Teismo praktikos rinkinys

GENERALINIO ADVOKATO
MANUEL CAMPOS SÁNCHEZ-BORDONA IŠVADA,
pateikta 2023 m. balandžio 20 d.[1]

Byla C-548/21

C. G.
prieš
Bezirkshauptmannschaft Landeck

(*Landesverwaltungsgericht Tirol* (Tirolio apygardos administracinis teismas, Austrija) prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Telekomunikacijos – Asmens duomenų apsauga – Direktyva (ES) 2016/680 – Baudžiamasis procesas – Valdžios institucijų bandymas gauti prieigą prie mobiliajame telefone įrašytų duomenų neturint teismo ar nepriklausomos administracinės institucijos leidimo“

1. Šis prašymas priimti prejudicinį sprendimą iš esmės pateiktas dėl sąlygų, kurias turi atitikti policijos institucijos, norėdamos gauti prieigą prie asmens, kurio atžvilgiu vykdomas nusikalstamos veikos tyrimas, mobiliajame telefone saugomų duomenų.

2. Kaip pabandysiu paaiškinti toliau, prašymas priimti prejudicinį sprendimą turi didelių trūkumų, susijusių su jo priimtinumu. Jeigu Teisingumo Teismas vis dėlto nuspręstų nagrinėti bylą iš esmės, jis turės priimti sprendimą dėl atitinkamų Direktyvos 2002/58/EB[2] ir Direktyvos (ES) 2016/680[3] taikymo sričių.

1 Originalo kalba: ispanų.

2 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).

3 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuri[a] panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89).

I. Teisinis pagrindas

A. Sąjungos teisė

1. Reglamentas (ES) 2016/679[4]

3. 2 straipsnio („Materialinė taikymo sritis“) 2 dalyje nurodyta:

„Šis reglamentas netaikomas asmens duomenų tvarkymui, kai:

<…>

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.“

2. Direktyva 2016/680

4. 2 konstatuojamojoje dalyje numatyta:

„[F]izinių asmenų apsaugos tvarkant jų asmens duomenis principais ir taisyklėmis turėtų būti gerbiamos asmenų pagrindinės teisės ir laisvės, visų pirma jų teisė į asmens duomenų apsaugą <…>. Šia direktyva siekiama prisidėti užbaigiant kurti laisvės, saugumo ir teisingumo erdvę[.]“

5. 46 konstatuojamojoje dalyje nustatyta:

„[B]et kokie duomenų subjekto teisių apribojimai turi atitikti Chartiją ir EŽTK, kaip išaiškinta atitinkamai pagal Teisingumo Teismo ir Europos Žmogaus Teisių Teismo[5] praktiką, ir visų pirma tokiais apribojimais negalima pažeisti tų teisių ir laisvių esmės[.]“

6. 49 konstatuojamojoje dalyje nurodyta:

„[J]eigu asmens duomenys tvarkomi vykdant nusikalstamų veikų tyrimą ir teismo procesuose baudžiamosiose bylose, valstybės narės turėtų turėti galimybę numatyti, kad naudojimasis teise gauti informaciją, teise susipažinti su [asmens] duomenimis bei teise reikalauti ištaisyti ar ištrinti asmens duomenis ir apriboti jų tvarkymą vykdomas pagal teismo procesą reglamentuojančias nacionalines taisykles[.]“

7. 1 straipsnyje („Dalykas ir tikslai“) numatyta:

„1. Šioje direktyvoje nustatytos taisyklės, susijusios su fizinių asmenų apsauga kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais.

[4] 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. 1). Toliau – RGPD.

[5] Toliau – EŽTT.

2. Remdamosi šia direktyva, valstybės narės:

a) saugo fizinių asmenų pagrindines teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą, ir

<…>

3. Šia direktyva valstybėms narėms netrukdoma taikyti griežtesnes apsaugos priemones nei tos, kurios numatytos šioje direktyvoje, siekiant užtikrinti duomenų subjektų teisių ir laisvių apsaugą kompetentingoms institucijoms tvarkant asmens duomenis.“

8. 2 straipsnio („Taikymo sritis“) 1 dalyje nustatyta:

„Ši direktyva taikoma kompetentingų institucijų vykdomam asmens duomenų tvarkymui 1 straipsnio 1 dalyje išdėstytais tikslais.“

9. 3 straipsnyje („Apibrėžtys“) nurodyta:

„Šioje direktyvoje:

<…>

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

<…>

7. kompetentinga institucija –

   a) bet kokia valdžios institucija, kompetentinga nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais; arba

<…>“

10. 4 straipsnio („Su asmens duomenų tvarkymu susiję principai“) 1 dalyje nustatyta:

„Valstybės narės numato, kad asmens duomenys turi būti:

a) tvarkomi teisėtai ir sąžiningai;

b) renkami konkrečiai nustatytais, aiškiai apibrėžtais ir teisėtais tikslais ir negali būti tvarkomi tokiu būdu, kuris būtų nesuderinamas su tais tikslais;

c) tinkami, aktualūs ir ne pernelyg išsamūs tikslų, kuriais jie yra tvarkomi, atžvilgiu;

<…>

e) saugomi tokia forma, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais jie tvarkomi;

f) tvarkomi taip, kad būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo tvarkymo be leidimo arba neteisėto tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo, taikant tinkamas technines ar organizacines priemones.“

11. 8 straipsnyje („Tvarkymo teisėtumas“) nurodyta:

„1. Valstybės narės numato, kad duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu jis būtinas, ir tiek, kiek jis būtinas kompetentingai institucijai atlikti užduotį 1 straipsnio 1 dalyje išdėstytais tikslais, ir kad jis turi būti grindžiamas Sąjungos arba valstybės narės teise.

2. Valstybės narės teisėje, kuria reglamentuojamas duomenų tvarkymas šios direktyvos taikymo srityje, konkrečiai nurodomi bent tvarkymo tikslai, tvarkytini asmens duomenys ir duomenų tvarkymo tikslai.“

12. 13 straipsnyje („Informacija, kuri padaroma prieinama duomenų subjektui arba kuri turi būti pateikta duomenų subjektui“) numatyta:

„1. Valstybės narės numato, kad duomenų valdytojas duomenų subjektui padarytų prieinama bent šią informaciją:

<…>

d) informaciją apie teisę pateikti skundą priežiūros institucijai ir priežiūros institucijos kontaktinius duomenis;

<…>

3. Valstybės narės gali priimti teisėkūros priemones, kuriomis informacijos teikimas duomenų subjektui pagal 2 dalį būtų atidėtas, apribotas arba kuriomis jo būtų nepaisoma tiek, kiek ir tol, kol tokia priemonė, tinkamai paisant atitinkamo fizinio asmens pagrindinių teisių ir teisėtų interesų, yra būtina ir proporcinga demokratinės visuomenės priemonė, siekiant:

a) netrukdyti atlikti oficialius arba teisinius nagrinėjimus, tyrimus ar procedūras;

b) nepakenkti nusikalstamų veikų prevencijai, tyrimui, atskleidimui ar baudžiamajam persekiojimui už jas arba bausmių vykdymui;

c) užtikrinti visuomenės saugumą;

d) užtikrinti nacionalinį saugumą;

e) apsaugoti kitų asmenų teises ir laisves.

