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

Byla C-623/17

Privacy International
prieš
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

(*Investigatory Powers Tribunal* (Tyrimo įgaliojimų teismas, Jungtinė Karalystė) prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį Sprendimą – Asmens duomenų tvarkymas ir privatumo apsauga elektroninių ryšių sektoriuje – Direktyva 2002/58/EB – Taikymo sritis – 1 straipsnio 3 dalis – 15 straipsnio 3 dalis – Europos Sąjungos pagrindinių teisių chartija – 7, 8 ir 51 straipsniai bei 52 straipsnio 1 dalis – ESS 4 straipsnio 2 dalis – Bendras ir nediferencijuotas elektroninių ryšių paslaugos vartotojų prisijungimo duomenų perdavimas saugumo tarnyboms“

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]; jame Teisingumo Teismas pripažino, kad Direktyva 2006/24/EB[3] negalioja, nes dėl jos galėjo būti neproporcingai ribojamos Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose įtvirtintos 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; toliau – Sprendimas *Digital Rights*, EU:C:2014:238.

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; toliau – Sprendimas *Tele2 Sverige ir Watson*, EU:C:2016:970.

5 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002, p. 37; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 514).

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

2. Šie sprendimai (visų pirma antrasis) kelia tam tikrų valstybių narių institucijų susirūpinimą, nes jos mano, kad juos taikydamos netenka priemonės, kurią laiko būtina siekiant apsaugoti nacionalinį saugumą ir kovoti su terorizmu. Taigi kai kurios valstybės narės prašo panaikinti arba patikslinti tą jurisprudenciją.

3. Tam tikri valstybių narių teismai tokį patį susirūpinimą išreiškė keturiuose prašymuose priimti prejuducinį sprendimą[7]; dėl šių prašymų savo išvadas 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 ta direktyva būtų taikoma, reikėtų išsiaiškinti, kokiu mastu valstybės narės gali riboti direktyvos saugomas teises į privatumą. Galiausiai reikia išnagrinėti, kiek su šia sritimi susijusiuose įvairiuose nacionalinės teisės aktuose (Jungtinės Karalystės[8], Belgijos[9] ir Prancūzijos[10]) atsižvelgiama į Sąjungos teisę, kaip ją aiškino Teisingumo Teismas.

I. Teisinis pagrindas

A. Sąjungos teisė

5. Darau nuorodą į atitinkamą savo išvados bylose C-511 ir C-512/18 punktą.

B. Nacionalinė teisė (taikoma pagrindinėje byloje)

1. Telecommunications Act 1984[11]

6. Pagal šio įstatymo 94 straipsnį valstybės sekretorius viešojo elektroninių ryšių tinklo operatoriui gali duoti bendrų ar konkrečių nurodymų, kuriuos laiko būtinais siekiant užtikrinti nacionalinį saugumą arba palaikyti ryšius su šalies ar teritorijos, esančios už Jungtinės Karalystės ribų, vyriausybe.

2. Data Retention and Investigatory Powers Act 2014[12]

7. 1 straipsnyje nustatyta:

„1. Valstybės sekretorius, pateikęs nurodymą saugoti duomenis, gali reikalauti iš viešųjų telekomunikacijų operatoriaus saugoti atitinkamus ryšių duomenis, jei mano, kad toks reikalavimas būtinas ir proporcingas atsižvelgiant į vieną ar kelis *Regulation of Investigatory Powers Act 2000* [(2000 m. Įstatymas dėl tyrimo įgaliojimų reglamentavimo; toliau – RIPA)] 22 straipsnio 2 dalies a–h punktuose nurodytus tikslus.

2. Nurodyme saugoti duomenis gali būti:

a) minimas konkretus operatorius arba visų tipų operatoriai;

7 Be šios bylos, Bylos *La Quadrature du Net ir kt.*, C-511/18 ir C-512/18 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 Byla *La Quadrature du Net ir kt.*, C-511/18 ir C-512/18.

11 1984 m. Telekomunikacijų įstatymas; toliau – 1984 m. įstatymas.

