstybės saugumu. Vis dėlto duomenis tvarkančio *subjekto* pobūdis buvo nesvarbus. Taigi siekiant nustatyti veiksmus, kuriems direktyva netaikoma, buvo laikomasi teleologinio arba į tikslą nukreipto požiūrio, nedarant skirtumo dėl asmenų kaip veiklos vykdytojų.

71. Darytina išvada, kad byloje *Parlamentas / Taryba ir Komisija* Teisingumo Teismas visų pirma atsižvelgė į tikslą, kurio siekiama tvarkant duomenis. Tai, kad „<…> duomenys komerciniais tikslais buvo surinkti privačių subjektų, organizuojančių jų perdavimą į trečiąją valstybę“, buvo nereikšminga, nes svarbiausia tai, kad „šis perdavimas vyksta pagal valstybės institucijų nustatytą tvarką, susijusią su visuomenės saugumu“ [37].

72. Priešingai, „su valstybės saugumu susijusios veiklos rūšys“, nepatenkančios į byloje *Tele2 Sverige ir Watson* nagrinėtą Direktyvos 2002/58 taikymo sritį, gali būti priskiriamos ne kokiems nors subjektams, o tik pačiai valstybei. Be to, šios veiklos rūšys apima ne valstybės funkcijas, susijusias su teisės aktais ar reguliavimu, o tik faktinius valdžios institucijų veiksmus.

73. Iš tikrųjų Direktyvos 2002/58 1 straipsnio 3 dalyje išvardytos *veiklos rūšys* „visais atvejais priskirtinos valstybės ar valstybės institucijų, o ne privačių subjektų veiklos sritims“ [38]. Vis dėlto šios „veiklos rūšys“ negali būti susijusios su teisės aktų leidimu. Jeigu taip būtų, visos valstybių narių priimtos nuostatos dėl asmens duomenų tvarkymo nepatektų į Direktyvos 2002/58 taikymo sritį, jei būtų siekiama jas pateisinti kaip reikalingas valstybės saugumui užtikrinti.

35 Kursyvu išskirta mano.

36 Kursyvu išskirta mano.

37 Sprendimo *Parlamentas / Taryba ir Komisija* 58 punktas.

38 Sprendimo *Ministerio Fiscal* 32 punktas. Taip pat žr. Sprendimo *Tele2 Sverige ir Watson* 72 punktą.

74. Pirma, tai reikštų, kad ši direktyva iš esmės netektų veiksmingumo, nes vien to, kad būtų remiamasi tokia neapibrėžta teisine sąvoka kaip nacionalinis saugumas, užtektų siekiant valstybėms narėms netaikyti apsaugos priemonių, kurias Sąjungos teisės aktų leidėjas sukūrė, norėdamas apsaugoti piliečių asmens duomenis. Šios apsaugos nebūtų galima įgyvendinti be valstybių narių pagalbos, be to, tokios apsaugos garantija piliečiams taip pat suteikiama nacionalinės valdžios institucijose.

75. Antra, aiškinant, kad sąvoka „valstybės veikla“ apima tokią veiklą, kaip teisės aktų ir teisės nuostatų priėmimas, Direktyvos 2002/58 15 straipsnis netektų prasmės; šiame straipsnyje valstybės narės būtent yra įgaliojamos apsaugos (*inter alia*, nacionalinio saugumo) sumetimais priimti „teisines priemones“, siekiant riboti tam tikrų toje pačioje direktyvoje įtvirtintų teisių ir pareigų taikymą [39].

76. Kaip Teisingumo Teismas pažymėjo byloje *Tele2 Sverige ir Watson*, „Direktyvos 2002/58 taikymo srities aprėptį reikia aiškinti atsižvelgiant, be kita ko, į jos bendrą sistemą“ [40]. Šiuo požiūriu Direktyvos 2002/58 1 straipsnio 3 dalies ir 15 straipsnio 1 dalies aiškinimas, pagal kurį šios dalys įgyja prasmę, neprarasdamos veiksmingumo, yra toks: pirmojoje nuostatoje nustatoma materialinė išimtis, susijusi su valstybių narių vykdoma *veikla* nacionalinio saugumo srityje (ir jai lygiaverte veikla), o antrojoje nuostatoje suteikiamas įgaliojimas priimti *teisines priemones* (t. y. bendrai taikomas teisės normas), kurios, siekiant užtikrinti nacionalinį saugumą, turi poveikį valstybių narių *imperium* pavaldžių asmenų veiklai, ribojant Direktyva 2002/58 užtikrinamas teises.

4. Direktyvoje 2002/58 įtvirtinta išimtis, susijusi su nacionaliniu saugumu

77. Nacionalinis saugumas (arba sinoniminė sąvoka „valstybės saugumas“, pateikta direktyvos 15 straipsnio 1 dalyje) Direktyvoje 2002/58 traktuojamas dvejopai. Pirma, jis yra pagrindas *netaikyti* šios direktyvos tuo atveju, kai vykdoma bet kokia valstybių narių veikla, be kita ko, „susijusi su nacionaliniu saugumu“. Antra, nacionalinis saugumas yra pagrindas *riboti* Direktyvoje 2002/58 nustatytas teises ir pareigas (toks ribojimas turi būti įgyvendinamas pagal įstatymą), t. y. riboti jas tuo atveju, kai vykdoma privataus pobūdžio ar komercinė veikla, nesusijusi su valstybės veiklos sritimis [41].

78. Kokia veikla minima Direktyvos 2002/58 1 straipsnio 3 dalyje? Manau, kad pati *Conseil d'État* (Valstybės Taryba) pateikia gerą pavyzdį, nurodydama Vidaus saugumo kodekso L. 851-5 ir L. 851-6 straipsnius; šiuose straipsniuose minimi „informacijos rinkimo būdai, kuriuos tiesiogiai įgyvendina valstybė, tačiau tuose straipsniuose nereglamentuojama elektroninių ryšių paslaugų teikėjų veikla jiems nustatant specifines pareigas“ [42].

79. Laikausi nuomonės, kad tai yra esminis dalykas siekiant apibrėžti Direktyvos 2002/58 1 straipsnio 3 dalyje numatytą direktyvos netaikymo sritį. Direktyvoje įtvirtinta sistema netaikoma nacionaliniam saugumui apsaugoti skirtai *tam tikrų rūšių veiklai*, kurią savo sąskaita vykdo valdžios institucijos ir kuriai nereikalingas privačių asmenų bendradarbiavimas, todėl šiems asmenims nenustatyta įpareigojimų dėl jų verslo valdymo.

39 Iš tikrųjų būtų sunku teigti, kad Direktyvos 2002/58 15 straipsnio 1 dalyje leidžiama riboti nustatytas teises ir pareigas, patvirtintas srityje, kuri (kaip antai nacionalinio saugumo sritis) iš esmės nepatenka į jos taikymo sritį pagal tos pačios direktyvos 1 straipsnio 3 dalį. Kaip Sprendimo *Tele2 Sverige ir Watson* 73 punkte pažymėjo Teisingumo Teismas, Direktyvos 2002/58 15 straipsnio 1 dalis „neišvengiamai paremta prielaida, kad joje numatytos nacionalinės priemonės <…> patenka į šios direktyvos taikymo sritį, nes joje aiškiai numatyta, kad valstybės narės gali jas patvirtinti, tik jeigu laikosi joje numatytų sąlygų“.