<…>“

13. 15 straipsnio („Teisės susipažinti su asmens duomenimis apribojimai“) 1 dalyje nurodyta:

„1. Valstybės narės gali priimti teisėkūros priemones, kuriomis visiškai arba iš dalies būtų apribota duomenų subjekto teisė susipažinti su duomenimis tiek, kiek ir kol toks dalinis arba visiškas apribojimas, tinkamai paisant atitinkamo fizinio asmens pagrindinių teisių ir teisėtų interesų, yra būtina ir proporcinga demokratinės visuomenės priemonė, siekiant:

a) netrukdyti atlikti oficialius arba teisinius nagrinėjimus, tyrimus ar procedūras;

b) nepakenkti nusikalstamų veikų prevencijai, tyrimui, atskleidimui ar baudžiamajam persekiojimui už jas arba bausmių vykdymui;

c) užtikrinti visuomenės saugumą;

d) užtikrinti nacionalinį saugumą;

e) apsaugoti kitų asmenų teises ir laisves.“

14. 27 straipsnyje („Poveikio duomenų apsaugai vertinimas“) nustatyta:

„1. Tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma naudojant naujas technologijas, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, valstybės narės numato, kad duomenų valdytojas, prieš pradedant vykdyti duomenų tvarkymą, turi atlikti numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą.

2. 1 dalyje nurodytame vertinime pateikiamas bent bendras numatytų duomenų tvarkymo operacijų aprašymas, pavojaus duomenų subjektų teisėms ir laisvėms vertinimas, numatytos priemonės tam pavojui pašalinti, apsaugos priemonės, saugumo priemonės ir mechanizmai, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi šios direktyvos, atsižvelgiant į duomenų subjektų ir kitų susijusių asmenų teises ir teisėtus interesus.“

15. 28 straipsnyje („Išankstinis konsultavimasis su priežiūros institucija“) nurodyta:

„1. Valstybės narės numato, kad duomenų valdytojas arba duomenų tvarkytojas turi iš anksto konsultuotis su priežiūros institucija prieš tvarkydamas asmens duomenis, kurie bus įtraukti į naują susistemintą rinkinį, kuris turi būti sukurtas, jeigu:

a) 27 straipsnyje numatytame poveikio duomenų apsaugai vertinime nurodyta, kad atliekant duomenų tvarkymą kiltų didelis pavojus tuo atveju, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti, arba

b) dėl duomenų tvarkymo rūšies, visų pirma naudojant naujas technologijas, mechanizmus ar taikant naujas procedūras, kyla didelis pavojus duomenų subjektų teisėms ir laisvėms.

<…>“

16. 54 straipsnyje („Teisė imtis veiksmingų teisminių teisių gynimo priemonių prieš duomenų valdytoją arba duomenų tvarkytoją“) numatyta:

„Nedarant poveikio jokioms galimoms administracinėms arba neteisminėms teisių gynimo priemonėms, įskaitant teisę pateikti skundą priežiūros institucijai pagal 52 straipsnį, valstybės narės numato duomenų subjekto teisę imtis veiksmingų teisminių teisių gynimo priemonių, jeigu jis mano, kad jo teisės, nustatytos pagal šią direktyvą priimtose nuostatose, buvo pažeistos dėl jo asmens duomenų tvarkymo nesilaikant tų nuostatų.“

B. Nacionalinė teisė

17. *Strafprozessordnung*[6] 18 straipsnyje nustatytos kriminalinės policijos funkcijos, susijusios su baudžiamojo teisingumo vykdymu (1 dalis). Už kriminalinės policijos atliekamus tyrimus atsakingos saugumo institucijos (2 dalis). Viešojo saugumo tarnybos organai vykdo kriminalinės policijos užduotis, kurias sudaro nusikalstamų veikų tyrimas ir baudžiamasis persekiojimas už jas (3 dalis).

18. Pagal *StPO* 99 straipsnį kriminalinė policija atlieka tyrimą *ex officio* arba pagal skundą ir turi atsižvelgti į prokuratūros bei teismų nurodymus (1 dalis). Kai norint taikyti tyrimo priemonę reikalingas prokuratūros nurodymas, kriminalinė policija gali pasinaudoti atitinkamais įgaliojimais net ir be tokio nurodymo, jeigu kyla tiesioginis pavojus. Tokiu atveju ji turi nedelsdama paprašyti leidimo (2 dalis).

19. Pagal *StPO* 111 straipsnio 2 dalį, kai turi būti renkama duomenų laikmenose saugoma informacija, bet kuris asmuo privalo suteikti prieigą prie tos informacijos ir, gavęs prašymą, pateikti arba leisti pateikti elektroninę duomenų laikmeną įprastai naudojamu rinkmenos formatu. Be to, jis turi leisti padaryti atsarginę duomenų laikmenose saugomos informacijos kopiją.

II. Faktinės aplinkybės, byla ir prejudiciniai klausimai

20. C. G. yra Vokietijos pilietis, dirbantis ir gyvenantis Austrijoje.

21. 2021 m. vasario 23 d. Insbruko muitinės (Austrija) pareigūnai, vykdydami narkotinių medžiagų kontrolę, areštavo C. G. adresuotą paketą, jame buvo 85 g kanapių žolės.

22. 2021 m. kovo 6 d. du policijos pareigūnai apklausė C. G. apie paketo siuntėją ir atliko kratą jo būste. Per šią kratą areštuotas C. G. mobilusis telefonas (įskaitant SIM ir SD korteles) ir jam įteiktas arešto protokolas.

23. Paprašytas leisti peržiūrėti mobiliojo telefono ryšio duomenis C. G. to nepadarė, taip pat atsisakė atskleisti telefono prieigos kodą.

24. Landeko apskrities (Austrija) policijos būstinei nepavyko atblokuoti mobiliojo telefono. Jis buvo perduotas Vienos *Bundeskriminalamt* (Federalinė kriminalinė policija, Austrija), kur vėl nesėkmingai bandyta atblokuoti telefoną ir nuskaityti jame saugomus duomenis.

[6] Baudžiamojo proceso kodeksas (BGBl Nr. 631/1975); redakcija, kuri buvo taikoma klostantis faktinėms aplinkybėms – BGBl I Nr. 24/2020 (toliau – *StPO*).

25. Tuo metu, kai policija ėmėsi šių priemonių, jos nebuvo grindžiamos nei prokuratūros nurodymu, nei teismo nutartimi.

26. 2021 m. kovo 31 d. C. G. pateikė skundą *Landesverwaltungsgericht Tirol* (Tirolio apygardos administracinis teismas, Austrija) dėl jam taikytos prievartos priemonės ir užginčijo mobiliojo telefono areštą. 2021 m. balandžio 20 d. telefonas buvo grąžintas C. G.

27. C. G. jokiame etape nebuvo informuotas apie bandymą išanalizuoti jo mobiliajame telefone saugomus duomenis; šis faktas tapo žinomas dėl to, kad kaip liudytojas, įsipareigojęs duoti teisingus parodymus, buvo apklaustas policijos pareigūnas, kuris areštavo telefoną ir paskui pradėjo jame saugomų skaitmeninių duomenų analizavimo procesą. Bandymo išanalizuoti šiuos duomenis faktas nebuvo užfiksuotas ir kriminalinės policijos protokole.

28. Šiomis aplinkybėmis *Landesverwaltungsgericht Tirol* (Tirolio apygardos administracinis teismas, Austrija) pateikė Teisingumo Teismui tokius prejudicinius klausimus:

„1. Ar Direktyvos 2002/58, iš dalies pakeistos Direktyva 2009/136/EB, 15 straipsnio 1 dalis (prireikus siejama su 5 straipsniu), atsižvelgiant į [Chartijos] 7 ir 8 straipsnius, turi būti aiškinama taip, kad valstybės institucijų prieiga prie mobiliuosiuose telefonuose saugomų duomenų yra šiuose Chartijos straipsniuose įtvirtintų pagrindinių teisių suvaržymas ir jis yra toks rimtas, kad ši prieiga užkardant, tiriant ir nustatant nusikalstamas veikas turėtų apsiriboti tik kova su sunkiais nusikaltimais?