12 2014 m. Įstatymas dėl duomenų saugojimo ir tyrimo įgaliojimų; toliau – DRIPA.

b) reikalaujama saugoti visus duomenis arba visų kategorijų duomenis;

c) nustatomas (-i) laikotarpis (-iai), per kurį (-iuos) reikia saugoti duomenis;

d) nustatomi kiti reikalavimai ar apribojimai dėl duomenų saugojimo;

e) numatomos įvairios nuostatos įvairiais tikslais;

f) nurodomi duomenys, kurie yra arba kurių nėra nurodymo saugoti duomenis priėmimo ar įsigaliojimo dieną.

3. Valstybės sekretorius reglamentu gali įtvirtinti daugiau nuostatų dėl atitinkamų duomenų, susijusių su ryšiais, saugojimo.

4. Šios nuostatos visų pirma gali būti susijusios su:

a) reikalavimais, nustatytais prieš priimant nurodymą saugoti duomenis;

b) ilgiausiu laikotarpiu, per kurį duomenys turi būti saugomi pagal nurodymą saugoti duomenis;

c) nurodymo saugoti duomenis turiniu, priėmimu, įsigaliojimu, peržiūra, pakeitimu ar panaikinimu;

d) pagal šį straipsnį saugomų duomenų išsamumu, saugumu ar apsauga, prieiga prie duomenų, taip pat duomenų platinimu ar sunaikinimu;

e) atitinkamų reikalavimų ar apribojimų laikymusi ar atitikties šiems reikalavimams ir apribojimams patikra;

f) gerosios praktikos, susijusios su reikalavimais, apribojimais ar atitinkamais įgaliojimais, kodeksu;

g) kompensacija, kurią valstybės sekretorius tam tikromis sąlygomis (arba nesant tokių sąlygų) skiria viešųjų telekomunikacijų operatorių išlaidoms, patirtoms siekiant įgyvendinti atitinkamus reikalavimus ar apribojimus, padengti;

<…>

5. Taikant 4 straipsnio b punktą nustatytas ilgiausias laikotarpis neturi viršyti 12 mėnesių, skaičiuojant nuo dienos, nurodytos dėl duomenų, kuriems taikytini 3 dalyje minimi reglamentai.

6. Taikant šį straipsnį, atitinkamus su ryšiais susijusius duomenis saugantis viešųjų telekomunikacijų operatorius negali perduoti šių duomenų, išskyrus atvejus, kai:

a) juos perduoda pagal:

   i) [RIPA] 2 skyriaus 1 dalį arba

   ii) teismo Sprendimą ar bet kurį kitą teismo leidimą ar įgaliojimą; arba

b) toks perdavimas numatytas 3 dalyje minimuose reglamentuose.

7. Valstybės sekretorius gali reglamentu priimti nuostatas dėl bet kurių taikant 4 dalies d–g punktus arba 6 dalį priimtų nuostatų (arba nuostatų, kurias galima priimti) dėl duomenų, susijusių su pranešimais, kuriuos telekomunikacijų paslaugų teikėjai saugo, taikydami gerosios praktikos kodeksą pagal *Anti-terrorism, Crime and Security Act 2001* (2001 m. Įstatymas dėl kovos su terorizmu, nusikalstamumo ir saugumo) 102 straipsnį.“

3. RIPA

8. 21 straipsnyje įtvirtinta:

„<…>

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

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

b) bet kokia informacija, kuri neapima jokio pranešimo turinio [išskyrus informaciją, patenkančią į a punkto taikymo sritį] ir yra susijusi su tuo, kad bet kuris asmuo naudojosi:

   i) bet kokiomis pašto ar telekomunikacijų paslaugomis arba

   ii) bet kuria telekomunikacijų sistemos dalimi, kiek tai susiję su telekomunikacijų paslaugos teikimu arba tuo, kad asmuo naudojosi tokia paslauga;

c) visa į a arba b punktų taikymo sritį nepatenkanti informacija, susijusi su paslaugos gavėjais, kurią turi arba gauna pašto arba telekomunikacijų paslaugas teikiantis asmuo.