40 Sprendimo *Tele2 Sverige ir Watson* 67 punktas.

41 Kaip savo išvados byloje *Ministerio Fiscal* (C-207/16, EU:C:2018:300) 47 punkte netiesiogiai nurodė generalinis advokatas H. Saugmandsgaard Øe, „negalima painioti, pirma, vykdant su viešosios valdžios funkcijomis susijusią veiklą, t. y. valstybės veiksmus baudžiamosios teisės srityje, *tiesiogiai* tvarkomų asmens duomenų ir, antra, vykdant elektroninių ryšių paslaugų teikėjo komercinio pobūdžio veiklą tvarkomų duomenų, kuriuos *paskui* naudoja kompetentingos valdžios institucijos“.

42 Nutarties dėl prašymo priimti prejudicinį sprendimą byloje C-511/18 18 ir 21 punktai.

80. Vis dėlto valdžios institucijų veiklos rūšių, kurioms netaikoma bendra asmens duomenų tvarkymo sistema, sąrašas turi būti aiškinamas siaurai. Konkrečiai kalbant, negalima išplėsti *nacionalinio saugumo* sąvokos (pagal ESS 4 straipsnio 2 dalį už nacionalinį saugumą išimtinai atsakinga kiekviena valstybė narė) ir ją taikyti kitiems daugiau ar mažiau artimiems visuomeninio gyvenimo sektoriams.

81. Kadangi šiuose prejudiciniuose klausimuose minimas privačių asmenų (t. y. naudotojams elektroninių ryšių paslaugas teikiančių asmenų) dalyvavimas, o ne vien valstybės institucijų veiksmai, nereikia papildomai analizuoti nacionalinio saugumo *stricto sensu* ribų apibrėžimo.

82. Vis dėlto manau, kad kaip gaire galima remtis Pamatiniame sprendime 2006/960/TVR[43] pateiktu kriterijumi: šio sprendimo 2 straipsnio a punkte išskiriamos, pirma, teisėsaugos institucijos plačiąja prasme (jos apima „nacionalin[ę] policij[ą], muitin[ę] ar kit[ą] institucij[ą], kuri pagal nacionalinę teisę yra įgaliota išaiškinti, užkardyti ir tirti teisės pažeidimus ar nusikalstamą veiklą [veiką] ir vykdyti įgaliojimus bei imtis prievartos priemonių tokios veiklos [veikos] atžvilgiu“) ir, antra, „agentūr[os] ar padalini[ai], kurie visų pirma dirba nacionalinio saugumo klausimų srityje“[44].

83. Direktyvos 2002/58 11 konstatuojamojoje dalyje nustatyta, kad ši direktyva, „kaip ir Direktyva 95/46/EB, nenagrinėja pagrindinių teisių ir laisvių apsaugos klausimų, susijusių su veiklos rūšimis, kurių nereglamentuoja [Sąjungos] teisės aktai“. Taigi Direktyva 2002/58 „nekeičia esamos pusiausvyros tarp fizinio asmens teisės į privatumą ir valstybių narių galimybės imtis šios direktyvos 15 straipsnio 1 dalyje nurodytų priemonių, kurių reikia [siekiant] užtikrinti <…> valstybės saugumą <…>“.

84. Iš tikrųjų Direktyva 2002/58 yra Direktyvos 95/46 tęsinys, kiek tai susiję su valstybių narių įgaliojimais nacionalinio saugumo srityje. Nė viena iš šių direktyvų nesusijusi su pagrindinių teisių apsauga šioje konkrečioje srityje, kurioje valstybių narių veiklos „nereglamentuoja [Sąjungos] teisės aktai“.

85. Toje konstatuojamojoje dalyje nurodyta „pusiausvyra“ įtvirtinta dėl to, kad reikia paisyti valstybių narių turimų įgaliojimų nacionalinio saugumo srityje, kai šiuos įgaliojimus jos įgyvendina *tiesiogiai ir savo lėšomis*. Priešingai, kai reikia privačių asmenų, kuriems nustatyti tam tikri įpareigojimai, pagalbos (net ir tais pačiais nacionalinio saugumo sumetimais), ši aplinkybė reiškia, kad patenkama į Sąjungos teisės reglamentuojamą sritį (privatumo apsaugos reikalavimas, taikomas privatiems subjektams).

86. Ir Direktyvoje 95/46, ir Direktyvoje 2002/58 šią pusiausvyrą siekiama užtikrinti leidžiant riboti privačių asmenų teises remiantis reguliavimo priemonėmis, kurias valstybės priėmė atitinkamai pagal šių direktyvų 13 straipsnio 1 dalį ir 15 straipsnio 1 dalį. Šiuo klausimu abi direktyvos niekuo nesiskiria.

87. Dėl Reglamento 2016/679, kuriame įtvirtintas (naujas) bendras asmens duomenų apsaugos pagrindas, pažymėtina, kad jo 2 straipsnio 2 dalyje nustatyta, jog reglamentas netaikomas „asmens duomenų tvarkymui“, kai duomenis tvarko valstybės narės, „vykdydamos veiklą, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius“.

43 2006 m. gruodžio 18 d. Tarybos pamatinis sprendimas dėl keitimosi informacija ir žvalgybos informacija tarp Europos Sąjungos valstybių narių teisėsaugos institucijų supaprastinimo (OL L 386, 2006, p. 89).

44 2008 m. lapkričio 27 d. Tarybos pamatinio sprendimo 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (OL L 350, 2008, p. 60) 1 straipsnio 4 dalyje taip pat numatyta, kad šis sprendimas „nepažeidžia esminių nacionalinio saugumo interesų ar specifinės žvalgybos veiklos nacionalinio saugumo srityje“.

88. Direktyvoje 95/46 asmens duomenų tvarkymas buvo vertinamas atsižvelgiant tik į jo tikslą, o ne į duomenis tvarkantį subjektą; Reglamente 2016/679 atvejai, kuriais reglamentas duomenų tvarkymui netaikomas, nustatyti atsižvelgiant tiek į tvarkymo tikslą, tiek į duomenis tvarkančius subjektus: reglamentas netaikomas tuo atveju, kai valstybės narės duomenis tvarko, vykdydamos *veiklą*, nepatenkančią į Sąjungos teisės taikymo sritį (2 straipsnio 2 dalies a ir b punktai), ir kai institucijos juos tvarko, *siekdamos kovoti su nusikalstamomis veikomis ir apsaugoti* nuo visuomenės saugumui kylančių grėsmių [45].

89. Ši valdžios institucijų veikla būtinai turi būti nustatyta laikantis siauro požiūrio, antraip su privatumo apsauga susiję Sąjungos teisės aktai netektų veiksmingumo. Reglamento 2016/679 23 straipsnyje, kaip ir Direktyvos 2002/58 15 straipsnio 1 dalyje, numatyta apriboti jame nustatytas teises ir pareigas *taikant teisėkūros priemones*, kai to reikia siekiant, be kitų tikslų, apsaugoti nacionalinį saugumą, gynybą arba visuomenės saugumą. Be to, jeigu siekiant nustatyti, kad Reglamentas 2016/679 netaikomas, užtektų šių tikslų apsaugos, nuoroda į nacionalinį saugumą, pateikta pagrindžiant tame reglamente užtikrinamų teisių apribojimą taikant teisėkūros priemones, būtų perteklinė.

90. Kaip ir Direktyvos 2002/58 atveju, būtų nenuoseklu, jei Reglamento 2016/679 23 straipsnyje numatytos teisėkūros priemonės (kartoju, jos leidžia valstybei riboti piliečių teises į privatumą nacionalinio saugumo sumetimais) patektų į šio reglamento taikymo sritį ir jei kartu, užtikrinant nacionalinį saugumą, pats reglamentas taptų nebetaikytinas ir tai reikštų, kad nepripažįstama jokia subjektinė teisė.