2. Ar Direktyvos 2002/58, iš dalies pakeistos Direktyva 2009/136, 15 straipsnio 1 dalis, atsižvelgiant į [Chartijos] 7, 8 ir 11 straipsnius bei 52 straipsnio 1 dalį, turi būti aiškinama taip, kad pagal ją draudžiama tokia nacionalinės teisės norma, kaip [*StPO*] 18 straipsnis, siejamas su 99 straipsnio 1 dalimi, pagal kurią saugumo institucijos, atlikdamos nusikalstamos veikos tyrimą, be teismo arba nepriklausomo administracinio subjekto leidimo pačios sau suteikia visišką ir nekontroliuojamą prieigą prie visų mobiliajame telefone saugomų skaitmeninių duomenų?

3. Ar [Chartijos] 47 straipsnis, prireikus siejamas su jos 41 ir 52 straipsniais, vertinant iš procesinio lygiateisiškumo ir veiksmingos teisinės gynybos perspektyvos, turi būti suprantamas taip, kad pagal jį draudžiama valstybės narės teisės norma, kaip antai [*StPO*] 18 straipsnis, siejamas su 99 straipsnio 1 dalimi, pagal kurią suteikiama galimybė išanalizuoti mobiliajame telefone saugomus skaitmeninius duomenis, apie tai nepranešus duomenų subjektui prieš taikant šią priemonę arba bent ją pritaikius?“

III. Procesas Teisingumo Teisme

29. Prašymas priimti prejudicinį sprendimą Teisingumo Teisme buvo įregistruotas 2021 m. rugsėjo 6 d.

30. 2021 m. spalio 20 d. Teisingumo Teismas prašymą priimti prejudicinį sprendimą pateikusio teismo paprašė nurodyti, ar Direktyva 2016/680 gali būti svarbi nagrinėjamai bylai.

31. 2021 m. lapkričio 11 d. šis teismas atsakė, kad pagrindinėje byloje turi būti taikoma Direktyva 2016/680.

32. Rašytines pastabas pateikė Vokietijos, Austrijos, Kipro, Danijos, Estijos, Prancūzijos, Vengrijos, Airijos, Nyderlandų, Norvegijos, Lenkijos bei Švedijos vyriausybės ir Europos Komisija.

33. 2023 m. sausio 16 d. vykusiame viešame teismo posėdyje dalyvavo rašytines pastabas pateikusių vyriausybių (išskyrus Vokietijos, Vengrijos ir Lenkijos), taip pat Suomijos vyriausybės atstovai. Teisingumo Teismas jų visų paprašė savo argumentus pateikti remiantis Direktyva 2016/680 ir žodžiu atsakyti į tam tikrus su ja susijusius klausimus.

IV. Analizė

A. Nepriimtinumas

34. Prašymą priimti prejudicinį sprendimą pateikęs teismas savo klausimuose iš pradžių prašė išaiškinti tik Direktyvą 2002/58. Vis dėlto beveik visos į bylą įstojusios šalys pritaria tam, kad ši direktyva nagrinėjamoje byloje netaikoma, todėl siekiant išspręsti ginčą jos aiškinti nereikia.

35. Pagal Direktyvos 2002/58 3 straipsnį direktyva taikoma „<…> asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais [Sąjungoje], įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius“.

36. Teisingumo Teismas nurodė, kad, „kai valstybės narės tiesiogiai įgyvendina priemones, nukrypstančias nuo elektroninių ryšių konfidencialumo, nenustatydamos tokių ryšių paslaugų teikėjams pareigos tvarkyti duomenis, duomenų subjektų duomenų apsaugai taikoma ne Direktyva 2002/58, o tik nacionalinė teisė, išskyrus atvejus, kai taikoma [Direktyva 2016/680]“ [7].

37. Nagrinėjamu atveju prieigą prie duomenų tiesiogiai bandė gauti policijos institucijos, vykdydamos nusikalstamos veikos tyrimą. Elektroninių ryšių paslaugų teikėjai, iš kurių nebuvo reikalaujama perduoti asmens duomenis, procese nedalyvavo. Taigi Direktyva 2002/58 netaikoma.

38. Šią situaciją reglamentuojantis Sąjungos teisės aktas yra Direktyva 2016/680; pagal jos 2 straipsnio 1 dalį direktyva taikoma kompetentingų institucijų vykdomam asmens duomenų tvarkymui siekiant „nusikalstamų veikų <…> tyrimo <…> tiksl[ų]“.

39. To, kas išdėstyta, pakanka, kad toks prašymas priimti prejudicinį sprendimą, kokį suformulavo nacionalinis teismas, būtų pripažintas nepriimtinu, nes Sąjungos teisės aktas, kurį prašoma išaiškinti, byloje netaikomas.

40. Vis dėlto iš tiesų pagal SESV 267 straipsnį Teisingumo Teismas gali performuluoti jam pateiktus prejudicinius klausimus arba nurodyti kitas Sąjungos teisės normas, kurios gali būti svarbios, siekdamas nacionaliniam teismui pateikti naudingą atsakymą [8].

41. Teisingumo Teismas kreipėsi į prašymą priimti prejudicinį sprendimą pateikusį teismą, kad jis nuspręstų dėl galimo Direktyvos 2016/680 poveikio. Taigi nacionaliniam teismui buvo suteikta galimybė papildyti ar performuluoti savo klausimus. Užuot tai padaręs, šis teismas tik pažymėjo,

[7] 2020 m. spalio 6 d. Sprendimo *La Quadrature du Net ir kt.* (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791; toliau – Sprendimas *La Quadrature du Net*) 103 punktas.

[8] Pavyzdžiui, 2016 m. balandžio 28 d. Sprendimo *Oniors Bio* (C-233/15, EU:C:2016:305) 30 punktas.

kad „nagrinėjamoje byloje bet kuriuo atveju turi būti laikomasi Direktyvos 2016/680 nuostatų“, tačiau nepaminėjo nuostatų, dėl kurių jam kilo abejonių, ir nepateikė išsamesnių esminių argumentų [9].

42. Teisingumo Teismas ne kartą yra pripažinęs, kad, „kaip nurodyta Procedūros reglamento 94 straipsnio c punkte, sprendime dėl prašymo priimti prejudicinį sprendimą turi būti nurodytos priežastys, paskatinusios jį teikiantį teismą kelti klausimą dėl tam tikrų Sąjungos teisės nuostatų išaiškinimo ar galiojimo, ir jo nustatytas šių nuostatų ir pagrindinėje byloje taikomų nacionalinės teisės aktų ryšys“ [10].

43. Taigi remiantis tuo, kas išdėstyta, matyti, kad šiame prašyme priimti prejudicinį sprendimą nesilaikyta Procedūros reglamento 94 straipsnio reikalavimų. Nors Teisingumo Teismo pozicija šiuo klausimu lanksti, bendradarbiavimas su prašymą priimti prejudicinį sprendimą pateikusiu teismu turi būti abipusis: manau, kad jeigu šis teismas be pagrindo nebendradarbiauja ir neišdėsto savo abejonių dėl, jo nuomone, taikytinos Sąjungos teisės (nagrinėjamu atveju Direktyvos 2016/680) aiškinimo, logiška, kad jo prašymas priimti prejudicinį sprendimą turi būti pripažintas nepriimtinu [11].