<…>

6. Šiame skirsnyje sąvoka „srauto duomenys“, susijusi su bet kokiu pranešimu, apima:

a) visus duomenis, padedančius arba galinčius padėti atpažinti bet kurį asmenį, aparatą ar buvimo vietą, į kurią ar iš kurios yra arba gali būti perduotas pranešimas;

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

c) visus duomenis, apimančius aparato, kuris ryšių sistemoje naudojamas siekiant perduoti bet kokius pranešimus, įjungimo signalus;

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

<…>“

9. 22 straipsnyje nustatyta:

„1. Šis straipsnis taikomas, kai pagal šį skyrių atsakingas asmuo mano, kad dėl šio straipsnio 2 dalyje išvardytų priežasčių reikia gauti visus ryšių duomenis.

2. Dėl šioje dalyje išvardytų priežasčių ryšių duomenis reikia gauti, jeigu jie būtini:

a) nacionaliniam saugumui užtikrinti;

b) siekiant vykdyti nusikalstamumo prevenciją ar nustatyti nusikalstamas veikas arba užkirsti kelią viešosios tvarkos trikdymui;

c) siekiant Jungtinės Karalystės ekonominės gerovės, jei tai taip pat svarbu nacionaliniam saugumui;

d) visuomenės saugumui užtikrinti;

e) visuomenės sveikatos apsaugai;

f) siekiant įvertinti bet kokių mokesčių, teisių, rinkliavų ar kitokių įpareigojimų, įmokų ar prievolių, atsiradusių dėl viešojo administravimo, nustatymą ar surinkimą;

g) skubos atvejais siekiant užkirsti kelią fizinių asmenų mirčiai, sužalojimui ar bet kokiai žalai jų fizinei ar psichinei sveikatai arba siekiant sušvelninti bet kokį fizinio asmens sužalojimą ar jo fizinei ar psichinei sveikatai daromą žalą;

h) siekiant bet kurio kito [a–g punktuose neminimo] tikslo, nustatyto pagal [DRIPA] 22 straipsnio 2 dalies h punktą valstybės sekretoriaus pateiktame nurodyme.

4. Pagal 5 dalį atsakingas asmuo, manantis, kad telekomunikacijų arba pašto operatorius turi, galėtų turėti arba galėtų turėti galimybę turėti duomenų, gali pareikalauti, kad telekomunikacijų arba pašto operatorius:

a) gautų duomenis, jei dar jų neturi, ir

b) bet kuriuo atveju atskleistų turimus arba vėliau gautus duomenis.

5. Atsakingas asmuo neturi duoti leidimo pagal 3 dalį arba pateikti reikalavimo pagal 4 dalį, nebent mano, kad atitinkamų duomenų gavimas, imantis leidžiamų ar reikalaujamų veiksmų pagal leidimą arba reikalavimą, yra proporcingas tikslui, kurio siekiama tokių duomenų gavimu.“

10. 65 straipsnyje nustatyta, kad jei yra priežasčių manyti, jog duomenys buvo gauti netinkamai, galima kreiptis į *Investigatory Powers Tribunal* (Tyrimo įgaliojimų teismas, Jungtinė Karalystė).

II. Faktinės aplinkybės ir prejudiciniai klausimai

11. *A quo* teismas teigia, kad pagrindinė byla susijusi su *United Kingdom Security and Intelligence Agencies* (Jungtinės Karalystės saugumo ir žvalgybos tarnybos; toliau – SŽT) gaunamais ir naudojamais masiniais ryšių duomenimis.

12. Šie duomenys apima informaciją, „kas, kada, kur, kaip ir su kuo“ kalbėjosi telefonu ir naudojosi internetu, įskaitant mobiliojo ir fiksuoto ryšio telefonų, iš kurių skambinama ar į kuriuos skambinama, ir kompiuterių, iš kurių prisijungiama prie interneto, buvimo vietą. Jie neapima šių ryšių turinio, kurį galima gauti tik teismo nutartimi.

13. Ieškovė pagrindinėje byloje (nevyriausybinė žmogaus teisių organizacija *Privacy International*) pateikė ieškinį prašymą priimti prejudicinį Sprendimą pateikusiam teismui, nes mano, kad dėl to, jog SŽT gauna ir naudoja minėtus duomenis, pažeidžiama teisė į privataus gyvenimo gerbimą, įtvirtinta Europos žmogaus teisių konvencijos (toliau – EŽTK) 8 straipsnyje, ir Sąjungos teisė.