B. Sprendimo Tele2 Sverige ir Watson patvirtinimas ir galimybės jį išplėtoti

91. Savo išvadoje byloje C-520/18 atlikau išsamią šios srities Teisingumo Teismo jurisprudencijos analizę [46]; ją atlikęs siūlau patvirtinti šią jurisprudenciją ir kartu rekomenduoju tam tikrą aiškinimo būdą, siekiant patikslinti jos turinį.

92. Remiuosi šia analize ir manau, kad dabar nebūtina jos kartoti vien taupymo sumetimais. Taigi pastabos, kurias pateiksiu dėl *Conseil d'Etat* (Valstybės Taryba) prejudicinių klausimų, turi būti skaitomos atsižvelgiant į atitinkamas išvados byloje C-520/18 dalis.

C. Atsakymas į prejudicinius klausimus

1. Dėl pareigos saugoti duomenis (pirmasis prejudicinis klausimas bylose C-511/18 ir C-512/18 ir antrasis prejudicinis klausimas byloje C-512/18)

93. Dėl pareigos saugoti duomenis, nustatytos elektroninių ryšių paslaugų teikėjams, prašymus priimti prejudicinį sprendimą pateikęs teismas konkrečiai nori išsiaiškinti:

– ar ši pareiga, privaloma pagal Direktyvos 2002/58 15 straipsnio 1 dalį, yra apribojimas, pateisinamas pagal Chartijos 6 straipsnį užtikrinama „teise į saugumą“ ir nacionalinio saugumo reikalavimais (pirmasis klausimas bylose C-511/18 ir C-512/18, taip pat trečiasis klausimas byloje C-511/18),

– ar pagal Direktyvą 2000/31 galima saugoti duomenis, leidžiančius nustatyti asmenų, prisidėjusių kuriant visuomenei internete prieinamą turinį, tapatybę (antrasis klausimas byloje C-512/18).

45 Iš tikrųjų Reglamentas 2016/679 netaikomas duomenų tvarkymui, kai valstybės narės juos tvarko, vykdydamos *veiklą*, nepatenkančią į Sąjungos teisės taikymo sritį, taip pat, kai institucijos duomenis tvarko, *siekdamos apsaugoti* visuomenės saugumą.

46 27–68 punktai.

a) Pirminės pastabos

94. *Conseil d'Etat* (Valstybės Taryba) nurodo pagrindines teises, pripažįstamas Chartijos 7 straipsnyje (teisė į privatų ir šeimos gyvenimą), 8 straipsnyje (asmens duomenų apsauga) ir 11 straipsnyje (saviraiškos ir informacijos laisvė). Iš tikrųjų Teisingumo Teismas mano, kad tokios teisės – tai teisės, kurios galėtų būti pažeistos įgyvendinant pareigą saugoti srauto duomenis, nacionalinių institucijų nustatytą elektroninių ryšių paslaugų teikėjams [47].

95. Prašymus priimti prejudicinį sprendimą pateikęs teismas taip pat mini Chartijos 6 straipsniu saugomą teisę į saugumą. Jis ją mini ne kaip teisę, kuri gali būti pažeista, o kaip veiksnį, dėl kurio gali būti įteisintas tokios pareigos nustatymas.

96. Pritariu Komisijai, kad rėmimasis taip suprantamu 6 straipsniu gali būti dviprasmiškas. Kaip ir Komisija, manau, kad nuostatos nereikia aiškinti kaip leidžiančios „nustatyti Sąjungai pozityvią pareigą priimti priemones, skirtas asmenų apsaugai nuo nusikalstamos veikos" [48].

97. Tame Chartijos straipsnyje užtikrinamas saugumas nėra tapatus visuomenės saugumui arba, galima sakyti, su šiuo saugumu jis susijęs tiek pat, kiek ir bet kuri kita pagrindinė teisė, nes visuomenės saugumas yra būtina sąlyga siekiant naudotis pagrindinėmis teisėmis ir laisvėmis.

98. Komisija primena, kad Chartijos 6 straipsnis atitinka Europos žmogaus teisių konvencijos (toliau – EŽTK) 5 straipsnį, kaip teigiama prie Chartijos pridėtuose išaiškinimuose. Skaitant EŽTK 5 straipsnį akivaizdu, kad jame užtikrinamas „saugumas" yra tik asmens saugumas, suprantamas kaip teisės į fizinę laisvę, apsaugant nuo savavališko laikino sulaikymo ar arešto, garantija, ir galiausiai saugumas, kai niekam laisvė negali būti atimta kitaip, kaip įstatymo nustatytais atvejais ir tvarka, laikantis jame numatytų sąlygų.

99. Taigi yra reglamentuojamas *asmens saugumas*, susijęs su sąlygomis, kuriomis galima apriboti fizinę asmenų laisvę [49], o ne su valstybės egzistavimu susijęs *visuomenės saugumas*, kuris išsivysčiusioje visuomenėje yra būtina sąlyga tam, kad būtų įgyvendinti viešosios valdžios įgaliojimai naudojantis individualiomis teisėmis.

100. Vis dėlto kai kurios vyriausybės prašo labiau atsižvelgti į antrąją teisės į saugumą reikšmę. Iš tikrųjų Teisingumo Teismas į ją atsižvelgė, be to, aiškiai nurodė ją savo sprendimuose [50] ir nuomonėse [51]. Jis niekada neneigė, kad bendrojo intereso tikslai – nacionalinio saugumo ir viešosios tvarkos apsauga [52], kova su tarptautiniu terorizmu palaikant tarptautinę taiką ir saugumą ir kova su sunkiais nusikaltimais siekiant užtikrinti visuomenės saugumą [53] – yra svarbūs; Teisingumo Teismas teisingai juos laikė „pirmaeilės svarbos" [54] tikslais. Anksčiau jis yra pažymėjęs: „be to, užtikrinant visuomenės saugumą prisidedama ir prie kitų asmenų teisių ir laisvių užtikrinimo" [55].

47 Sprendimo *Tele2 Sverige ir Watson* 92 punktas, kuriame pagal analogiją nurodomi Sprendimo *Digital Rights* 25 ir 70 punktai.

48 Komisijos pastabų 37 punktas.

49 Taip aiškina EŽTT. Be kita ko, 2016 m. liepos 5 d. Sprendimas *Buzadji prieš Moldovos Respubliką*, ECHR:2016:0705JUD002375507; jo 84 punkte pažymima, kad svarbiausias EŽTK 5 straipsnyje pripažįstamos teisės tikslas yra užkirsti kelią savavališkam ar nepagrįstam asmens laisvės atėmimui.

50 Sprendimo *Digital Rights* 42 punktas.

51 2017 m. liepos 26 d. Nuomonės Nr. 1/15 dėl ES ir Kanados susitarimo dėl PNR (toliau – Nuomonė Nr. 1/15, EU:C:2017:592) 149 punktas ir jame nurodyta jurisprudencija.

52 2016 m. vasario 15 d. Sprendimo *N.* (C-601/15 PPU, EU:C:2016:84) 53 punktas.

53 Sprendimo *Digital Rights* 42 punktas ir jame nurodyta jurisprudencija.

54 Ten pat, 51 punktas.

55 Nuomonės Nr. 1/15 149 punktas.

101. Galima pasinaudoti proga, kurią suteikia šie prašymai priimti prejudicinį sprendimą, ir aiškiau pasiūlyti, kaip užtikrinti, pirma, teisės į saugumą ir, antra, teisės į privatumą ir teisės į asmens duomenų apsaugą pusiausvyrą. Taip būtų išvengta kritikos, kad pastarosios teisės yra remiamos kenkiant teisei į saugumą.