44. Be to, prašymą priimti prejudicinį sprendimą pateikęs teismas:

– nepatikslino, kokio pobūdžio duomenis policijos institucijos bandė tvarkyti ir kokių konkrečiai asmens duomenų buvo prašoma. Iš pradžių, regis, jis minėjo tik ryšio duomenis (t. y. srauto ir buvimo vietos duomenis), tačiau vėliau neatmetė galimybės, kad atblokavus telefoną būtų suteikta prieiga prie „visų saugomų skaitmeninių duomenų“ [12] ir net prie bendravimo ir elektroninių pokalbių telefonu turinio [13],

– nurodė tiek telefono areštą ir prieigą ar bandymą gauti prieigą prie jame esančių duomenų, tiek vėlesnį šių duomenų „panaudojimą“ (*Auswertung*), t. y. jų analizę ir skaitymą. Jis pažymėjo, kad skaitymas „apima visišką ir nekontroliuojamą prieigą prie viso duomenų subjekto skaitmeninio bendravimo“, todėl galima „atkurti labai tikslų ir išsamų vaizdą apie beveik visas privataus gyvenimo sritis“.

45. Tokiomis aplinkybėmis Teisingumo Teismas, užuot *performulavęs* prašymą priimti prejudicinį sprendimą pateikusio teismo klausimus, iš tikrųjų *perrašytų* prašymą priimti prejudicinį sprendimą, iš dalies remdamasis, be kita ko, hipotetiniais argumentais, o ne įrodytomis faktinėmis aplinkybėmis. Svarbu pakartoti, kad visa tai jis darytų suteikęs teismui galimybę pačiam papildyti arba performuluoti savo klausimus.

46. Taigi siūlau prašymą priimti prejudicinį sprendimą pripažinti nepriimtinu, kaip to reikalauja kelios į bylą įstojusios valstybės.

[9] Teisingumo Teismas turėjo paraginti šalis nurodyti, „kokios, jų nuomone, Direktyvos 2016/680 nuostatos, į kurias atsižvelgdamas Teisingumo Teismas prireikus turėtų performuluoti tris prašymą priimti prejudicinį sprendimą pateikusio teismo prejudicinius klausimus, yra reikšmingos“ (ketvirtasis klausimas iš tų, kurie pateikti, kad į juos žodžiu būtų atsakyta teismo posėdyje).

[10] 2021 m. spalio 6 d. Sprendimo *Consorzio Italian Management ir Catania Multiservizi* (C-561/19, EU:C:2021:799) 69 punktas.

[11] Tokia mano pozicija sutampa su Prancūzijos vyriausybės pozicija (jos rašytinių pastabų 36–41 punktai).

[12] Taip nurodyta antrajame prejudiciniame klausime.

[13] Prašymą priimti prejudicinį sprendimą pateikęs teismas teigia, kad „pagal ryšio duomenis galima nustatyti beveik visus kontaktus – bendravimo dažnumą, laiką ir trukmę, o pagal SMS ir kitas pokalbių programas, kuriomis buvo naudojamasi, galima netgi atkurti turinį; išanalizavus saugomas nuotraukas ir naršymo istoriją taip pat galima susidaryti labai išsamų vaizdą apie duomenų subjekto privatų gyvenimą“.

47. Tokią išvadą dėl nepriimtinumo reikėtų padaryti ir dėl per teismo posėdį nurodytos aplinkybės, kad prašymą priimti prejudicinį sprendimą pateikusiame teisme nebėra tikro ginčo, dėl kurio reikėtų aiškinti Sąjungos teisės normas.

48. Iš tiesų Austrijos vyriausybė (kuriai yra pavaldžios tyrime dalyvavusios policijos institucijos) pripažįsta, kad šių institucijų veiksmai buvo neteisėti ir pažeidė duomenų subjekto teises. Kadangi, kaip nurodyta nutartyje dėl prašymo priimti prejudicinį sprendimą, pareiškėjo reikalavimas administraciniame teisme buvo nukreiptas būtent prieš policijos priemones, kurias administracija (atsakovė) laiko neteisėtomis, prašymą priimti prejudicinį sprendimą pateikusiame teisme ginčo nebėra.

49. Bet kuriuo atveju, jeigu Teisingumo Teismas nepritartų mano nuomonei, toliau papildomai aptarsiu esmines problemas, kuriomis grindžiami prejudiciniai klausimai.

50. Vis dėlto visų pirma manau, kad reikia atmesti dar vieną nepriimtinumo pagrindą, kurį nurodė kai kurios į bylą įstojusios šalys[14]. Jos laikosi nuomonės, kad atsižvelgiant į tai, jog Direktyva 2016/680 susijusi su fizinių asmenų apsauga *tvarkant* jų duomenis, ji netaikoma tokiems atvejams kaip šis, kai duomenys nebuvo tvarkomi, o tik *bandyta gauti prieigą* prie jų ir galiausiai duomenų nepavyko gauti.

51. Priešingai, Komisija mano, kad siekiant užtikrinti Direktyvos 2016/680 veiksmingumą pirmenybė turėtų būti teikiama aiškinimui, kad direktyvos dalykas apima ne tik duomenų tvarkymą siaurąja prasme, bet ir tiesiogiai su juo susijusius klausimus. Vienas iš tokių klausimų – bandymas gauti prieigą prie duomenų, kuriuos siekiama tvarkyti[15].

52. Manau, kad nereikia peržengti Direktyvos 2016/680 taikymo srities ribų[16]; nagrinėjamoje byloje ji pagrįstai taikoma ne dėl to, kad mobilusis telefonas buvo areštuotas[17], o dėl vėlesnių policijos institucijų veiksmų, kuriais jos siekė iš telefono išgauti tam tikrus duomenų subjekto asmens duomenis ir tuo tikslu bandė telefoną atblokuoti ir gauti prieigą prie jo turinio.

53. Viena iš operacijų, kurios Direktyvos 2016/680 3 straipsnio 2 punkte apibrėžtos kaip „duomenų tvarkymo“ operacijos, yra „[bet kuriuo] kitu būdu sudar[yta] galimyb[ė] <…> naudotis“ asmens duomenimis atliekant nusikalstamos veikos tyrimą. Manau, kad policijos institucija, areštavusi telefoną, kuriame saugomi tokie duomenys, ir jį naudodama tam, kad išgautų iš jo duomenis, pradeda duomenų tvarkymo „operaciją“, net jeigu ji nepavyksta dėl techninių priežasčių, susijusių su kriptografiniu saugumu.

[14] Turiu omenyje būtent Austrijos, Prancūzijos, Nyderlandų ir Norvegijos vyriausybes.

[15] Komisija teigia, kad „nėra skirtumo, ar bandymai buvo sėkmingi. Kilę techniniai sunkumai, dėl kurių bandymai gauti prieigą nesėkmingi, yra aplinkybė, kurios negalima žinoti iš anksto ir kuri neturi įtakos asmens duomenų apsaugos rizikai“.

[16] Visų pirma manau, kad nereikia taikyti Direktyvos 2016/680 27 ir 28 straipsnių, kuriuos taikyti siūlo Komisija savo rašytinėse pastabose. „Poveikio duomenų apsaugai vertinimas“, numatytas 27 straipsnyje, apskritai yra susijęs su „duomenų tvarkymo rūši[mi]“, o ne konkrečiomis ar individualiomis duomenų tvarkymo operacijomis. Tai matyti iš Direktyvos 2016/680 58 konstatuojamosios dalies: „[p]oveikio vertinimai turėtų apimti atitinkamas duomenų tvarkymo operacijų sistemas ir procesus, bet *ne atskirus atvejus*“ (kursyvu išskirta mano). Per teismo posėdį Komisija patikslino, kodėl remiasi šiomis dviem nuostatomis: ji jas nurodė tik siekdama pabrėžti, kad Direktyvoje 2016/680 taip pat numatytos situacijos, susidariusios prieš atliekant pačias duomenų tvarkymo operacijas.

[17] Direktyvoje 2016/680 nereglamentuotas telefono, kaip įrodymo, konfiskavimas atliekant nusikalstamos veikos tyrimą.