14. Valdžios institucijos (atsakovės)[13] teigia, kad jos savo įgaliojimais šioje srityje naudojasi teisėtai ir kad tai visų pirma būtina nacionaliniam saugumui užtikrinti.

15. Pagal nutartyje dėl prašymo priimti prejudicinį Sprendimą pateiktą informaciją, remiantis valstybės sekretoriaus nurodymais, pateiktais pagal 1984 m. Įstatymo 94 straipsnį, SŽT masinius ryšių duomenis gauna iš elektroninių ryšių viešųjų tinklų operatorių.

16. Šie duomenys apima srauto ir buvimo vietos duomenis, taip pat informaciją apie naudotojų socialinę, komercinę ir finansinę veiklą, ryšius ir keliones. Gavusios šiuos duomenis SŽT juos laiko saugiai, taikydamos metodus (pvz., filtravimą ir sutapčių ieškojimą), kurie nėra tiksliniai, t. y. nėra nukreipti į konkrečius ir žinomus taikinius.

17. Prašymą priimti prejudicinį Sprendimą pateikęs teismas yra įsitikinęs, kad šie metodai labai svarbūs SŽT darbui, kuriuo siekiama užkirsti kelią rimtoms grėsmėms visuomenės saugumui, visų pirma kovos su terorizmu, šnipinėjimu ir branduolinių ginklų platinimu srityse. Tai, kad SŽT turi galimybę rinkti ir naudoti duomenis, yra labai svarbu Jungtinės Karalystės nacionalinio saugumo apsaugai.

18. Prašymą priimti prejudicinį Sprendimą pateikęs teismas mano, kad nagrinėjamos priemonės atitinka nacionalinę teisę ir EŽTK 8 straipsnį. Vis dėlto atsižvelgdamas į Sprendimą *Tele2 Sverige ir Watson* jis abejoja dėl šių priemonių suderinamumo su Sąjungos teise.

19. Tokiomis aplinkybėmis minėtas teismas teikia Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar, atsižvelgiant į ESS 4 straipsnį ir Direktyvos 2002/58/EB <…> 1 straipsnio 3 dalį, *Secretary of State* (valstybės sekretorius) įpareigojimas nurodyti elektroninių ryšių tinklo paslaugų teikėjui, kad jis turi teikti masinius ryšių duomenis valstybės narės saugumo ir žvalgybos tarnyboms (SŽT), patenka į Sąjungos teisės ir Direktyvos [2002/58] taikymo sritį?

2. Jei atsakymas į pirmąjį klausimą yra teigiamas, ar kuris nors iš Sprendimo *Watson* reikalavimų[14] arba bet kokie kiti reikalavimai, be nustatytųjų EŽTK, taikomi tokiam *Secretary of State* nurodymui? O jei taip, kaip ir kiek šie reikalavimai taikomi, atsižvelgiant į SŽT būtinybę naudoti masinio duomenų gavimo ir automatizuoto tvarkymo metodus norint apsaugoti nacionalinį saugumą, ir kiek tokioms galimybėms, jeigu jos atitinka EŽTK, galima iš esmės sukliudyti nustatant tokius reikalavimus?“

20. Prašymą priimti prejudicinį Sprendimą pateikęs teismas nurodo tokias aplinkybes, kuriomis pateikti jo klausimai:

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

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

13 T. y. *Secretary of State for Foreign and Commonwealth Affairs* (Valstybės užsienio ir sandraugos reikalų sekretorius), *Secretary of State for the Home Department* (Valstybės vidaus reikalų sekretorius) ir trys Jungtinės Karalystės SŽT, t y. *Government Communications Headquarters* (Vyriausybės ryšių žvalgybos centras; GCHQ), *Security Service* (Saugumo tarnyba; MI5) ir *Secret Intelligence Service* (Slaptoji žvalgybos tarnyba; MI6).