102. Manau, kad ši pusiausvyra yra minima Direktyvos 2002/58 11 konstatuojamojoje dalyje ir 15 straipsnio 1 dalyje, kalbant apie priemonių būtinumo ir proporcingumo sąlygas *demokratinėje visuomenėje*. Teisė į saugumą, kartoju, yra neatskiriamas paties demokratijos egzistavimo ir išlikimo veiksnys, todėl pagrįstai turi būti visapusiškai atsižvelgiama į aplinkybes, kuriomis vertinamas toks proporcingumas. Kitaip tariant, jei demokratinėje visuomenėje labai svarbu laikytis duomenų konfidencialumo principo, tai taip pat neturi būti nuvertinta šios visuomenės saugumo svarba.

103. Taigi reikia atsižvelgti į aplinkybes, kuriomis patiriama didelių ir nuolatinių grėsmių nacionaliniam saugumui, visų pirma patiriama terorizmo rizika, kaip nurodyta Sprendimo *Tele2 Sverige ir Watson* 119 punkto paskutiniame sakinyje. Taikant nacionalinę sistemą galima proporcingai reaguoti į patiriamų grėsmių pobūdį ir intensyvumą, o ši reakcija nebūtinai turi būti tokia pati kaip kitų valstybių narių.

104. Galiausiai turiu pridurti, kad susidarius visiškai *išimtinėms* situacijoms, kai patiriama didelė grėsmė arba labai didelė rizika ir dėl to valstybėje narėje pagrįstai oficialiai paskelbiama nepaprastoji padėtis, pirmesnės pastabos netrukdo nacionalinės teisės aktuose numatyti galimybę ribotą laikotarpį taikyti tokią plačią ir bendrą pareigą saugoti duomenis, kokia, kaip manoma, yra būtina [56].

105. Taigi pirmąjį abiejuose prašymuose priimti prejudicinį sprendimą suformuluotą klausimą reikėtų performuluoti, labiau orientuojantis į galimybę teisės apribojimą pateisinti nacionalinio saugumo motyvais. Vadinasi, abejonių kiltų dėl to, ar elektroninių ryšių paslaugų teikėjams nustatyta pareiga atitinka Direktyvos 2002/58 15 straipsnio 1 dalį.

b) Vertinimas

1) Nacionalinės teisės normų, nurodytų abiejuose prašymuose priimti prejudicinį sprendimą, apibūdinimas atsižvelgiant į Teisingumo Teismo jurisprudenciją

106. Atsižvelgiant į nutartis dėl prašymo priimti prejudicinį sprendimą, pagrindinėse bylose pagal nagrinėjamus teisės aktus duomenis privalo saugoti:

– elektroninių ryšių operatoriai, visų pirma operatoriai, kurie teikia visuomenei ryšių paslaugas internetu,

– fiziniai ar juridiniai asmenys, kurie užtikrina, net ir nemokamai, internetu teikiant visuomenei ryšių paslaugas šių paslaugų gavėjų pateiktų signalų, rašytinės medžiagos, garso, vaizdo ar kokio pobūdžio pranešimų saugojimą [57].

107. Operatoriai vienus metus nuo duomenų įregistravimo dienos turi saugoti informaciją, leidžiančią nustatyti naudotojo tapatybę, duomenis apie naudojamus galinius ryšių įrenginius, informaciją apie kiekvieno ryšio technines savybes, datą, laiką ir trukmę, duomenis apie prašytas arba naudotas papildomas paslaugas ir jų teikėjus, taip pat duomenis, leidžiančius nustatyti ryšių adresato tapatybę, ir, jei vykdoma telefonijos veikla, duomenis, padedančius nustatyti ryšio šaltinį ir vietą [58].

56 Žr. mano išvados byloje C-520/18 105–107 punktus.

57 Tai nurodyta Vidaus saugumo kodekso L. 851-1 straipsnyje, kuriame pateikiama nuoroda į Pašto ir elektroninių ryšių kodekso L. 34-1 straipsnį ir Įstatymo Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika 6 straipsnį.

58 Tai nurodyta Pašto ir elektroninių ryšių kodekso R. 10-13 straipsnyje.

108. Visų pirma kalbant apie prieigos prie interneto ir saugojimo paslaugas, atrodo, kad nacionalinės teisės aktuose yra reikalaujama saugoti IP adresus [59], slaptažodžius ir, jeigu pasirašoma sutartis arba naudojamasi mokėjimo sąskaita, atlikto mokėjimo tipą, taip pat jo numerį, sumą, sandorio dieną ir laiką [60].

109. Pareigos saugoti duomenis reikalaujama laikytis tam, kad būtų atskleistos ir ištirtos nusikalstamos veikos ir vykdomas persekiojimas dėl jų [61]. Tai reiškia, kad, kaip bus įrodyta, pareigos *saugoti duomenis* tikslas nėra vien terorizmo prevencija, priešingai nei pareigos *rinkti* srauto ir vietos nustatymo duomenis [62].

110. Dėl *prieigos* prie saugomų duomenų sąlygų pažymėtina, kad remiantis nutartyse pateikta informacija darytina išvada, jog šios sąlygos yra numatytos taikyti pagal bendrą sistemą (teisminės institucijos dalyvavimas) arba tokia prieiga suteikiama tik individualiai paskirtiems ir įgaliotiems pareigūnams, prieš tai gavus ministro pirmininko leidimą, išduotą remiantis neprivaloma nepriklausomos administracinės institucijos nuomone [63].

111. Lengva pastebėti, kad, kaip pažymėjo Komisija [64], duomenys, kuriuos saugoti reikalaujama pagal nacionalinės teisės aktus, iš esmės atitinka Teisingumo Teismo sprendimuose *Digital Rights* ir *Tele2 Sverige ir Watson* [65] nagrinėtus duomenis. Kaip ir tada, taikoma „pareiga bendrai ir nediferencijuojant saugoti“ šiuos duomenis – taip savo prejudicinių klausimų pradžioje visiškai atvirai nurodo *Conseil d'État* (Valstybės Taryba).

112. Jeigu taip yra (tai galiausiai turi įvertinti prašymus priimti prejudicinį sprendimą pateikęs teismas), galima tik padaryti išvadą, kad nagrinėjamais teisės aktais yra ribojamos „Chartijos 7 ir 8 straipsniuose įtvirtint[os] pagrindin[ės] teis[ės] <…> [ir šis apribojimas] yra plataus masto ir laikytinas itin rimtu“ [66].

113. Nė vienai proceso šaliai nekilo abejonių dėl to, kad šios teisės tokio pobūdžio teisės aktais yra ribojamos. Dabar šio klausimo nagrinėti nereikia, net ir norint priminti, kad šių teisių pažeidimas neišvengiamai kenkia patiems visuomenės, siekiančios gerbti, be kitų vertybių, Chartijos saugomą asmens privatumą, pagrindams.

114. Taikant Sprendimu *Tele2 Sverige ir Watson* suformuotą jurisprudenciją, patvirtintą Sprendime *Ministerio Fiscal*, natūraliai reikėtų teigti, kad šioje byloje nagrinėjami teisės aktai „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 Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi“ [67].

59 Šį aspektą turi patikrinti prašymus priimti prejudicinį sprendimą pateikęs teismas; per teismo posėdį nuomonės dėl jo išsiskyrė.

60 Dekreto 2011-219 1 straipsnis.

61 Pašto ir elektroninių ryšių kodekso R. 10-13 straipsnis.

62 Ir *La Quadrature du Net*, ir *Fédération des founisseurs d'accès à Internet associatifs* pabrėžia, kad tikslai, dėl kurių renkami duomenys, yra platūs, institucijos naudojasi diskrecija ir nėra objektyvių kriterijų duomenų saugojimui apibrėžti, taip pat pabrėžia tam tikrų formų nusikalstamai veikai, kurios negalima laikyti sunkia, teikiamą reikšmę.

