GENERALINIO ADVOKATO
MANUEL CAMPOS SÁNCHEZ-BORDONA IŠVADA,
pateikta 2016 m. gegužės 12 d.[1]

Byla C-582/14

Patrick Breyer
prieš
Vokietijos Federacinę Respubliką

(Bundesgerichtshof (Aukščiausiasis federalinis teismas, Vokietija) pateiktas prašymas priimti prejudicinį sprendimą)

„Asmens duomenų tvarkymas — Direktyva 95/46 — 2 straipsnio a punktas ir 7 straipsnio f punktas — Sąvoka „asmens duomenys“ — IP adresai — Elektroninių ryšių paslaugų teikėjų atliekamas saugojimas — Nacionalinės teisės aktai, pagal kuriuos neleidžiama atsižvelgti į duomenų valdytojo teisėtus interesus“

1. Interneto protokolo (IP) adresai yra įrenginiams (kompiuteriams, planšetiniams kompiuteriams, išmaniesiems telefonams) priskirtos binarinės skaitmenų sekos, kurios juos identifikuoja ir leidžia jiems prisijungti prie elektroninių telekomunikacijų tinklo. Tam, kad prisijungtų prie interneto, įrenginys turi naudoti interneto prieigos paslaugų teikėjų suteiktą skaitmenų seką. IP adresas perduodamas serveriui su išsaugotu interneto puslapiu, kuriame apsilankoma.

2. Konkrečiai kalbant, interneto prieigos paslaugų teikėjai (paprastai telefono ryšio bendrovės) laikinai suteikia savo klientams vadinamuosius dinamiškus IP adresus kiekvieno prisijungimo prie interneto atveju ir juos keičia per paskesnius prisijungimus. Tokios bendrovės turi registrą, kuriame mato, koks IP adresas tam tikru momentu buvo suteiktas konkrečiam įrenginiui[2].

3. Interneto puslapių, prie kurių prisijungiama naudojantis dinamiškais IP adresais, savininkai taip pat turi registrus, iš kurių matyti, kokiuose puslapiuose, kada ir iš kokio dinamiško IP adreso buvo apsilankyta. Techniniu požiūriu, naudotojui atsijungus nuo interneto tokie įrašai gali būti saugomi neribotą laiką.

4. Vien dinamiško IP adreso nepakanka tam, kad paslaugos teikėjas nustatytų savo interneto puslapio naudotoją. Tai įmanoma padaryti derinant dinamišką IP adresą su kita papildoma prieigos prie tinklo paslaugos teikėjo turima informacija.

1 — Originalo kalba: ispanų.

2 — 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvos 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančios Direktyvą 2002/58/EB (OL L 105, 2006, p. 54) 5 straipsnyje, be kitų pareigų, numatyta pareiga tyrimo, atskleidimo ir nubaudimo už sunkius pažeidimus tikslu saugoti tokius duomenis, kokie yra „prisijungimo prie interneto ir atsijungimo nuo interneto prieigos paslaugų data ir laikas <...> ir dinamiškas ar statiškas interneto protokolo (IP) adresas, kurį ryšiui suteikė prieigos prie interneto paslaugos teikėjas, ir abonento ar registruoto naudotojo atpažinimo kodas“.

5. Šioje byloje nesutariama, ar dinamiški IP adresai yra asmens duomenys, kaip jie suprantami pagal Direktyvos 95/46/EB 2 straipsnio a punktą[3]. Norint atsakyti į šį klausimą, pirmiausiai reikia įvertinti, kokią reikšmę tam turi aplinkybė, kad naudotojui nustatyti būtiną papildomą informaciją turi ne interneto puslapio savininkas, bet trečioji šalis (konkrečiai – prieigos prie tinklo paslaugos teikėjas).

6. Teisingumo Teismas dar nėra nagrinėjęs šio klausimo, nors Sprendimo *Scarlet Extended*[4] punkte pripažino, kad IP adresai „yra saugomų asmens duomenų dalis, nes leidžia tiksliai nustatyti tokius vartotojus“; minėtas sprendimas susijęs su situacija, kai IP adresus rinko ir nustatė prieigos prie tinklo teikėjas[5], o ne turinio teikėjas, kaip yra šiuo atveju.

7. Jeigu interneto paslaugų teikėjui dinamiški IP adresai būtų asmens duomenys, toliau reikėtų nagrinėti, ar jų tvarkymas patenka į Direktyvos 95/46 taikymo sritį.

8. Net jei tai būtų asmens duomenys, gali būti, kad Direktyvoje 95/46 numatyta apsauga jiems netaikoma, jeigu, pavyzdžiui, jie būtų tvarkomi siekiant vykdyti galimų įsibrovėlių į interneto puslapį baudžiamąjį persekiojimą. Tokiu atveju Direktyva 95/46 netaikoma pagal 3 straipsnio 2 dalies pirmą įtrauką.