14 *Id est*, Sprendime *Tele2 Sverige ir Watson* įtvirtinta jurisprudencija.

c) elektroninių ryšių tinklų paslaugų teikėjai neprivalo saugoti minėtų duomenų (ilgiau, nei to reikalaujama pagal įprastas veiklos taisykles) ir juos saugo tik valstybė (SŽT);

d) nacionalinis teismas nustatė (taikydamas tam tikras išlygas), kad garantijos, susijusios su tuo, kaip SŽT naudoja [šiuos duomenis], atitinka EŽTK reikalavimus;

e) nacionalinis teismas pripažino, kad Sprendime [*Tele2 Sverige ir Watson*] sukonkretintų reikalavimų, jeigu jie būtų taikomi, nustatymas pakenktų priemonėms, kurių SŽT ėmėsi nacionaliniam saugumui užtikrinti, ir taip kiltų grėsmė Jungtinės Karalystės nacionaliniam saugumui.“

III. Procesas Teisingumo Teisme

21. Prašymas priimti prejudicinį Sprendimą Teisingumo Teismo kanceliarijoje užregistruotas 2017 m. spalio 31 d.

22. Rašytines pastabas pateikė Vokietijos, Belgijos, Jungtinės Karalystės, Čekijos, Kipro, Ispanijos, Estijos, Prancūzijos, Vengrijos, Airijos, Latvijos, Nyderlandų, Norvegijos, Lenkijos, Portugalijos ir Švedijos vyriausybės bei Komisija.

23. 2019 m. rugsėjo 9 d. buvo surengtas viešas teismo posėdis (kartu su teismo posėdžiais bylose C-511/18, C-512/18 ir C-520/18); jame dalyvavo bylų, susijusių su keturiais prašymais priimti prejudicinį sprendimą, šalys, pirma minėtų vyriausybių, taip pat Komisijos atstovai ir Europos asmens duomenų apsaugos priežiūros pareigūnas.

IV. Analizė

A. Dėl Direktyvos 2002/58 taikymo srities ir jos netaikymo nacionaliniam saugumui (pirmasis prejudicinis klausimas)

24. Išvadoje, kurią tą pačią dieną pateikiau bylose C-511/18 ir C-512/18, paaiškinu priežastis, kodėl manau, kad 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“ [15].

25. Išplėsdamas savo argumentus, nagrinėju 2006 m. gegužės 30 d. Teisingumo Teismo Sprendimo *Parlamentas / Taryba ir Komisija* [16] ir Sprendimo *Tele2 Sverige ir Watson* poveikį ir siūlau juos abu aiškinti darniai [17].

26. Toje pačioje išvadoje patvirtinęs, kad Direktyva 2002/58 taikytina, nagrinėju nacionalinio saugumo neįtraukimą į jos taikymo sritį, kaip nustatyta toje direktyvoje, ir ESS 4 straipsnio 2 dalies poveikį [18].

27. Atsižvelgdamas į tai, kas išdėstyta toliau, darau nuorodą į minėtoje išvadoje ir išvadoje byloje C-520/18 pateiktas pastabas.

15 Išvados bylose C-511/18 ir C-512/18 42 punktas.

16 Bylos C-317/04 ir C-318/04, EU:C:2006:346.

17 Išvados bylose C-511/18 ir C-512/18 44–76 punktai.

18 Ten pat, 77–90 punktai.

1. Direktyvos 2002/58 taikymas šioje byloje

28. Šioje byloje nagrinėjamose teisės normose elektroninių ryšių paslaugų teikėjams nustatytas įpareigojimas, pagal kurį jie turi ne tik saugoti duomenis, gaunamus teikiant paslaugas Sąjungos viešųjų ryšių tinklų naudotojams, bet ir juos tvarkyti [19].

29. Iš tiesų minėti operatoriai privalo perduoti šiuos duomenis SŽT. Taigi kyla klausimas, ar pagal Direktyvos 2002/58 15 straipsnio 1 dalį leidžiama šiam perdavimui netaikyti Sąjungos teisės, atsižvelgiant į perdavimo tikslą.

30. Manau, kad taip nėra. Nurodytų duomenų saugojimas ir jų paskesnis perdavimas gali būti laikomi elektroninių telekomunikacijų paslaugų teikėjų vykdomu asmens duomenų tvarkymu, todėl savaime suprantama, kad šios operacijos patenka į Direktyvos 2002/58 taikymo sritį.