63 *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija). Šiuo klausimu žr. Prancūzijos vyriausybės pastabų 145–148 punktus.

64 Komisijos pastabų 60 punktas.

65 Iš tikrųjų duomenų yra šiek tiek daugiau, nes, regis, prieigos prie interneto paslaugų atveju taip pat numatyta saugoti IP adresus ar slaptažodžius.

66 Sprendimo *Tele2 Sverige ir Watson* 100 punktas.

67 Ten pat, 107 punktas.

115. Iš tikrųjų kaip ir Sprendime *Tele2 Sverige ir Watson* analizuoti teisės aktai, šioje byloje nagrinėjami teisės aktai „bendrai apima visus abonentus ir registruotus naudotojus, bet kokias elektroninio ryšio priemones ir visus srauto <…> duomenis [ir] nenumato jokio skirtumo, apribojimo arba išimties atsižvelgiant į siekiamą tikslą“ [68]. Taigi „jie taikomi net tiems asmenims, dėl kurių neegzistuoja jokių požymių, leidžiančių manyti, kad jų elgesys gali turėti bent netiesioginį ar tolimą ryšį su sunkiais nusikaltimais“, ir juose neleidžiamos jokios išimtys, „taigi jie taikomi net tiems asmenims, kurių komunikacija pagal nacionalinę teisę pripažįstama profesine paslaptimi“ [69].

116. Be to, nagrinėjamuose teisės aktuose „nereikalaujama jokios sąsajos tarp numatytų saugoti duomenų ir grėsmės visuomenės saugumui. Visų pirma, juose nenustatyta, kad saugomi tik tie duomenys, kurie susiję su tam tikru laikotarpiu ir (arba) geografine zona, ir (arba) asmenų, kurie, vienaip ar kitaip, galėtų būti siejami su vienu iš sunkių nusikaltimų, ratu arba asmenimis, kurių duomenų saugojimas dėl kitų priežasčių galėtų prisidėti prie kovos su nusikalstamumu“ [70].

117. Atsižvelgiant į tai darytina išvada, kad šie teisės aktai „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 Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi“ [71].

118. To, kas pirma išdėstyta, užteko, kad Teisingumo Teismas padarytų išvadą, jog atitinkamos nacionalinės teisės normos neatitinka Direktyvos 2002/58 15 straipsnio 1 dalies, nes jose „kovos su nusikalstamumu tikslais numatyta pareiga bendrai nediferencijuojant saugoti visus su visais abonentais ir registruotais naudotojais susijusius srauto ir vietos nustatymo duomenis, perduodamus bet kokia elektroninio ryšio priemone“ [72].

119. Dabar kyla klausimas, ar Teisingumo Teismo jurisprudencija dėl asmens duomenų saugojimo gali būti jei ne persvarstyta, tai bent patikslinta tuo atveju, kai tikslas, kurio siekiama „bendrai ir nediferencijuotai“ saugant šiuos duomenis, yra kova su terorizmu. Pirmasis klausimas byloje C-511/18 suformuluotas būtent nurodant „tok[ias] aplinkyb[es], kai nacionaliniam saugumui keliama rimta nuolatinė grėsmė, ypač susijusi su terorizmo pavojumi“.

120. Vis dėlto šios *aplinkybės*, kuriomis taikoma pareiga saugoti duomenis, yra *faktinės* ir akivaizdu, kad, *reglamentuojant* jas *teisės aktuose*, atsižvelgiama ne tik į terorizmą. Pagal duomenų saugojimo ir prieigos prie jų sistemą, kurią byloje nagrinėja *Conseil d'État* (Valstybės Taryba), tokia pareiga taikoma siekiant apskritai atskleisti ir ištirti nusikalstamas veikas ir vykdyti persekiojimą dėl jų.

121. Bet kuriuo atveju primenu, kad kova su terorizmu buvo paminėta Sprendime *Tele2 Sverige ir Watson* pateiktuose argumentuose; tada Teisingumo Teismas nemanė, kad dėl šios nusikalstamos veikos reikės padaryti kokių nors jo jurisprudencijos pakeitimų [73].

122. Taigi iš esmės manau, kad į prašymus priimti prejudicinį sprendimą pateikusio teismo klausimą, kuriame akcentuojama konkreti terorizmo grėsmė, reikėtų atsakyti taip, kaip nuspręsta Teisingumo Teismo sprendime *Tele2 Sverige ir Watson*.

68 Ten pat, 105 punktas.

69 *Loc. ult. cit.*

70 Sprendimo *Tele2 Sverige ir Watson* 106 punktas.

71 Ten pat, 107 punktas.

72 Ten pat, 112 punktas.

73 Ten pat, 103 punktas.

123. Kaip pažymėjau išvadoje byloje *Stichting Brein*, „[t]eisės taikymo tikrumas nereikalauja, kad teismai taikytų *stare decisis* tiesiogine prasme, bet jie turi būti atidūs ir laikytis to, ką patys nusprendė, po daugybės apmąstymų apie konkrečią teisinę problemą“ [74].

2) Ribotas duomenų saugojimas atsižvelgiant į grėsmes nacionaliniam saugumui, įskaitant terorizmą

124. Ar vis dėlto būtų galima patikslinti arba papildyti šią jurisprudenciją, atsižvelgiant į jos pasekmes siekiant kovoti su terorizmu ar apsaugoti valstybę nuo kitų panašių grėsmių nacionaliniam saugumui?

125. Jau esu pabrėžęs, kad vien asmens duomenų saugojimas reiškia, jog pagal Chartijos 7, 8 ir 11 straipsnius užtikrinamos teisės yra ribojamos [75]. Nepaisant to, kad tokiu saugojimu galiausiai siekiama suteikti galimybę tam tikru momentu gauti *prieigą* prie praeityje ar šiuo metu gautų duomenų [76], vien saugant duomenis, kurie viršija tai, kas griežtai būtina siekiant perduoti informaciją arba pateikti sąskaitą už paslaugų teikėjo suteiktas paslaugas, nesilaikoma Direktyvos 2002/58 5 ir 6 straipsniuose numatytų apribojimų.

126. Šių paslaugų naudotojai (iš tikrųjų beveik visi labiausiai išsivysčiusių visuomenių piliečiai) turi ar privalo turėti teisėtų lūkesčių, kad jeigu jie neduos sutikimo, nebus saugoma daugiau jų duomenų, negu jau saugoma pagal tokias nuostatas. Direktyvos 2002/58 15 straipsnio 1 dalyje numatytos išimtys turi būti aiškinamos remiantis šia prielaida.

127. Kaip jau paaiškinau, Teisingumo Teismas, taip pat atsižvelgdamas į kovą su terorizmu, Sprendime *Tele2 Sverige ir Watson* paneigė, kad asmens duomenys gali būti saugomi bendrai ir nediferencijuojant [77].

128. Atsižvelgdamas į pateiktą kritiką nemanau, kad šiuo sprendimu įtvirtintoje jurisprudencijoje nuvertinama grėsmė, kurią kelia terorizmas, kaip labai sunkaus nusikalstamumo forma, apimanti aiškų tikslą priešintis valstybės autoritetui ir destabilizuoti ar naikinti jos institucijas. Kova su terorizmu valstybei iš esmės yra gyvybiškai svarbi, o sėkmė šioje kovoje – tai teisinės valstybės bendrojo intereso tikslas, kurio negalima atsisakyti.