9. Be to, reikia nustatyti, ar paslaugų teikėjas, registruojantis dinamiškus IP adresus tada, kai naudotojas prisijungia prie jo interneto puslapių (šiuo atveju Vokietijos Federacinė Respublika), veikia kaip viešosios valdžios subjektas, ar veikiau kaip privatus asmuo.

10. Jei Direktyva 95/46 būtų taikoma, reikėtų patikslinti, kiek su 7 straipsnio f punktu suderinama nacionalinė teisės norma, kuri riboja vienos iš minėtame punkte įtvirtintų sąlygų, kuriomis pateisinamas asmens duomenų tvarkymas, taikymo sritį.

I – Teisinis pagrindas

A – *Sąjungos teisė*

11. Direktyvos 95/46 26 konstatuojamojoje dalyje nustatyta:

„(26) kadangi apsaugos principai turi būti taikomi visai informacijai apie asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta; kadangi norint nustatyti, ar asmens tapatybė gali būti nustatyta, reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti; kadangi apsaugos principai netaikomi duomenims, kurie paversti anoniminiais tokiu būdu, kad duomenų subjekto tapatybė nebegali būti nustatyta; kadangi šiuo tikslu etikos kodeksai, apibrėžti 27 straipsnyje, gali būti naudinga priemonė, nurodant, kaip duomenys galėtų būti paversti anoniminiais ir išlaikyti tokio pavidalo, kad duomenų subjekto tapatybės nebebūtų įmanoma nustatyti.“

12. Direktyvos 95/46 1 straipsnyje nustatyta:

„1. Pagal šią direktyvą valstybės narės saugo fizinių asmenų pagrindines teises ir laisves, o ypač jų privatumo teisę tvarkant asmens duomenis.“

3 — 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k., 13 sk., 15 t., p. 355).

4 — 2011 m. lapkričio 24 d. sprendimo (C-70/10, EU:C:2011:771) 51 punktas.

5 — Tokia pati situacija nagrinėta 2012 m. balandžio 19 d. Sprendime *Bonnier Audio ir kt.* (C-461/10, EU:C:2012:219, 51 ir 52 punktai).

2. Valstybės narės nevaržo ir nedraudžia laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su apsauga, skiriama pagal šio straipsnio 1 dalį.“

13. Direktyvos 95/46 2 straipsnyje nustatyta:

„Šioje direktyvoje:

a) „asmens duomenys“ reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais;

b) „asmens duomenų tvarkymas“ (tvarkymas) reiškia bet kurią operaciją ar operacijų rinkinį, automatiniais arba neautomatiniais būdais atliekamus 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;

<...>

d) „duomenų valdytojas“ reiškia tokį fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus; jeigu tvarkymo tikslus ir būdus nusako nacionaliniai arba Bendrijos įstatymai bei norminiai aktai, tai duomenų valdytoją arba specifinius kriterijus, pagal kuriuos skiriamas duomenų valdytojas, gali apibrėžti nacionaliniai arba Bendrijos įstatymai;

<...>

f) „trečioji šalis“ reiškia bet kurį fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, nesantį duomenų subjektu, duomenų valdytoju ar duomenų tvarkytoju, arba tokiu asmeniu, kuriam leidžiama tvarkyti duomenis, tiesiogiai įgaliotam duomenų valdytojo ar duomenų tvarkytojo;

<...>.“

14. Pagal Direktyvos 95/46 3 straipsnį „Taikymo sritis“:

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

2. Ši direktyva netaikoma tvarkant asmens duomenis:

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

<...>.“

15. Direktyvos 95/46 II skyrius, kuriame numatytos „Bendrosios asmens duomenų tvarkymo teisėtumo taisyklės“, pradedamas 5 straipsniu, kuriame numatyta, kad „[k]iek leidžia šio skyriaus nuostatos, valstybės narės tiksliau apibrėžia sąlygas, kuriomis asmens duomenų tvarkymas yra teisėtas“.

16. Pagal Direktyvos 95/46 6 straipsnį:

„1. Valstybės narės numato, kad asmens duomenys turi būti:

a) tvarkomi teisingai ir teisėtai;

b) surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to [paskui] tvarkomi su šiais tikslais suderintais būdais. Tolesnis duomenų tvarkymas istoriniais, statistiniais ar moksl[o] tikslais laikomas suderinamu dalyku, su sąlyga, kad valstybės narės numato atitinkamas apsaugos priemones;

c) adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi;

d) tikslūs ir, jei būtina, nuolat atnaujinami; turi būti imtasi visų reikalingų priemonių, kad duomenys, kurie yra netikslūs ar neišsamūs, palyginti su tikslais, dėl kurių jie buvo surinkti ar po to tvarkomi, būtų ištrinti arba ištaisyti;

e) laikomi tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi. Valstybės narės išdėsto asmens duomenų, ilgesnį laiką saugomų dėl istorinės, statistinės ar mokslinės paskirties, atitinkamas apsaugos priemones.