54. Nesėkmingo bandymo gauti prieigą prie mobiliajame telefone saugomų asmens duomenų, atliekant nusikalstamų veikų tyrimą, atveju Direktyva 2016/680 taikoma dėl panašių priežasčių į tas, dėl kurių Teisingumo Teismas pripažino, kad Direktyva 2002/58 taikytina *bandymui* (taip pat nesėkmingam) gauti teismo leidimą susipažinti su tam tikrais elektroninių ryšių paslaugų teikėjo saugomais asmens, dėl kurio atliekamas tyrimas, duomenimis [18].

55. Šiomis aplinkybėmis, jeigu prašymą priimti prejudicinį sprendimą pateikęs teismas turėtų spręsti dėl policijos veiksmų neteisėtumo (kaip nurodžiau, jų neteisėtumą pripažino Austrijos vyriausybė), jo vertinimas galėtų priklausyti nuo tikslo, kurio siekta tais veiksmais, teisėtumo ir tuo atveju, jei priemonė buvo sėkmingai įvykdyta, ir tuo atveju, jeigu ji tik pradėta nesėkmingai vykdyti.

B. Dėl esmės

1. Pirmasis prejudicinis klausimas

56. Prašymą priimti prejudicinį sprendimą pateikęs teismas nori išsiaiškinti, ar pagal Direktyvos 2002/58 15 straipsnio 1 dalį (prireikus siejamą su 5 straipsniu) ir atsižvelgiant į Chartijos 7 ir 8 straipsnius „valstybės institucijų prieiga prie mobiliuosiuose telefonuose saugomų duomenų yra šiuose Chartijos straipsniuose įtvirtintų pagrindinių teisių suvaržymas ir jis yra toks rimtas, kad ši prieiga užkardant, tiriant ir nustatant nusikalstamas veikas turėtų apsiriboti tik kova su sunkiais nusikaltimais“.

57. Jeigu prašymas priimti prejudicinį sprendimą būtų pripažintas priimtinu, atsižvelgiant į tai, kad Direktyva 2002/58 netaikytina, pirmąjį klausimą reikėtų performuluoti taip, kad Teisingumo Teismo atsakyme būtų išaiškinta Direktyva 2016/680.

58. Šiame atsakyme turėtų būti patikslinta, ar tokiais atvejais, kaip nagrinėjamas šioje byloje, galima kalbėti apie teisių suvaržymą, ir jeigu jis yra, ar Direktyvoje 2016/680 reikalaujama, kad prieiga prie duomenų būtų suteikta tik kovos su sunkiais nusikaltimais atveju.

59. Dėl duomenų tvarkymo operacijų iš esmės gali kilti pavojus teisei į privataus gyvenimo gerbimą (Chartijos 7 straipsnis) ir teisei į asmens duomenų apsaugą (Chartijos 8 straipsnis). Todėl valdžios institucijos, norėdamos pateisinti savo veiksmus, kai įgyvendinamos šios pagrindinės teisės, turi laikytis Chartijos 52 straipsnio 1 dalyje nustatytų sąlygų.

60. Pagal Chartijos 7 ir 8 straipsnius saugomos teisės dar labiau paveikiamos, kai dėl tokių veiksmų: a) siekiama gauti prieigą prie neskelbtinų duomenų, kurie paprastai įrašomi į mobiliuosius telefonus ir su kuriais susipažinus gali paaiškėti jų turėtojų gyvenimo aspektai, neatskleistini tretiesiems asmenims; ir b) suteikiama galimybė gauti prieigą prie bendravimo turinio.

61. Vis dėlto apskritai, atsižvelgiant į Direktyvos 2016/680 turinį, ši direktyva negali būti aiškinama taip, kad joje minimas duomenų tvarkymas apsiriboja tik kovos su sunkiais nusikaltimais atvejais.

[18] 2018 m. spalio 2 d. Sprendimas *Ministerio Fiscal* (C-207/16, EU:C:2018:788).

62. Direktyvos 2016/680 dalykas yra bet kuri kompetentingų institucijų vykdoma asmens duomenų tvarkymo operacija [19], kuria siekiama *visų rūšių* nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas tikslų.

63. Iš Direktyvoje 2016/680 nustatytų principų, susijusių su asmens duomenų tvarkymu siekiant tų tikslų (4 straipsnis), arba iš duomenų tvarkymo teisėtumo sąlygų (8 straipsnis) nematyti, kad paprastai duomenis galima tvarkyti tik sunkaus nusikaltimo atveju.

64. Apribojimo, pagal kurį duomenys tvarkomi tik kovojant su sunkiais nusikaltimais, taip pat negalima pagrįsti vien su Direktyva 2002/58 susijusios Teisingumo Teismo jurisprudencijos [20] ekstrapoliacija tokiems atvejams, kaip nagrinėjamas šioje byloje.

65. Manau, kad to negalima daryti, nes ši jurisprudencija susijusi su visuotiniu ir nediskriminaciniu bendros neapibrėžtos grupės asmens duomenų saugojimu, kurį sistemingai vykdo elektroninių ryšių paslaugų teikėjai (nepažeidžiant to, ką nurodysiu toliau). Remiantis tokio saugojimo nulemtu visai visuomenei taikomo suvaržymo mastu galima paaiškinti, kodėl Teisingumo Teismas laikėsi itin griežtos pozicijos, uždrausdamas jį ir numatydamas šio draudimo išimtis.

66. Kitaip yra tuo atveju, kai prašoma prieiga susijusi ne su visais gyventojais ar didelėmis jų grupėmis (t. y. bendros neapibrėžtos grupės asmens duomenimis), o su informacija, saugoma individualiame mobiliajame telefone, vykdant nusikalstamos veikos tyrimo procedūrą, kuri taip pat yra individuali ir kuriai taikoma būtent Direktyva 2016/680.

67. Direktyvos 2016/680 dalykas yra tik kompetentingų institucijų vykdomos duomenų tvarkymo operacijos siekiant nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas tikslų. Nusikalstamos veikos yra visų rūšių veikos, ne tik sunkios.

68. Be to, kaip pabrėžė kai kurios į bylą dėl prejudicinio sprendimo priėmimo įstojusios šalys, kadangi Direktyvoje 2016/680 nėra jokių nuostatų dėl nusikalstamų veikų sunkumo, ši direktyva negali būti vienodai taikoma valstybėse narėse, nes pagal kiekvieną nacionalinę teisę veikos, už kurią baudžiama, sunkumo lygis vertinamas labai skirtingai [21].

69. Taigi Direktyvoje 2016/680 kaip teisėtumo sąlyga nėra numatytas reikalavimas, kad asmens duomenys pagal šią direktyvą būtų tvarkomi tik siekiant kovoti su sunkiais nusikaltimais.

70. Atsižvelgiant į tai, kas išdėstyta, matyti, kad nekyla kliūčių tam, kad pagal proporcingumo principą kiekvienu konkrečiu atveju duomenų, kuriuos tvarkyti siekia kompetentingos institucijos pagal Direktyvą 2016/680, tvarkymas būtų pritaikytas atsižvelgiant į: a) nusikalstamų veikų, dėl kurių vykdomas persekiojimas, pobūdį; ir b) asmens duomenų, kuriuos siekiama tvarkyti, kokybę.

[19] Direktyvos 2016/680 3 straipsnio 2 punkte nurodyta „operacijų“ tipologija yra labai plati. Žr. šios išvados 9 punktą, kuriame ji pakartota.

[20] 2016 m. gruodžio 21 d. Sprendimas *La Quadrature du Net*, 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970; toliau – Sprendimas *Tele2 Sverige ir Watson*), 2018 m. spalio 2 d. Sprendimas *Ministerio Fiscal* (C-207/16, EU:C:2018:788), 2020 m. spalio 6 d. Sprendimas *Privacy International* (C-623/17, EU:C:2020:790) ir 2021 m. kovo 2 d. Sprendimas *Prokuratuur (Prieigos prie elektroninių ryšių duomenų sąlygos)* (C-746/18, EU:C:2021:152; toliau – Sprendimas *Prokuratuur*).