129. Beveik visos vyriausybės, kurios dalyvauja procese, taip pat Komisija laikėsi tos pačios nuomonės, kad dėl dalinio ir diferencijuoto asmens duomenų saugojimo ne tik kiltų techninių sunkumų, bet ir nacionalinės žvalgybos tarnybos netektų galimybės gauti informacijos, būtinos siekiant nustatyti grėsmes visuomenės saugumui ir valstybės gynybai, taip pat patraukti atsakomybėn teroristinių išpuolių vykdytojus [78].

74 Byla C-527/15, EU:C:2016:938, 41 punktas.

75 Kaip Teisingumo Teismas dar kartą priminė Nuomonės Nr. 1/15 124 punkte, „asmens duomenų perdavimas trečiajam asmeniui, kaip antai valdžios institucijai, yra Chartijos 7 straipsnyje įtvirtintos pagrindinės teisės apribojimas, nesvarbu, kaip perduoda informacija bus naudojama vėliau. Tas pats taikytina asmens duomenų saugojimui ir prieigai prie jų, kai juos siekia panaudoti valdžios institucijos. Šiuo klausimu pažymėtina, kad nelabai svarbu, ar atitinkama su privačiu gyvenimu susijusi informacija yra ypatingo pobūdžio ir ar dėl šio apribojimo suinteresuotieji asmenys galbūt patyrė nepatogumų“.

76 Kaip pažymėjo generalinis advokatas P. Cruz Villalón savo išvados byloje *Digital Rights*, C-293/12 ir C-594/12 (EU:C:2013:845) 72 punkte, „rinkimas, ypač saugojimas milžiniškose duomenų bazėse, daugybės duomenų, kurie generuojami arba tvarkomi Sąjungos piliečiams naudojantis dauguma įprastinių elektroninio ryšio priemonių, yra akivaizdus jų privataus gyvenimo apribojimas, net jei toks rinkimas ir saugojimas sudaro sąlygas patikrinti tik praeityje vykdytą asmeninę ir profesinę veiklą. Tokių duomenų rinkimas sudaro sąlygas stebėti ir nors toks stebėjimas nukreiptas tik į praeityje vykusį duomenų naudojimą, visą šių duomenų saugojimo laikotarpį Sąjungos piliečių teisei į jų privataus gyvenimo slaptumą išlieka nuolatinė grėsmė. Dėl sukeliamo nepaaiškinamo pojūčio, jog yra stebima, tokioje situacijoje ypač svarbus tampa duomenų saugojimo laikotarpio klausimas“.

77 Sprendimo *Tele2 Sverige ir Watson* 103 punktas: „[bendrojo intereso tikslas] <…> negali pateisinti to, kad nacionalinės teisės aktai, kuriuose numatyta pareiga bendrai nediferencijuojant saugoti visus srauto ir vietos nustatymo duomenis, būtų laikomi būtinais tokios kovos tikslams pasiekti“.

78 Pavyzdžiui, taip aiškina Prancūzijos vyriausybė, kuri šį teiginį iliustruoja konkrečiais pavyzdžiais, rodančiais, kad bendras duomenų saugojimas yra naudingas – toks saugojimas leido valstybei reaguoti į sunkius teroristinius išpuolius, Prancūzijoje patirtus per pastaruosius kelerius metus (Prancūzijos vyriausybės pastabų 107 ir 122–126 punktai).

130. Atsižvelgdamas į šį vertinimą manau, kad reikia atkreipti dėmesį į tai, jog kova su terorizmu neturi būti nagrinėjama galvojant tik apie jos veiksmingumą. Taigi kova su terorizmu yra sunki, tačiau taip pat plataus masto, nes jos priemonės ir būdai derinami su teisinės valstybės reikalavimais, t. y. visų pirma valdžios institucijoms ir jėgos struktūroms taikomais apribojimais, įtvirtintais teisėje, ypač teisine tvarka, kurios buvimo priežastis ir tikslas yra pagrindinių teisių apsauga.

131. Jei terorizmo atveju teroristinės priemonės pateisinamos atsižvelgiant tik į vieną kriterijų – vien (didžiausią) nustatytos tvarkos pažeidimų veiksmingumą, teisinės valstybės atveju efektyvumas vertinamas netoleruojant to, kad ginant teisinę valstybę nepaisoma procedūrų ir garantijų, dėl kurių tos valstybės tvarka laikoma teisėta. Atsižvelgiant vien į efektyvumą ir į nieką daugiau, teisinė valstybė netektų išskirtinės savybės ir kraštutiniais atvejais pati galėtų tapti grėsme piliečiams. Niekas negalėtų užtikrinti, kad valdžios institucijoms suteikus pernelyg plačių priemonių, skirtų persekioti dėl nusikalstamos veikos, kurias taikydamos jos galėtų nepaisyti pagrindinių teisių ar jas paneigti, nekontroliuojami ir visiškai laisvai vykdomi jų veiksmai galiausiai nepakenktų visų laisvei.

132. Kartoju, piliečių pagrindinės teisės – tai kliūtis, kurios negalima peržengti užtikrinant valdžios institucijų efektyvumą; kaip nustatyta Chartijos 52 straipsnio 1 dalyje, šių teisių apribojimai gali būti įtvirtinti tik įstatyme ir negali keisti šių teisių esmės, „kai jie būtini ir tikrai atitinka Sąjungos pripažintus bendrojo intereso tikslus arba reikalingi tam, kad būtų apsaugotos kitų asmenų teisės ir laisvės“ [79].

133. Kalbėdamas apie sąlygas, kuriomis pagal Sprendimą *Tele2 Sverige ir Watson* leidžiamas *tikslinis* duomenų saugojimas, remiuosi savo išvada byloje C-520/18 [80].

134. Aplinkybės, kuriomis teisėsaugos institucijų turima informacija leidžia patvirtinti pagrįstą įtarimą, kad rengiamasi įvykdyti teroristinį išpuolį, gali būti teisėtas atvejis, kai taikoma pareiga saugoti tam tikrus duomenis. Juo labiau toks atvejis gali būti tada, kai iš tikrųjų įvykdomas išpuolis. Jeigu pastaruoju atveju vien nusikalstamos veikos įvykdymas gali būti veiksnys, pateisinantis tam tikros priemonės priėmimą, vien esant įtarimui, kad gali būti įvykdytas išpuolis, reikėtų, kad atsižvelgiant į šį įtarimą pagrindžiančias aplinkybes toks išpuolis būtų minimaliai tikėtinas – tai būtina siekiant objektyviai įvertinti požymius, galinčius pagrįsti šį įtarimą.

135. Nors sunku, tačiau nėra neįmanoma tiksliai ir pagal objektyvius kriterijus nustatyti tiek duomenų, kurių saugojimas laikomas būtinu, kategorijas, tiek duomenų subjektų ratą. Žinoma, *praktiškiausia* ir *veiksmingiausia* būtų bendrai ir nediferencijuojant saugoti visus duomenis, kuriuos gali rinkti elektroninių ryšių paslaugų teikėjai, tačiau jau nurodžiau, kad klausimas nagrinėtinas atsižvelgiant ne į *praktinį efektyvumą*, o į *teisinę galią*, taip pat į aplinkybes, susijusias su teisine valstybe.

136. Ši nustatymo veikla yra tipiška teisėkūros veikla, vykdoma laikantis Teisingumo Teismo jurisprudencijoje numatytų ribų. Dar kartą remiuosi savo pastabomis, kurios šiuo klausimu pateikiamos mano išvadoje byloje C-520/18 [81].