2. Duomenų valdytojo pareiga užtikrinti, kad būtų laikomasi šio straipsnio 1 dalies.“

17. Pagal Direktyvos 95/46 7 straipsnį:

„Valstybės narės numato, kad asmens duomenis galima tvarkyti tik tuo atveju, jeigu:

a) duomenų subjektas yra nedviprasmiškai davęs sutikimą;

b) tvarkyti reikia vykdant sutartį, kai duomenų subjektas yra viena iš šalių, arba duomenų subjektui paprašius būtų imtasi priemonių prieš sudarant sutartį, arba

c) tvarkyti reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui;

d) tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus;

e) tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui, arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai atskleidžiami duomenys; arba

f) tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto, kuriam pagal 1 straipsnio 1 dalį reikalinga apsauga, teisės ir laisvės yra viršesnės nei šie interesai.“

18. Direktyvos 95/46 13 straipsnyje numatyta:

„1. Valstybės narės gali priimti teisines priemones, kad apribotų 6 straipsnio 1 dalyje, 10 straipsnyje, 11 straipsnio 1 dalyje bei 12 ir 21 straipsniuose numatytų prievolių ir teisių mastą, kai toks apribojimas yra reikalinga apsaugos priemonė norint užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

d) kriminalinių nusikaltimų bei reglamentuojamų profesijų etikos pažeidimų prevenciją, tyrimą, išaiškinimą ir persekiojimą;

e) svarbius ekonominius ar finansinius valstybės narės ar Europos Sąjungos interesus, įskaitant ir monetarinius, biudžeto ar mokesčių klausimus;

f) kontrolės, tikrinimo ar taisyklių nustatymo funkciją, kuri susijusi, bent atsitiktinai, su įgaliojimų vykdymu c, d ir e punktuose nurodytais atvejais;

g) duomenų subjekto apsaugą arba kitų asmenų teisių ir laisvių apsaugą.

<...>“

B – *Nacionalinė teisė*

19. *Telemediengesetz* (Elektroninių paslaugų įstatymas, toliau – TMG) 12 straipsnyje [6] numatyta:

„1. Teikdamas elektroninę paslaugą paslaugų teikėjas gali rinkti ir panaudoti asmens duomenis tik tuo atveju, kai tai leidžiama pagal šį įstatymą ar kitą teisės aktą, aiškiai reglamentuojantį elektronines paslaugas, arba kai naudotojas su tuo sutiko.

2. Paslaugų teikėjas asmens duomenis, surinktus teikiant elektroninę paslaugą, gali panaudoti kitiems tikslams tik tuo atveju, kai tai leidžiama pagal šį įstatymą ar kitą teisės aktą, aiškiai reglamentuojantį elektronines paslaugas, arba kai naudotojas su tuo sutiko.

3. Jei nenustatyta kitaip, taikomi galiojantys asmens duomenų apsaugos srities teisės aktai, net kai duomenys nėra apdorojami automatiškai.“

20. Pagal TMG 15 straipsnį:

„1. Paslaugų teikėjas gali rinkti ir panaudoti naudotojo asmens duomenis tik tuo atveju, kai tai būtina siekiant suteikti galimybę naudotis elektroninėmis paslaugomis ir atsiskaityti už jas (naudojimosi duomenys). Naudojimosi duomenys visų pirma yra šie:

1. požymiai, padedantys identifikuoti naudotoją,

2. informacija apie naudojimosi pradžią, pabaigą ir trukmę,

3. informacija apie elektronines paslaugas, kuriomis naudotojas naudojosi.

6 — 2007 m. vasario 26 d. įstatymas (BGBl, 2007 I, p. 179).

2. Paslaugų teikėjas gali derinti naudotojo naudojimosi duomenis, susijusius su įvairiomis elektroninėmis paslaugomis, jei tai būtina siekiant, kad naudotojas atsiskaitytų už tas paslaugas.

<...>

4. Paslaugų teikėjas gali panaudoti naudojimosi duomenis baigus naudotis paslauga, jei tai būtina siekiant, kad naudotojas atsiskaitytų už tas paslaugas (atsiskaityti reikalingi duomenys). Laikydamasis įstatymuose, nuostatuose ar sutartyse numatytų saugojimo terminų, paslaugų teikėjas gali duomenis užblokuoti. <...>“

21. Pagal *Bundesdatenschutzgesetz* (Federalinis duomenų apsaugos įstatymas, toliau – BDSG) 3 straipsnio 1 dalį[7] „asmens duomenys yra konkretūs duomenys apie fizinio asmens, kurio tapatybė nustatyta arba gali būti nustatyta (duomenų subjektas), asmeninius ar profesinius ryšius <...>“.

II – Faktinės aplinkybės

22. P. Breyer pareiškė ieškinį Vokietijos Federacinei Respublikai siekdamas, kad ši nutrauktų veiksmus, susijusius su IP adresų įrašymu.