[21] Prancūzijos vyriausybė kaip pavyzdį pateikia nusikalstamas veikas, susijusias su narkotikų laikymu ir prekyba narkotikais, kurių sunkumas pagal Austrijos ir Prancūzijos baudžiamąją teisę skiriasi. Panašios nuomonės laikosi ir Švedijos vyriausybė.

71. Šiuo klausimu pritariu kai kuriems Vokietijos vyriausybės teiginiams dėl prieigos prie konfiskuotų telefonų duomenų ribojimo, kai iš tų duomenų galima susidaryti išsamų vaizdą apie telefono savininko asmenybę, atsižvelgiant į skaitmeninį telefono turinį. Vokietijos vyriausybė mano, kad prieiga turėtų būti suteikta tik prie tų duomenų, kurie reikalingi kaip įrodymas konkrečioje byloje, ir galbūt jos nereikia suteikti esant tokiems veiksniams, kaip „veikos, dėl kurios atliekamas tyrimas, nereikšmingumas arba menka prašomų duomenų įrodomoji vertė“ [22].

72. Taigi *apskritai* prieiga prie mobiliajame telefone saugomų asmens duomenų, siekiant palengvinti veikų, kurios gali būti priskiriamos prie bendrųjų ar įprastų nusikalstamų veikų, tyrimą, pagal Direktyvą 2016/680 savaime nėra neteisėta. Tai, ar *konkrečiai* tokią prieigą reikia suteikti, kiekviena proga turi įvertinti atitinkama institucija, atsižvelgdama į prieigos būtinumą ir minėtą proporcingumo kriterijų.

73. Manau, kad tokia išvada darytina remiantis Direktyvos 2016/680 nuostatomis, kuriose numatytos asmens duomenų tvarkymo kovojant su nusikalstamumu teisėtumo sąlygos:

– 4 straipsnio 1 dalies a punktu, pagal kurį duomenys turi būti „tvarkomi teisėtai“,

– 8 straipsnio 1 dalimi, kurioje pabrėžiama, kad duomenų tvarkymas turi būti *būtinas* ir pagrįstas Sąjungos arba valstybės narės teise.

2. Antrasis prejudicinis klausimas

74. Antruoju prejudiciniu klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, ar pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, „draudžiama [tokia] nacionalinės teisės norma, kaip [*StPO*] 18 straipsnis, siejamas su 99 straipsnio 1 dalimi, pagal kurią saugumo institucijos, atlikdamos nusikalstamos veikos tyrimą, be teismo arba nepriklausomo administracinio subjekto leidimo pačios sau suteikia visišką ir nekontroliuojamą prieigą prie visų mobiliajame telefone saugomų skaitmeninių duomenų“.

75. Klausimo formuluotė šiek tiek dviprasmiška. Prašymą priimti prejudicinį sprendimą pateikęs teismas:

– pripažįsta, kad *StPO* 110 straipsnio 2 dalyje numatyta, jog siekiant areštuoti turtą iš esmės reikalingas prokuratūros leidimas. Policijos institucija be tokio leidimo turtą gali areštuoti tik susiklosčius ypatingoms aplinkybėms, numatytoms to paties straipsnio 3 dalyje (atrodo, kad nagrinėjamu atveju tokių aplinkybių nėra),

– vis dėlto jis priduria, kad mobiliuosiuose telefonuose saugomos informacijos analizė „[*StPO*] reglamentuota nevienareikšmiškai“ ir saugumo institucijos gali ją gauti savo iniciatyva, neturėdamos išankstinio leidimo.

[22] Vokietijos vyriausybės rašytinių pastabų 20 punktas.

76. Austrijos vyriausybė pateikė nacionalinės teisės akto redakciją, kuri neatitinka pateiktosios nutartyje dėl prašymo priimti prejudicinį sprendimą. Konkrečiai kalbant, ji teigia, kad pagal nacionalinę teisę ir telefono areštas (išskyrus skubius atvejus), ir jame saugomų duomenų analizė galimi tik gavus prokuratūros leidimą [23]. Be prokuratūros nurodymo tai, kad policija naudoja telefone saugomus duomenis, yra neteisėta.

77. Prašymą priimti prejudicinį sprendimą pateikęs teismas turi patikrinti, kas numatyta nacionalinės teisės aktuose. Vykstant SESV 267 straipsnyje numatytam procesui, Teisingumo Teismas neturi kompetencijos aiškinti nacionalinės teisės ir tik prašymą priimti prejudicinį sprendimą pateikęs teismas turi nustatyti tikslią nacionalinių įstatymų ir kitų teisės aktų nuostatų apimtį [24].

78. Nesiekdamas įsitraukti į ginčą dėl Austrijos teisės aiškinimo manau, kad vien iš prašymą priimti prejudicinį sprendimą pateikusio teismo nurodytų nuostatų (*StPO* 18 straipsnio, siejamo su to paties įstatymo 99 straipsnio 1 dalimi) sunku daryti išvadą, kurią padarė pats teismas. Vis dėlto, kartoju, tai gali nuspręsti tik šis teismas.

79. Bet kuriuo atveju prašymą priimti prejudicinį sprendimą pateikęs teismas laikosi nuomonės, kad Sprendime *Prokuratuur* įtvirtintą jurisprudenciją [25], susijusią su teismo ar nepriklausomos institucijos atliekama išankstine prieigos prie saugomų duomenų kontrole, galima taikyti tokiai bylai, kaip ši.

80. Priešingai, Nyderlandų vyriausybė mano, kad ši jurisprudencija turi būti vertinama atsižvelgiant į nacionalinės teisės aktus, pagal kuriuos kompetentingoms institucijoms buvo suteikta *bendra* prieiga prie *visų* saugomų srauto ir buvimo vietos duomenų. Tai paaiškintų reikalavimą turėti išankstinį teismo leidimą, kuris vis dėlto gali būti nepagrįstas tuo atveju, kai norima gauti prieigą prie vieno mobiliojo telefono duomenų.

81. Norvegijos vyriausybė taip pat teigia, kad priemonė, pagal kurią reikia gauti išankstinį nepriklausomos teisminės ar administracinės institucijos leidimą, aiškiai nenumatyta tarp daugelio Direktyvoje 2016/680 nustatytų apsaugos priemonių [26].

82. Komisija, remdamasi tuo, kad Direktyvos 2016/680 nuostatos turi būti aiškinamos atsižvelgiant į Chartiją, teigia, jog šios direktyvos 8 straipsnio 1 dalyje (duomenų tvarkymo teisėtumo sąlygos) valstybėms narėms nustatyta pareiga reiškia, kad turi būti gerbiamos Chartijos 7 ir 8 straipsniuose garantuojamos pagrindinės teisės.

83. Pritariu Komisijai, kad laikydamiesi šių Chartijos nuostatų nacionalinės teisės aktų leidėjai privalo nustatyti taisykles, būtinas siekiant užtikrinti, kad prieiga prie duomenų kiekvienu atveju būtų pagrįsta ir suteikta tik tiek, kiek griežtai būtina ir proporcinga.

[23] Austrijos vyriausybės pastabų 19 punktas. Ji remiasi 2020 m. spalio 13 d. *Oberster Gerichtshof* (Aukščiausiasis Teismas, Austrija) sprendimu (byla Nr. 11 Os 56/20z), kuriame kriminalinės policijos vykdyta mobiliojo telefono duomenų analizė neturint prokuratūros leidimo pripažinta neteisėta, nes dėl jos pažeistos subjektinės duomenų subjekto teisės.