79 2016 m. vasario 15 d. Sprendimo *N.* (C-601/15 PPU, EU:C:2016:84) 50 punktas. Taigi sunku užtikrinti viešosios tvarkos ir laisvės pusiausvyrą, kurią jau nurodžiau ir kurios iš esmės siekiama visais Sąjungos teisės aktais. Kaip pavyzdį galima paminėti 2017 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvą (ES) 2017/541 dėl kovos su terorizmu, pakeičiančią Tarybos pamatinį sprendimą 2002/475/TVR ir iš dalies keičiančią Tarybos sprendimą 2005/671/TVR (OL L 88, 2017, p. 6). Šios direktyvos 20 straipsnio 1 dalyje įtvirtinta, jog valstybės narės turi užtikrinti, kad už teroristinių nusikaltimų tyrimą ar baudžiamąjį persekiojimą dėl jų atsakingi subjektai „galėtų naudotis veiksmingomis tyrimo priemonėmis“, o 21 konstatuojamojoje dalyje numatyta, kad tokių veiksmingų priemonių naudojimas „turėtų būti tikslingas, jas taikant turėtų būti atsižvelgiama į proporcingumo principą bei tiriamų nusikalstamų veikų pobūdį bei sunkumą ir turėtų būti gerbiama teisė į asmens duomenų apsaugą“.

80 87–95 punktai.

81 100–107 punktai.

3) Prieiga prie saugomų duomenų

137. Kaip prielaida remiantis tuo, kad operatoriai duomenis surinko laikydamiesi Direktyvos 2002/58 nuostatų ir kad šie duomenys buvo saugomi pagal jos 15 straipsnio 1 dalį[82], prieiga prie šios informacijos kompetentingoms institucijoms turi būti suteikiama tomis sąlygomis, kurių reikalavo Teisingumo Teismas ir kurias išnagrinėjau byloje C-520/18 pateiktoje išvadoje (šia išvada remiuosi)[83].

138. Taigi šiuo atveju nacionalinės teisės aktuose taip pat turi būti numatytos materialinės ir procedūrinės sąlygos, reglamentuojančios kompetentingų nacionalinių institucijų prieigą prie saugomų duomenų[84]. Atsižvelgiant į šių prašymų priimti prejudicinį sprendimą aplinkybes, tokios sąlygos leistų suteikti prieigą prie asmenų, kurie įtariami planuojantys teroro aktą, jį darantys arba padarę, arba dalyvavę jį darant, duomenų[85].

139. Atsižvelgiant į visa tai iš esmės būtina, kad prieš suteikiant prieigą prie atitinkamų duomenų, išskyrus tinkamai pagrįstus skubos atvejus, teismas arba nepriklausoma administracinė institucija atliktų išankstinę kontrolę ir toks teismas ar tokia institucija savo sprendimą priimtų gavę motyvuotą kompetentingų institucijų prašymą[86]. Taigi tuo atveju, kai negalima priimti abstraktaus sprendimo dėl teisės akto, garantuojama, kad būtų priimtas šios nepriklausomos institucijos, taip pat įpareigotos užtikrinti nacionalinį saugumą ir ginti pagrindines piliečių teises, sprendimas *in concreto*.

4) Pareiga saugoti duomenis, leidžiančius nustatyti turinio autorių tapatybę, remiantis Direktyva 2000/31 (antrasis prejudicinis klausimas byloje C-512/18)

140. Prašymus priimti prejudicinį sprendimą pateikęs teismas Direktyvą 2000/31 nurodo kaip atskaitos tašką, siekiant nustatyti, ar galima tam tikrus asmenis[87] ir operatorius, kurie teikia ryšių paslaugas visuomenei, įpareigoti saugoti duomenis, „leidžiančius nustatyti asmenis, dalyvavusius kuriant jų teikiamų paslaugų turinį, kad prireikus teisminė institucija galėtų iš jų pareikalauti perduoti šiuos duomenis, siekdama užtikrinti, kad būtų laikomasi civilinę ar baudžiamąją atsakomybę reglamentuojančių nuostatų“.

141. Pritariu Komisijai, kad nereikia nagrinėti šios pareigos atitikties Direktyvai 2000/31[88], nes jos 1 straipsnio 5 dalies b punkte nustatyta, kad ji netaikoma „sprendžiant klausimus, susijusius su informacinės visuomenės paslaugomis, kurias reglamentuoja [d]irektyvos 95/46/EB ir 97/66/EB“ – teisės aktai, dabar atitinkantys Reglamentą 2006/679 ir Direktyvą 2002/58[89], kurių atitinkamos nuostatos (23 straipsnio 1 dalis ir 15 straipsnio 1 dalis), mano nuomone, turi būti aiškinamos taip, kaip išdėstyta pirma.

82 Žinoma, jeigu laikomasi sąlygų, nurodytų Sprendimo *Tele2 Sverige ir Watson* 122 punkte: Teisingumo Teismas priminė, kad Direktyvos 2002/58 15 straipsnio 1 dalyje nesuteikiama galimybė nukrypti nuo šios direktyvos 4 straipsnio 1 ir 1a dalių, kuriose reikalaujama, kad paslaugų teikėjai imtųsi priemonių, siekdami užtikrinti saugomų duomenų apsaugą nuo piktnaudžiavimo pavojaus ir neteisėtos prieigos prie šių duomenų. Šiuo klausimu Teisingumo Teismas pripažino, kad, „[a]tsižvelgiant į saugomų duomenų kiekį, jautrų tokių duomenų pobūdį ir neteisėtos prieigos prie jų pavojų, elektroninių ryšių paslaugų teikėjai privalo užtikrinti itin aukštą apsaugos ir saugumo lygį, imdamiesi tinkamų techninių ir organizacinių priemonių, siekdami garantuoti visišką tokių duomenų integralumą ir konfidencialumą. Konkrečiai kalbant, nacionalinės teisės aktuose turi būti numatyta, kad duomenys saugomi Sąjungos teritorijoje ir kad jie neatkuriamai sunaikinami pasibaigus jų saugojimo terminui“.

83 52–60 punktai.

84 Sprendimo *Tele2 Sverige ir Watson* 118 punktas.

85 Ten pat, 119 punktas.

86 Ten pat, 120 punktas.

87 Asmenys, kurie „užtikrina <…> internetu teikiant visuomenei ryšių paslaugas šių paslaugų gavėjų pateiktų signalų, rašytinės medžiagos, vaizdo, garso ar bet kokio pobūdžio pranešimų saugojimą“.

88 Prašymus priimti prejudicinį sprendimą pateikęs teismas šią direktyvą bendrai nurodo antrajame klausime, pateiktame byloje C-512/18, neišskirdamas jokios konkrečios jos nuostatos.

89 Komisijos pastabų 112 ir 113 punktai.

2. Dėl pareigos realiuoju laiku rinkti srauto ir vietos nustatymo duomenis (antrasis prejudicinis klausimas byloje C-511/18)

142. Prašymus priimti prejudicinį sprendimą pateikęs teismas mano, kad Vidaus saugumo kodekso L. 851-2 straipsnyje leidžiama išimtinai terorizmo prevencijos tikslais realiuoju laiku rinkti informaciją apie asmenis, kurie prieš tai identifikuoti kaip keliantys terorizmo grėsmę. Šio kodekso L. 851-4 straipsnyje operatoriams taip pat leidžiama realiuoju laiku perduoti techninius duomenis apie galinių įrenginių vietą.

143. Prašymus priimti prejudicinį sprendimą pateikęs teismas teigia, kad dėl šių metodų paslaugų teikėjams nenustatyta papildoma pareiga saugoti duomenis, palyginti su tuo, kas reikalinga sąskaitoms už jų paslaugas pateikti ir šių paslaugų rinkodarai vykdyti.