23. Dauguma Vokietijos viešosios valdžios įstaigų turi viešai prieinamus interneto portalus, kuriuose pateikiama aktuali informacija. Siekiant išvengti atakų ir suteikti galimybę vykdyti įsibrovėlių baudžiamąjį persekiojimą, daugumoje iš šių portalų visi apsilankymai išsaugomi protokolo rinkmenų sistemose ir registruose. Pasibaigus prisijungimo operacijai, išsaugomi rinkmenos arba interneto puslapio pavadinimas, į paieškos laukelį įvesti paieškos žodžiai, apsilankymo laikas, perduotų duomenų kiekis, pranešimas, ar duomenys gauti sėkmingai, ir kompiuterio, iš kurio atlikta paieška, IP adresas.

24. P. Breyer, kuris lankėsi įvairiuose minėtuose puslapiuose, reikalavo įpareigoti Federacinę Respubliką nebeįrašyti arba nebeleisti trečiosioms šalims įrašyti *host* sistemos, iš kurios atliktos paieškos, IP adresų, jei tai nebūtina siekiant atkurti galimybę vėl naudotis telekomunikacijų paslaugomis sutrikimų atvejais.

25. Pirmojoje instancijoje P. Breyer ieškinys buvo atmestas. Jo apeliacinis skundas buvo patenkintas iš dalies; Federacinei Respublikai buvo leista informaciją išsaugoti iki kiekvienos prisijungimo operacijos pabaigos. Nurodymas nutraukti veiksmus buvo pateiktas su sąlyga, kad ieškovas per prisijungimo operaciją pateiks savo asmens duomenis, taip pat elektroninio pašto adresą ir kad išsaugojimas nebus būtinas siekiant atkurti galimybę naudotis telekomunikacijų paslaugomis.

III – Pateikti klausimai

26. Abiem šalims pateikus kasacinį skundą, *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) suformulavo šiuos 2014 m. gruodžio 17 d. pateiktus prejudicinius klausimus:

„1. Ar <...> Direktyvos 95/46/EB <...> 2 straipsnio a punktą reikia aiškinti taip, kad interneto protokolo (IP) adresas, kurį paslaugos teikėjas išsaugo apsilankius jo interneto puslapyje, yra asmens duomenys jau tuo atveju, kai trečioji šalis (šiuo atveju prieigos teikėjas) turi papildomos informacijos, būtinos atitinkamam asmeniui nustatyti?

7 — 1990 m. gruodžio 20 d. įstatymas (BGBl, 1990 I, p. 2954).

2. Ar pagal Duomenų apsaugos direktyvos 7 straipsnio f punktą draudžiama nacionalinės teisės nuostata, pagal kurią paslaugos teikėjas naudotojo asmens duomenis be jo sutikimo gali rinkti ir naudoti tik tiek, kiek tai būtina siekiant leisti tam naudotojui pasinaudoti konkrečia elektronine paslauga ir atsiskaityti už ją, ir pagal kurią tikslas užtikrinti bendrą elektroninių paslaugų veikimą negali pateisinti duomenų naudojimo pasibaigus konkrečiai naudojimosi operacijai?“

27. Remiantis prašymą priimti prejudicinį sprendimą pateikusio teismo paaiškinimais, pagal Vokietijos teisę ieškovas galėtų reikalauti nebeįrašyti IP adresų, jeigu išsaugojus IP adresą neleistinai pažeidžiama, remiantis teisės aktais dėl duomenų apsaugos, jo teisė į privatumą, konkrečiai – jo teisė „pačiam tvarkyti savo asmens duomenis“ (*Bürgerliches Gesetzbuch* (Vokietijos Civilinis kodeksas) 1004 straipsnio 1 dalis ir 823 straipsnio 1 dalis, siejamos su *Grundgesetz* (Konstitucija) 1 ir 2 straipsniais).

28. Taip būtų, jei: a) IP adresas (bet kuriuo atveju kartu su apsilankymo interneto puslapyje momentu) būtų priskirtas prie „asmens duomenų“, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą, siejamą su jos 26 konstatuojamosios dalies antru sakiniu, ir TMG 12 straipsnio 1 ir 3 dalis, siejamas su BDSG 3 straipsnio 1 dalimi; ir b) jei nėra jokio pagrindo duoti leidimo, kaip tai suprantama pagal Direktyvos 95/46 7 straipsnio f punktą ir TMG 12 straipsnio 1 ir 3 dalis bei 15 straipsnio 1 ir 4 dalis.

29. *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nuomone, aiškinant nacionalinę teisę (TMG 12 straipsnio 1 dalį) svarbu tai, kaip turi būti suprantami asmens duomenys, į kuriuos daroma nuoroda Direktyvos 95/46 2 straipsnio a punkte.