[24] 2022 m. balandžio 28 d. Sprendimo *SeGEC ir kt.* (C-277/21, EU:C:2022:318) 21 punktas.

[25] Sprendimo *Prokuratuur* 51 punkte numatyta: „[B]ūtina, kad[,] prieš suteikiant kompetentingoms nacionalinėms institucijoms prieigą prie saugomų duomenų, teismas arba nepriklausomas administracinis subjektas atliktų išankstinę kontrolę, o toks teismas ar toks subjektas savo sprendimą priimtų gavę motyvuotą tų institucijų prašymą, kurį jos pateiktų, be kita ko, vykdydamos prevencijos, atskleidimo arba baudžiamojo persekiojimo procedūras“.

[26] Be 4 ir 8 straipsniuose minimų priemonių, priemonės, nurodytos III skyriuje („Duomenų subjekto teisės“), IV skyriuje („Duomenų valdytojas ir duomenų tvarkytojas“), VI skyriuje („Nepriklausomos priežiūros institucijos“) ir VIII skyriuje („Teisių gynimo priemonės, atsakomybė ir sankcijos“).

84. Vis dėlto tokios nacionalinės taisyklės nebūtinai turi būti konkrečiai skirtos prieigai prie asmens duomenų, esančių, kaip nagrinėjamu atveju, mobiliajame telefone, o gali būti numatytos bendrose nacionalinės teisės normose, reglamentuojančiuose įrodymų rinkimą.

85. Šiuo klausimu jau pakartojau Sprendimo *La Quadrature du Net* 103 punktą dėl valstybių narių priemonių, darančių poveikį elektroninių ryšių konfidencialumui, kai tokių ryšių paslaugų teikėjams nenustatyta pareiga tvarkyti duomenis [27].

86. Taigi, nesant poreikio pagal Direktyvą 2016/680 nustatyti *specialiųjų* procesinių taisyklių, pagal kurias būtų užtikrintas prieigos prie mobiliajame telefone saugomų duomenų teisėtumas [28], taikomos nacionalinės taisyklės, reglamentuojančios naudojimąsi įgaliojimais vykdyti kratą ir areštą atliekant nusikalstamų veikų tyrimą [29].

87. Be to, nuoroda į nacionalinės teisės nuostatas, pateikta siekiant užtikrinti prieigos teisėtumą pagal Direktyvą 2016/680, atitinka EŽTT jurisprudenciją. EŽTT būtent byloje dėl Austrijos Respublikos, susijusioje su EŽTK 8 straipsniu (teisė į privataus ir šeimos gyvenimo, būsto neliečiamybės ir susirašinėjimo slaptumo gerbimą), konstatavo, kad daiktų, ypač dokumentų, areštą reglamentuojantys Austrijos teisės aktai taikomi kompiuterinėse laikmenose saugomų duomenų kratai ir areštui [30].

88. Jeigu, kaip teigia Austrijos vyriausybė, remdamasi *Oberster Gerichtshof* (Aukščiausiasis Teismas, Austrija) jurisprudencija, policijos institucijos neturi teisės gauti prieigos prie konkrečiame mobiliajame telefone saugomų duomenų be prokuratūros leidimo, antrasis prejudicinis klausimas iš esmės tampa beprasmis.

89. Bet kuriuo atveju atsakant į šį klausimą negalima atmesti galimybės, kad turint prieigą prie areštuotame telefone esančių asmens duomenų būtų „atkurt[as] labai tiksl[us] ir išsam[us] vaizd[as] apie beveik visas privataus gyvenimo sritis“ [31]. Jeigu taip būtų, policijos institucijos negalėtų imtis veiksmų, neturėdamos Sprendime *Prokuratuur* nurodyto išankstinio leidimo.

90. Iš pirmo žvilgsnio atrodo, kad šis teiginys neatitinka pirma nurodyto požiūrio, jog Direktyva 2002/58 (išaiškinta Sprendime *Prokuratuur*) šioje byloje netaikoma. Vis dėlto manau, kad remiantis to sprendimo *ratio* galima patvirtinti tokią pačią išvadą.

91. Nors byloje, kurioje priimtas Sprendimas *Prokuratuur*, suteikus prieigą buvo gauti duomenys (metaduomenys) iš elektroninių ryšių paslaugų teikėjų, joje, kaip ir nagrinėjamu atveju, buvo sprendžiama dėl individualus nusikalstamos veikos tyrimo, nukreipto prieš konkretų asmenį. Buvo siekiama surinkti „įvairių <…> telefono numerių duomen[is] [ir duomenis, susijusius su] <…> įvairiais tarptautiniais judriojo ryšio įrangos identifikatoriais“ [32].

[27] Žr. šios išvados 36 punktą.

[28] Tai, kad nustatyti tokias taisykles sunku, gerai matyti iš Komisijos pastangų savo pastabų 34–39 punktuose padėti apibrėžti aiškias ir tikslias taisykles dėl ribų nustatymo ir tinkamų apsaugos priemonių, susijusių su prieiga prie duomenų mobiliajame telefone.

[29] Taisyklės, kurios nepatenka į Sąjungos teisės taikymo sritį, tačiau gali būti taikomos siekiant įvykdyti iš šios teisės kylantį reikalavimą, kaip nurodo, pavyzdžiui, Danijos ir Airijos vyriausybės.

[30] 2007 m. spalio 16 d. EŽTT sprendimo *Wieser ir Bicos Beteiligungen prieš Austriją* (CE:ECHR:2007:1016JUD007433601) 54 punkte nurodyta: „Austrijos baudžiamojo proceso kodekse nėra konkrečių nuostatų dėl elektroninių duomenų kratos ir arešto. Vis dėlto jame pateikta išsamių nuostatų dėl daiktų arešto, taip pat konkrečių taisyklių dėl dokumentų arešto. Nacionalinių teismų jurisprudencijoje nustatyta, kad šios nuostatos taip pat taikomos elektroninių duomenų kratai ir areštui“.

[31] Žr. šios išvados 44 punkte pakartotus prašymą priimti prejudicinį sprendimą pateikusio teismo argumentus.

[32] Sprendimo *Prokuratuur* 17 punktas.

92. Manau, kad Sprendime *Prokuratuur* galima išskirti du aspektus: a) abejones dėl bendrųjų valstybės narės taisyklių, susijusių su bendru ir nediferencijuotu paslaugų teikėjų turimų duomenų saugojimu ir vėlesne prieiga prie jų; ir b) konkrečiu atveju atliekamą išankstinę prieigos prie tokių metaduomenų kontrolę, kai jie leidžia susidaryti tikslų vaizdą apie asmens privatų gyvenimą.

93. Manau, kad aplinkybė, jog nagrinėjamoje byloje paslaugų teikėjai nevaldo privatų gyvenimą atskleidžiančių duomenų ir šie duomenys gauti (arba siekiama juos gauti) iš vieno areštuoto telefono, turi antraeilę reikšmę atsižvelgiant į Sprendime *Prokuratuur* nurodyto reikalavimo vykdyti išankstinę kontrolę *ratio*.

94. Išankstinė kontrolė galiausiai grindžiama Chartijos 7 ir 8 straipsniuose užtikrinta apsauga. Ją atliekanti institucija turi „galėt[i] užtikrinti teisingą pusiausvyrą tarp interesų, susijusių su tyrimo poreikiais kovojant su nusikalstamumu, ir asmenų, prie kurių duomenų suteikiama prieiga, pagrindinių teisių į privataus gyvenimo gerbimą ir asmens duomenų apsaugą“ [33].

3. Trečiasis prejudicinis klausimas

95. Trečiuoju prejudiciniu klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas nori išsiaiškinti, ar pagal Chartijos 47 straipsnį (prireikus siejamą su 41 ir 52 straipsniais) draudžiama tokia teisės norma, kaip numatyta Austrijos teisės akte [34], „pagal kurią suteikiama galimybė išanalizuoti mobiliajame telefone saugomus skaitmeninius duomenis, apie tai nepranešus duomenų subjektui prieš taikant šią priemonę arba bent jau ją pritaikius“.