144. Be to, pagal Vidaus saugumo kodekso L.851-3 straipsnį elektroninių ryšių operatoriai ir techninių paslaugų teikėjai gali būti įpareigoti „savo tinkluose automatizuotomis priemonėmis tvarkyti duomenis tam, kad atsižvelgiant į leidime apibrėžtus parametrus būtų nustatomi prisijungimai, galintys kelti terorizmo grėsmę“. Taikant šį informacijos rinkimo būdą, duomenys nėra saugomi bendrai ir nediferencijuojant ir siekiama ribotą laikotarpį rinkti tuos prisijungimo duomenis, kurie gali būti susiję su teroristinio pobūdžio nusikalstama veika.

145. Laikausi nuomonės, kad sąlygos, kurių reikalaujama laikytis siekiant gauti prieigą prie saugomų asmens duomenų, taip pat turi būti taikomos realiuoju laiku suteikiamai prieigai prie duomenų, generuojamų naudojantis elektroniniais ryšiais. Taigi remiuosi tuo, kas šiuo klausimu yra išdėstyta. Nesvarbu tai, ar duomenys yra saugomi, ar ką tik gauti, nes abiem atvejais asmens duomenys sužinomi ir nesvarbu, ar jie gauti anksčiau, ar dabar.

146. Konkrečiai kalbant, jeigu prieiga realiuoju laiku būtų suteikiama prisijungus ir tas prisijungimas nustatomas taikant automatizuotas duomenų tvarkymo priemones, kaip įtvirtinta Vidaus saugumo kodekso L. 851-3 straipsnyje, turi būti iš anksto nustatyti konkretūs, patikimi ir nediskriminaciniai šio duomenų tvarkymo modeliai ir kriterijai, kad juos taikant būtų galima lengvai nustatyti asmenis, pagrįstai įtariamus dalyvavus vykdant teroristinę veiką [90].

3. Dėl pareigos informuoti duomenų subjektus (trečiasis prejudicinis klausimas byloje C-511/18)

147. Teisingumo Teismas patvirtino, kad institucijos, kurioms suteikiama prieiga prie duomenų, turi apie tai informuoti duomenų subjektus, jeigu dėl to nebus pakenkta atliekamiems tyrimams. Ši pareiga motyvuojama aplinkybe, kad tokia informacija reikalinga tam, kad tie asmenys galėtų pasinaudoti teise į veiksmingą teisinę gynybą, aiškiai numatyta Direktyvos 2002/58 15 straipsnio 2 dalyje, tuo atveju, kai pažeidžiamos jų teisės [91].

148. *Conseil d'État* (Valstybės Taryba) byloje C-511/18 pateiktu trečiuoju klausimu nori išsiaiškinti, ar šis reikalavimas informuoti bet kuriuo atveju yra neišvengiamas, ar jo galima netaikyti, kai yra numatyta kitų garantijų, kaip antai aprašytų jos nutartyje dėl prašymo priimti prejudicinį sprendimą.

149. Kaip nurodė prašymus priimti prejudicinį sprendimą pateikęs teismas [92], minimos garantijos – tai asmenims, kurie nori patikrinti, ar buvo neteisėtai įgyvendintas koks nors informacijos rinkimo būdas, suteikiama galimybė kreiptis į pačią *Conseil d'État* (Valstybės Taryba). Ši institucija prireikus gali panaikinti leidimą taikyti priemonę ir nurodyti sunaikinti surinktą informaciją, vykdydama procedūrą, pagal kurią netaikomas teismo procesams įprastas rungimosi principas.

90 Sprendimo *Digital Rights* 59 punktas.

91 Sprendimo *Tele2 Sverige ir Watson* 121 punktas.

92 Nutarties dėl prašymo priimti prejudicinį sprendimą 8–11 punktai.

150. Prašymus priimti prejudicinį sprendimą pateikęs teismas mano, kad šiomis teisės normomis teisė į veiksmingą teisinę gynybą nepažeidžiama. Vis dėlto laikausi nuomonės, kad teoriškai ji galėtų būti pažeista tuo atveju, kai asmenys nusprendžia patikrinti, ar dėl jų vykdoma žvalgybos operacija. Priešingai, minėtos teisės nepaisoma, jei asmenims, dėl kurių buvo ar yra vykdoma tokia operacija, nepranešama apie šią aplinkybę, todėl jie net negali prašyti išnagrinėti, ar jų teisės buvo pažeistos.

151. Atrodo, kad prašymus priimti prejudicinį sprendimą pateikusio teismo nurodytos teisminės garantijos priklauso nuo to, ar asmenys, įtariantys, kad buvo renkama informacija apie juos, imasi iniciatyvos. Vis dėlto teisė kreiptis į teismą siekiant apginti savo teises turi būti veiksminga visiems, todėl asmenys, kurių asmens duomenys buvo tvarkomi, privalo turėti galimybę teisme užginčyti tokio tvarkymo teisėtumą, taigi jiems turi būti pranešta apie šį tvarkymą.

152. Žinoma, kaip matyti iš pateiktos informacijos, procesą teisme galima pradėti *ex officio* arba remiantis administraciniu skundu, tačiau bet kuriuo atveju duomenų subjektui turi būti suteikiama galimybė pačiam jį pradėti, todėl reikia jį informuoti apie tai, kad buvo vykdomas tam tikras jo asmens duomenų tvarkymas. Negalima remtis tuo, kad šio asmens teisės bus apgintos gavus žinių apie tokį tvarkymą iš trečiųjų asmenų arba iš savo šaltinių.

153. Taigi duomenų subjektui turi būti pranešama apie suteiktą prieigą prie saugomų duomenų, jeigu tai nepakenks tyrimų, dėl kurių suteikta tokia prieiga, eigai.

154. Kitaip yra tuo atveju, kai duomenų subjektą informavus apie prieigą prie jo duomenų ir jam pradėjus procesą teisme, vėliau teismo procesas vykdomas laikantis konfidencialumo ir slaptumo reikalavimų, susijusių su tuo, kad tikrinami valdžios institucijų veiksmai tokiose jautriose srityse, kaip nacionalinis saugumas ir valstybės gynyba. Vis dėlto tas klausimas nesusijęs su šiais prašymais priimti prejudicinį sprendimą, todėl manau, kad Teisingumo Teismas neturi jo nagrinėti.

V. Išvada

155. Atsižvelgdamas į tai, kas išdėstyta, siūlau Teisingumo Teismui *Conseil d'État* (Valstybės Taryba, Prancūzija) pateikti tokį atsakymą:

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) 15 straipsnio 1 dalis, siejama su Europos Sąjungos pagrindinių teisių chartijos 7, 8 bei 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją:

1) draudžiamos nacionalinės teisės normos, kuriose tokiomis aplinkybėmis, kai nacionaliniam saugumui keliama rimta nuolatinė grėsmė, ypač susijusi su terorizmo pavojumi, elektroninių ryšių paslaugų teikėjams ir operatoriams numatyta pareiga bendrai ir nediferencijuojant saugoti visų abonentų srauto ir vietos nustatymo duomenis, taip pat duomenis, leidžiančius nustatyti turinio, kurį siūlo šių paslaugų teikėjai, kūrėjų tapatybę;

2) draudžiamos nacionalinės teisės normos, kuriose nenumatyta pareiga informuoti duomenų subjektus apie tai, kad kompetentingos institucijos tvarko jų asmens duomenis, išskyrus atvejus, kai dėl šio informavimo kyla pavojus minėtų institucijų veiksmams;

3) nedraudžiamos nacionalinės teisės normos, kuriose leidžiama realiuoju laiku rinkti pavienių asmenų srauto ir vietos nustatymo duomenis, jeigu šie veiksmai atliekami laikantis nustatytos tvarkos, susijusios su prieiga prie teisėtai saugomų asmens duomenų, ir suteikiant tas pačias garantijas.