30. Be to, teismas *a quo* nurodo, kad pagal TMG 15 straipsnio 1 dalį paslaugų teikėjas gali rinkti ir panaudoti naudotojo asmens duomenis tik tuo atveju, kai tai būtina siekiant suteikti galimybę naudotis elektronine paslauga ir atsiskaityti už ją (naudojimosi duomenys) [8], todėl tokios nacionalinės teisės nuostatos aiškinimas yra susijęs su Direktyvos 95/46 7 straipsnio f punkto aiškinimu.

IV – Procesas Teisingumo Teisme. Šalių argumentai

31. Vokietijos, Austrijos ir Portugalijos vyriausybės bei Komisija pateikė rašytines pastabas. Tik Komisija ir P. Breyer dalyvavo 2016 m. vasario 25 d. vykusiame viešame posėdyje. Vokietijos vyriausybė minėtame posėdyje dalyvauti atsisakė.

A – *Šalių argumentai dėl pirmojo klausimo*

32. P. Breyer nuomone, asmens duomenimis laikomi ir tokie duomenys, kurių derinys galimas tik teoriniu požiūriu, t. y. kai remiamasi abstrakčiu galimu pavojumi, ir nesvarbu tai, ar toks derinys buvo praktikoje. Jo nuomone tai, kad institucija santykinai negalėtų nustatyti asmens pagal IP adresą, nereiškia, jog nekyla pavojus minėtam asmeniui. Be to, jis mano, kad svarbi aplinkybė, jog Vokietija išsaugo jo IP adresus tam, kad prireikus nustatytų galimas atakas ar pradėtų baudžiamąjį persekiojimą pagal *Telekommunikationsgesetz* (Telekomunikacijų įstatymas) 113 straipsnį, kaip jau ne kartą buvo daroma.

33. Vokietijos vyriausybė mano, kad į pirmąjį klausimą reikia atsakyti neigiamai. Ji tvirtina, kad dinamiški IP adresai neatskleidžia asmens, „kurio tapatybė yra nustatyta“, kaip tai suprantama pagal Direktyvos 95/46 2 straipsnio a punktą. Vertinant, ar jie pateikia informacijos apie asmenį, „kurio tapatybė gali būti nustatyta“, kaip tai suprantama pagal tą pačią nuostatą, reikia atlikti „galėjimo

8 — *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nuomone, naudojimusi duomenimis laikoma informacija, padedanti nustatyti naudotoją, informacija apie naudojimosi pradžią, pabaigą ir trukmę, informacija apie elektronines paslaugas, kuriomis naudotojas naudojosi.

identifikuoti“ taikant „santykinį“ kriterijų patikrinimą. Tai, jos nuomone, matyti iš Direktyvos 95/46 26 konstatuojamosios dalies, pagal kurią reikėtų atsižvelgti tik į priemones, kuriomis galėtų [„pagrįstai“] pasinaudoti duomenų valdytojas ar trečioji šalis asmens tapatybei nustatyti. Toks patikslinimas rodo, kad Sąjungos teisės aktų leidėjas neketino į Direktyvos 95/46 taikymo sritį įtraukti tokių situacijų, kai nustatymą gali atlikti bet kuri trečioji šalis.

34. Be to, Vokietijos vyriausybė mano, kad Direktyvos 95/46 2 straipsnio a punkte apibrėžta sąvoka „asmens duomenys“ turi būti aiškinama atsižvelgiant į šios direktyvos tikslą užtikrinti, jog bus laikomasi pagrindinių teisių. Būtinybė apsaugoti fizinius asmenis gali būti skirtingai vertinama pagal tai, kas turi duomenis, ir ar esama priemonių, kuriomis naudojantis būtų galima minėtus asmenis nustatyti.

35. Vokietijos vyriausybė tvirtina, kad P. Breyer negali būti nustatytas pagal IP adresus, derinamus su kitais duomenimis, kuriuos išsaugo turinio teikėjai. Tam reikėtų informacijos, kurią turi prieigos prie interneto paslaugos teikėjai, kurie, neturėdami teisėto pagrindo, negali jos suteikti turinio teikėjams.

36. Austrijos vyriausybės nuomone, atvirkščiai, atsakymas turėtų būti teigiamas. Pagal Direktyvos 95/46 26 konstatuojamąją dalį tam, kad asmuo būtų laikomas asmeniu, kurio tapatybė gali būti nustatyta, nereikalaujama, kad visą informaciją, padedančią jį nustatyti, turėtų tik vienas subjektas. Taigi IP adresas galėtų būti laikomas asmens duomenimis, jeigu trečioji šalis (pavyzdžiui, prieigos prie interneto paslaugos teikėjas) turi priemones, leidžiančias nustatyti tokio IP adreso savininką be pernelyg didelių pastangų.

37. Portugalijos vyriausybė taip pat mano, kad atsakymas turėtų būti teigiamas, ir nurodo, jog IP adresas, derinamas su apsilankymo interneto puslapyje data, yra asmens duomenys tiek, kiek dėl jo subjektas, kuris nėra IP adresą išsaugojęs subjektas, gali nustatyti naudotoją.