31. Su nacionaliniu saugumu susijusios priežastys negali būti nurodytos kaip pagrindas šiam faktui paneigti, kaip siūlo prašymą priimti prejudicinį Sprendimą pateikęs teismas, taigi nagrinėjamas įpareigojimas nepatenka į Sąjungos teisės taikymo sritį. Manau, kad, kartoju, paslaugų teikėjai privalo tvarkyti duomenis, teikdami elektroninių ryšių paslaugas, prieinamas Sąjungos viešuosiuose ryšių tinkluose, o tai patenka į Direktyvos 2002/58 taikymo sritį, kaip nustatyta jos 3 straipsnio 1 dalyje.

32. Remiantis šia prielaida, ginčas kyla ne dėl SŽT veiklos (kaip pažymėjau pirma, ši veikla galėtų nepatekti į Sąjungos teisės taikymo sritį, jei nedarytų poveikio elektroninių ryšių operatoriams), o dėl šių operatorių turimų duomenų saugojimo ir paskesnio perdavimo. Laikantis tokio požiūrio, nagrinėjamu atveju kalbama apie Sąjungos užtikrinamas pagrindines teises.

33. Siekiant išspręsti šį ginčą, svarbiausia yra pareiga bendrai ir nediferencijuotai saugoti duomenis, su kuriais gali susipažinti valdžios institucijos.

2. Rėmimasis nacionaliniu saugumu

34. Kadangi šioje byloje prašymą priimti prejudicinį Sprendimą pateikęs teismas visų pirma pabrėžia SŽT veiklą, susijusią su nacionaliniu saugumu, šiuo klausimu pakartoju kai kuriuos savo tą pačią dieną pateiktos išvados bylose C-511/18 ir C-512/18 punktus:

„77. Nacionalinis saugumas <…> 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.

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“. <…>

19 Pagal Direktyvos 2002/58 2 straipsnį šioje direktyvoje vartojamos sąvokos yra apibrėžiamos taip, kaip apibrėžta Direktyvoje 95/46. Direktyvos 95/46 2 straipsnio b punkte nustatyta, kad „asmens duomenų tvarkymas“ – tai „bet kur[i] operacij[a] ar operacijų rinkin[ys], automatiniais arba neautomatiniais būdais atliekam[i] su asmens duomenimis, kaip antai: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, *atskleidimas perduodant*, platinant ar kitu *būdu padarant juos prieinamus*, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimas ar naikinimas“ (pasviruoju šriftu išskirta mano).

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.

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.

<…>

82. <…> manau, kad kaip gaire galima remtis Pamatiniame Sprendime 2006/960/TVR <…> 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“ <…>

<…>

84. <…> 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. [Direktyvos 2002/58 11] konstatuojamoje 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.

<…>

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.“

3. Sprendimo „Tele2 Sverige ir Watson“ taikymo šioje byloje pasekmės

35. Prašymą priimti prejudicinį Sprendimą pateikęs teismas daugiausia dėmesio skyrė Teisingumo Teismo aiškinimui, pateiktam Sprendime *Tele2 Sverige ir Watson*; jis išdėstė sunkumus, kurių, kaip jis mano, kiltų taikant šį aiškinimą nagrinėjamoje byloje.

36. Sprendime *Tele2 Sverige ir Watson* iš tiesų nurodytos sąlygos, kurias turi atitikti nacionalinės teisės aktai, įpareigojantys saugoti srauto ir vietos nustatymo duomenis, kad valdžios institucijos vėliau turėtų prieigą prie jų.

37. Kaip ir bylose C-511/18 bei C-512/18, dėl panašių priežasčių manau, kad nacionalinės teisės normos, dėl kurių pateiktas šis prašymas priimti prejudicinį sprendimą, neatitinka Sprendime *Tele2 Sverige ir Watson* nustatytų sąlygų, nes pagal jas asmens duomenys saugotini bendrai ir nediferencijuotai, todėl suteikiama galimybė ilgą laikotarpį gauti išsamių duomenų apie atitinkamų asmenų gyvenimą.

38. Šiose dviejose bylose pateiktoje išvadoje keliu klausimą, ar būtų įmanoma patikslinti arba papildyti minėtame Sprendime įtvirtintą jurisprudenciją, atsižvelgiant į jos pasekmes kovai su terorizmu ar saugant valstybę nuo kitų panašių grėsmių nacionaliniam saugumui.