96. Manau, kad taip suformuluotas klausimas gali būti nereikalingas siekiant išspręsti ginčą, nes duomenų subjektas galėjo pasinaudoti Chartijos 47 straipsnyje įtvirtinta teise ir prašymą priimti prejudicinį sprendimą pateikusio teismo prašyti pripažinti negaliojančiais policijos veiksmus, susijusius su areštuotu telefonu, įskaitant vėlesnį (ir nesėkmingą) jame saugomų duomenų panaudojimą.

97. Atsižvelgiant į šias dvi policijos veiksmų aplinkybes, reikėtų išskirti tokius aspektus:

– dėl paties telefono arešto iš byloje esančios informacijos matyti, kad duomenų subjektas apie jį žinojo ir atsisakė pateikti policijos institucijoms atblokavimo kodą, kai telefonas buvo konfiskuotas,

– dėl bandymo analizuoti duomenis, atrodo, kad duomenų valdytojas neinformavo duomenų subjekto apie šią operaciją, nors Austrijos vyriausybė teigia, kad duomenų subjektas žinojo apie ataskaitą, kurioje konstatuota, jog kriminalinė policija ėmėsi veiksmų dėl telefono [35].

98. Taigi lieka tam tikrų neaiškumų dėl duomenų naudojimo ir dėl to, ar duomenų subjektas žinojo apie jį; kaip minėjau, dėl šių neaiškumų prašymą priimti prejudicinį sprendimą pateikęs teismas turėjo pateikti paaiškinimų nutartyje dėl prašymo priimti prejudicinį sprendimą ir jie neleidžia naudingai atsakyti į trečiąjį prejudicinį klausimą.

[33] Sprendimo *Prokuratuur* 52 punktas.

[34] Jis vėl nurodo *StPO* 18 straipsnį, siejamą su 99 straipsniu.

[35] Jos rašytinių pastabų 37 punktas.

99. Bet kuriuo atveju pateiksiu savo nuomonę dėl šio klausimo, jeigu Teisingumo Teismas nepripažintų jo nepriimtinu. Jeigu taip būtų, atsižvelgiant į tai, kad Direktyva 2002/58 netaikoma, klausimą reikėtų performuluoti remiantis Direktyva 2016/680, kurios 13, 15 ir 54 straipsniuose pateiktos gairės, kaip į jį atsakyti.

100. Pagal Direktyvą 2016/680 duomenų subjektui turi būti pateikta tokia informacija apie jo duomenų tvarkymą, kurios reikia siekiant, be kita ko: a) pateikti skundą priežiūros institucijai (13 straipsnio 1 dalies d punktas); b) imtis veiksmingų teisminių teisių gynimo priemonių, jeigu pažeistos pagal Direktyvą 2016/680 užtikrinamos teisės, nedarant poveikio galimoms administracinėms arba neteisminėms teisių gynimo priemonėms (54 straipsnis).

101. Vis dėlto negalima pamiršti, kad ir Direktyvos 2016/680 13 straipsnio 3 dalyje, ir jos 15 straipsnio 1 dalyje valstybėms narėms leidžiama priimti teisėkūros priemones, pagal kurias:

– informacijos teikimas duomenų subjektui pagal 13 straipsnio 2 dalį atidedamas, apribojamas arba jo nepaisoma,

– duomenų subjekto teisė naudotis prieiga prie tvarkomų duomenų visiškai arba iš dalies apribojama, jei toks apribojimas yra būtina ir proporcinga priemonė siekiant, *inter alia*, netrukdyti atlikti oficialius arba teisinius tyrimus ar procedūras arba nepakenkti nusikalstamų veikų tyrimui [36].

102. Bet kuriuo atveju duomenų tvarkymo teisėtumas priklauso ne nuo to, ar kompetentingos institucijos įvykdė Direktyvos 2016/680 13 straipsnyje joms nustatytas (vėlesnes) pareigas, o nuo tvarkymą pateisinančio tikslo teisėtumo, t. y. nuo to, ar administracinės institucijos teisėtai tvarkė asmens duomenis.

103. Vertinant iš šios perspektyvos, aplinkybė, kad duomenų subjektas buvo informuotas apie bandymus gauti prieigą prie duomenų, saugomų areštuotame jo telefone, dėl esminių priežasčių pati savaime neturi reikšmės policijos veiksmų teisėtumui. Duomenų valdytojo elgesys, galimai nesuderinamas su Direktyvos 2016/680 13 straipsnyje jam nustatytomis pareigomis, gali turėti kitų pasekmių, tačiau, kartoju, pats savaime nedaro įtakos to duomenų tvarkymo teisėtumui ar neteisėtumui.

104. Prašymą priimti prejudicinį sprendimą pateikęs teismas turi nustatyti, ar pagal nacionalinę teisę duomenų subjektas gali veiksmingai naudotis minėtomis teisėmis.

V. Išvada

105. Atsižvelgdamas į tai, kas išdėstyta, siūlau Teisingumo Teismui *Landesverwaltungsgericht Tirol* (Tirolio apygardos administracinis teismas, Austrija) prašymą priimti prejudicinį sprendimą pripažinti nepriimtinu.

[36] Šiuo klausimu žr. Sprendimo *Tele2 Sverige ir Watson* 121 punktą. Jame įtvirtinta su Direktyva 2002/58 susijusi jurisprudencija taikoma ir Direktyvos 2016/680 atveju, siekiant užtikrinti teismines tvarkomų duomenų turėtojų teisių gynimo priemones.

Kaip alternatyvą dėl šio prašymo siūlau pateikti tokį atsakymą:

1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuri[a] panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, 4 straipsnio 1 dalies a punktas ir 8 straipsnio 1 dalis, siejami su Europos Sąjungos pagrindinių teisių chartijos 7, 8 ir 52 straipsniais,

   turi būti aiškinami taip:

   atliekant nusikalstamos veikos tyrimą prieiga prie mobiliajame telefone saugomų asmens duomenų, siekiant juos tvarkyti, valdžios institucijoms suteikiama ne tik kovos su sunkiais nusikaltimais atvejais.

   Tokia prieiga kiekvienu atveju turi būti pagrįsta ir suteikta tik tiek, kiek griežtai būtina ir proporcinga, atsižvelgiant į nusikalstamų veikų, dėl kurių vykdomas persekiojimas, ir asmens duomenų, prie kurių siekiama gauti prieigą, pobūdį.

   Vykdydamos nusikalstamos veikos tyrimą policijos institucijos be išankstinio teismo leidimo pačios negali gauti visiškos ir nekontroliuojamos prieigos prie visų mobiliajame telefone saugomų duomenų, kai iš šių duomenų galima susidaryti tikslų vaizdą apie asmens privatų gyvenimą.

2. Direktyvos 2016/680 13, 15 ir 54 straipsniai, siejami su Chartijos 47 ir 52 straipsniais,

   turi būti aiškinami taip:

   nedarant poveikio Direktyvos 2016/680 15 straipsnio 1 dalyje leidžiamiems apribojimams arba kitoms galimoms administracinėms ar neteisminėms teisių gynimo priemonėms, mobiliojo telefono turėtojas turi būti informuotas apie tai, kad atitinkamos institucijos tvarko jo telefone saugomus asmens duomenis, tokiu metu ir tokiomis sąlygomis, kurių reikia siekiant užtikrinti, kad jis veiksmingai pasinaudotų teise prašyti teisminės teisių apsaugos dėl galimo Direktyvoje 2016/680 pripažintų teisių pažeidimo.