38. Komisija taip pat siūlo pateikti teigiamą atsakymą ir remiasi Teisingumo Teismo sprendimu byloje *Scarlet Extended*[9] . Komisijos nuomone, dėl to, kad IP adresų išsaugojimas skirtas konkrečiai naudotojams nustatyti kibernetinių atakų atveju, papildomos informacijos, kurią išsaugo prieigos prie interneto paslaugų teikėjai, naudojimas laikytinas priemone, kuri gali būti „pagrįstai“ naudojama pagal Direktyvos 95/46 26 konstatuojamąją dalį. Galiausiai Komisija tvirtina, kad ir iš šios direktyvos siekiamo tikslo, ir iš Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7 ir 8 straipsnių matyti, kad Direktyvos 95/46 2 straipsnio a punktas turi būti aiškinamas plačiai.

B – *Šalių argumentai dėl antrojo klausimo*

39. P. Breyer mano, kad Direktyvos 95/46 7 straipsnio f punktas yra bendro pobūdžio nuostata, kurią praktikoje reikia sukonkretinti. Remiantis Teisingumo Teismo praktika, konkrečiu atveju reikia įvertinti ir nustatyti, ar yra teisėtų interesų, kaip tai suprantama pagal šią nuostatą, turinčių grupių žinant, jog tam, kad būtų galima taikyti šią nuostatą, ne tik leidžiama, bet ir būtina tokioms grupėms įtvirtinti specialias nuostatas. Šiuo atveju, o taip mano ir P. Breyer, nacionalinės teisės aktai būtų suderinami su Direktyvos 95/46 7 straipsnio f punktu, jeigu viešas portalas nesuinteresuotas išsaugoti asmens duomenis arba jeigu svarbesnis yra suinteresuotumas apsaugoti anonimiškumą. Jo nuomone, nuolatinis ir asmeninio pobūdžio informacijos išsaugojimas nesuderinamas su demokratine visuomene, nėra būtinas ir neproporcingas siekiant užtikrinti elektroninių priemonių veikimą, nes, kaip patvirtina kai kurių federalinių ministerijų interneto puslapiai, jis puikiai įmanomas neišsaugant šių asmens duomenų.

9 — 2011 m. lapkričio 24 d. sprendimo (C-70/10, EU:C:2011:771) 51 punktas.

40. Vokietijos vyriausybė tvirtina, kad nereikia atsakyti į antrąjį klausimą, kuris teikiamas tuo atveju, jeigu į pirmąjį klausimą būtų atsakyta teigiamai; jos nuomone, šiuo atveju taip nėra dėl pirma išdėstytų motyvų.

41. Austrijos vyriausybė siūlo atsakyti taip, kad Direktyva 95/46 nenumato bendro draudimo išsaugoti tokios informacijos, kaip nagrinėjamoji pagrindinėje byloje, kai tai būtina siekiant užtikrinti gerą elektroninių priemonių veikimą. Šios vyriausybės nuomone, ribojimas IP adresą saugoti ilgiau, nei trunka apsilankymas interneto puslapyje, gali būti teisėtas, jeigu laikomasi asmens duomenų valdytojo pareigos taikyti tokių duomenų apsaugos priemones, kaip numatyta Direktyvos 95/46 17 straipsnio 1 dalyje. Kova su kibernetinėmis atakomis gali pateisinti informacijos, susijusios su ankstesnėmis atakomis, analizavimą ir draudimą tam tikriems IP adresams patekti į interneto puslapį. Atsižvelgiant į tikslą garantuoti gerą elektroninių priemonių veikimą, tokių nagrinėjamų duomenų, kaip pagrindinėje byloje, išsaugojimo proporcingumas turėtų būti vertinamas kiekvienu konkrečiu atveju, remiantis Direktyvos 95/46 6 straipsnio 1 dalyje įtvirtintais principais.

42. Portugalijos vyriausybė tvirtina, kad Direktyvos 95/46 7 straipsnio f punktas nedraudžia pagrindinėje byloje nagrinėjamų nacionalinės teisės normų, nes Vokietijos teisės aktų leidėjas jau palygino, kaip reikalaujama pagal minėtą nuostatą, asmens duomenų valdytojo teisėtus interesus ir minėtų duomenų savininko teises bei laisves.

43. Komisijos nuomone, nacionalinėje teisės normoje, kuri perkelia direktyvos 7 straipsnio f punktą, asmens duomenų tvarkymo tikslai turi būti apibrėžti taip, kad konkretus duomenų subjektas juos suvoktų. Ji tvirtina, kad Vokietijos teisės normos neatitinka šio reikalavimo nes pagal TMG 15 straipsnio 1 dalį išsaugoti IP adresus leidžiama, „kai tai būtina siekiant suteikti galimybę naudotis elektroninėmis paslaugomis <...> “.