39. Toliau taip pat norėčiau pakartoti kelis minėtos išvados punktus, kuriuose iš esmės teigiu, kad, atsižvelgiant į tai, jog nurodytą jurisprudenciją galima patikslinti, ją reikia iš esmės patvirtinti:

„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. <…>

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 <…>, 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).

138. Taigi šiuo atveju nacionalinės teisės aktuose taip pat turi būti numatytos materialinės ir procedūrinės sąlygos, reglamentuojančios kompetentingų nacionalinių institucijų prieigą prie saugomų duomenų <…>. 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 <…>.

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 <…>. 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*.“

B. Dėl antrojo prejudicinio klausimo

40. Prašymą priimti prejudicinį Sprendimą pateikęs teismas antrąjį savo klausimą kelia tuo atveju, jei atsakymas į pirmąjį būtų teigiamas. Tokiu atveju jis norėtų žinoti, „kokie kiti reikalavimai, be nustatytųjų EŽTK“ ar minimų Sprendime *Tele2 Sverige ir Watson*, turėtų būti taikomi.

41. Šiuo klausimu jis teigia, kad įpareigojimas laikytis Sprendime *Tele2 Sverige ir Watson* nustatytų sąlygų „pakenktų priemonėms, kurių SŽT ėmėsi nacionaliniam saugumui užtikrinti“.

42. Kadangi į pirmąjį klausimą siūlau atsakyti neigiamai, antrojo klausimo nagrinėti nebūtina. Kaip pažymi pats prašymą priimti prejudicinį Sprendimą pateikęs teismas, į antrąjį klausimą reikėtų atsakyti tik tada, jei visų Jungtinės Karalystės naudotojų asmens duomenų, kuriuos elektroninių ryšių paslaugų operatoriai turėtų perduoti SŽT, „masinio duomenų gavimo ir automatizuoto tvarkymo metodai“ būtų pripažintini atitinkančiais Sąjungos teisę.

43. Jei Teisingumo Teismas nuspręstų, kad į antrąjį klausimą atsakyti būtina, manau, jis turėtų patvirtinti minėtas Sprendime *Tele2 Sverige ir Watson* nustatytas sąlygas, kiek tai susiję su:

– netikslinės prieigos prie duomenų uždraudimu,

– būtinybe gauti išankstinį teismo ar nepriklausomos valdžios institucijos leidimą siekiant įteisinti šią prieigą,

– įpareigojimu apie tai informuoti atitinkamus asmenis, nebent taip būtų pakenkta priemonės veiksmingumui,

– duomenų saugojimu Sąjungoje.

44. Manau, kad, kartoju, dėl priežasčių, kurias išdėsčiau išvadoje bylose C-511/18, C-512/18 ir C-520/18, pakaktų patvirtinti šias privalomai taikytinas sąlygas ir nereikia nustatyti „kitų“ papildomų sąlygų, kaip jas supranta prašymą priimti prejudicinį Sprendimą pateikęs teismas.

V. Išvada

45. Atsižvelgdamas į tai, kas išdėstyta, siūlau Teisingumo Teismui taip atsakyti *Investigatory Powers Tribunal* (Tyrimo įgaliojimų teismas, Jungtinė Karalystė):

ESS 4 straipsnis ir 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) 1 straipsnio 3 dalis turi būti aiškinami taip, kad pagal juos draudžiami nacionalinės teisės aktai, kuriuose elektroninių ryšių tinklo paslaugų teikėjams nustatytas įpareigojimas teikti valstybės narės saugumo ir žvalgybos tarnyboms „masinius ryšių duomenis“, prieš tai surinktus bendrai ir nediferencijuotai.

Papildomai siūlau atsakyti taip:

Valstybės narės saugumo ir žvalgybos tarnybų prieiga prie duomenų, kuriuos perduoda elektroninių ryšių tinklo paslaugų teikėjai, privalo atitikti sąlygas, nustatytas 2016 m. gruodžio 21 d. Sprendime *Tele2 Sverige ir Watson* (C-203/15 ir C-698/15, EU:C:2016:970).