44. Taigi Komisija siūlo į antrąjį klausimą pateikti tokį atsakymą: ši nuostata draudžia nacionalinės teisės nuostatą aiškinti taip, kad viešosios valdžios įstaiga, veikianti kaip paslaugų teikėja, gali rinkti ir naudoti naudotojo asmens duomenis be jo sutikimo, net jeigu siekiamas tikslas yra užtikrinti gerą elektroninės priemonės veikimą, jeigu minėtoje nacionalinės teisės nuostatoje toks tikslas neįtvirtintas pakankamai aiškiai ir tiksliai.

V – Vertinimas

A – *Pirmasis klausimas*

1. Pateikto klausimo ribų nustatymas

45. Kaip matyti iš *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) pateikto pirmojo prejudicinio klausimo formuluotės, juo siekiama išsiaiškinti, ar IP adresas, kuriuo naudojantis patenkama į interneto puslapį, viešosios valdžios subjektui, to puslapio savininkui, yra asmens duomenys (kaip tai suprantama pagal Direktyvos 95/46/EB 2 straipsnio a punktą), kai prieigos prie interneto tinklo paslaugos teikėjas turi papildomos informacijos, leidžiančios nustatyti duomenų subjektą.

46. Taip suformuluotas klausimas yra pakankamai tikslus, kad būtų galima iš karto atmesti kitus klausimus, kuriais *in abstracto* klausiama apie teisinį IP adresų statusą atsižvelgiant į asmens duomenų apsaugą.

47. Pirmiausiai *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nurodo tik „dinamiškus IP adresus“, t. y. tuos, kurie laikinai priskiriami kiekvieno prisijungimo prie tinklo atveju ir keičiasi vėlesnių prisijungimų atveju. Nenurodomi „fiksuoti arba statiški IP adresai“, kurie nesikeičia ir nuolat leidžia identifikuoti prie tinklo prisijungusį įrenginį.

48. Antra, prašymą priimti prejudicinį sprendimą pateikęs teismas remiasi prielaida, kad interneto puslapio teikėjas proceso *a quo* metu neturi galimybės pagal dinamišką IP adresą nustatyti, kas lankosi jo puslapiuose, ir neturi papildomos informacijos, kuri, suderinta su IP adresu, leistų nustatyti naudotoją. Panašu, kad šiomis aplinkybėmis *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) mano, jog *interneto puslapio teikėjui* dinamiškas IP adresas nėra asmens duomenys, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą.

49. Prašymą priimti prejudicinį sprendimą pateikęs teismas abejoja dėl to, ar dinamiški IP adresai interneto puslapio teikėjui gali būti asmens duomenys, *jeigu trečioji šalis turi papildomos informacijos*, iš kurios kartu su minėtais adresais būtų galima nustatyti, kas lankosi jo puslapiuose. Įdomiausia tai, kad *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nurodo ne bet kokią asmens duomenų turinčią trečiąją šalį, o tik prieigos prie tinklo teikėją (taigi neatsižvelgiama į kitus potencialius tokios rūšies informacijos turėtojus).

50. Taigi neanalizuojami, be kita ko, šie klausimai: a) ar statiški IP adresai yra asmens duomenys pagal Direktyvą 95/46[10]; b) ar dinamiški IP adresai visada ir bet kokiomis aplinkybėmis yra asmens duomenys, kaip jie suprantami pagal šią direktyvą; ir galiausiai c) ar dinamiškus IP adresus neišvengiamai reikia laikyti asmens duomenimis tada, kai yra bet kokia trečioji šalis, galinti juos panaudoti tinklo naudotojams nustatyti.

51. Kalbama tik apie tai, ar dinamiškas IP adresas interneto paslaugos teikėjui yra asmens duomenys, kai prieigos prie tinklo paslaugą teikianti ryšių bendrovė (prieigos teikėjas) turi papildomos informacijos, kuri, suderinta su tokiu adresu, leidžia nustatyti, kas lankosi interneto paslaugos teikėjo administruojamame interneto puslapyje.

2. Dėl esmės

52. Dėl šiame prašyme priimti prejudicinį sprendimą keliamo klausimo aktyviai diskutuojama Vokietijos teisės doktrinoje ir teismų praktikoje. Galima skirti dvi nuomones[11]. Pagal vieną iš jų (kurioje remiamasi „objektyviu“ arba „absoliučiu“ kriterijumi) naudotojas laikomas tokiu, kurio tapatybę galima nustatyti ir dėl to IP adresas yra saugomi asmens duomenys, kai, neatsižvelgiant į interneto paslaugos teikėjo gebėjimus ir priemones, jį nustatyti galima suderinus jo dinamišką IP adresą su trečiosios šalies (pavyzdžiui, prieigos prie tinklo teikėjo) pateikta informacija.

53. Kitos srovės šalininkai (kurie remiasi „santykiniu“ kriterijumi) mano, kad galimybės tikėtis trečiosios šalies pagalbos nustatant naudotoją nepakanka tam, kad dinamiškas IP adresas būtų pripažintas asmens duomenimis. Svarbus yra to, kas turi prieigą prie informacijos, gebėjimas ja pasinaudoti savo turimomis priemonėmis ir taip nustatyti asmenį.

10 — Šią problemą Teisingumo Teismas sprendė 2011 m. lapkričio 24 d. Sprendimo *Scarlet Extended* (C-70/10, EU:C:2011:771) 51 punkte ir 2012 m. balandžio 19 d. Sprendime *Bonnier Audio ir kt.* (C-461/10, EU:C:2012:219). Pastarojo sprendimo 51 ir 52 punktuose Teisingumo Teismas padarė išvadą, kad „interneto <...> naudotojo, naudojančio IP adresą, iš kurio, kaip preziumuojama, buvo neteisėtai siunčiamos saugomų kūrinių rinkmenos, asmenvard[žio] ir adres[o] pateikimas, siekiant nustatyti jo tapatybę, yra asmens duomenų tvarkymas pagal Direktyvos 2002/58 2 straipsnio pirmą dalį, siejamą su Direktyvos 95/46 2 straipsnio b punktu“.

11 — Dėl abiejų doktrinos srovių žr., pavyzdžiui, M. Schreibauer „Kommentar zum Bundesdatenschutzgesetz“; M. Esser, P. Kramer ir K. von Lewinski „Nebengesetze“, (leid.) *Carl Heymanns Verlag / Wolters Kluwer*, Kelnas, 2014, 4-asis leidimas, § 11 *Telemediengesetz* (4–10); J. Nink ir J. Pohle „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze“, *Multimedia und Recht*, 9/2015, p. 563–567; J. Heidrich ir C. Wegener „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging“, *Multimedia und Recht*, 8/2015, p. 487–492; H. Leisterer „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr“, *Computer und Recht*, 10/2015, p. 665–670.

54. Nesvarbu, kaip šis ginčas būtų išspręstas pagal nacionalinę teisę, Teisingumo Teismas turi tik išaiškinti dvi Direktyvos 95/46 nuostatas, kurias nurodė ir teismas *a quo*, ir proceso šalys, t. y. 2 straipsnio a punktą [12] ir 26 konstatuojamąją dalį [13].

55. Vien dėl to, kad dinamiški IP adresai suteikia informaciją apie apsilankymo interneto puslapyje, naudojantis kompiuteriu (ar kitu įrenginiu), datą ir laiką, atskleidžiami tam tikri interneto naudotojų elgesio įpročiai ir galimai pažeidžiama jų teisė į privatų gyvenimą [14], kuri garantuojama pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnį ir Chartijos 7 straipsnį; Direktyva turi būti aiškinama atsižvelgiant į šiuos straipsnius ir jos pačios 8 straipsnį [15]. Iš tikrųjų bylos šalys neginčija šios prielaidos, kuri nėra prejudicinio klausimo dalykas.

56. Asmuo, su kuriuo susijusi minėta informacija, nėra „asmuo, kurio tapatybė yra nustatyta“. Prisijungimo data ir laikas, taip pat jų skaitmeninis pobūdis tiesiogiai ir nedelsiant neatskleidžia fizinio asmens, kuriam priklauso įrenginys, iš kurio lankomasi interneto puslapyje, nei jį naudojančio naudotojo tapatybės (gali būti bet kuri trečioji šalis).

57. Vis dėlto tiek, kiek dinamiškas IP adresas padeda nustatyti – vienas arba kartu su kita informacija – kam priklauso įrenginys, naudotas lankantis interneto puslapyje, jis gali būti laikomas informacija apie „asmenį, kurio tapatybė gali būti nustatyta“ [16].

58. Kaip matyti iš *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) prašymo priimti prejudicinį sprendimą, vien dinamiško IP adreso nepakanka, kad būtų nustatytas naudotojas, kuris, naudodamasis tokiu adresu, lankėsi interneto puslapyje. Jeigu, priešingai, interneto paslaugos teikėjas galėtų pagal dinamišką IP adresą nustatyti naudotoją, be jokios abejonės, toks adresas būtų laikomas asmens duomenimis, kai jie suprantami pagal Direktyvą 95/46. Tačiau neatrodo, kad taip reikia suprasti prejudicinį klausimą, nes jame nurodoma, jog ginče *a quo* dalyvaujantys interneto paslaugų teikėjai negali nustatyti naudotojo vien pagal dinamišką IP adresą.

59. Suderintas su kita informacija dinamiškas IP adresas padeda „netiesiogiai“ nustatyti naudotoją; šios aplinkybės niekas neginčija. Ar tai, kad gali egzistuoti tokia papildoma informaciją, kurią galima derinti su dinamišku IP adresu, leidžia pripažinti tokį adresą asmens duomenimis, kaip jie suprantami pagal Direktyvą? Reikia išsiaiškinti, ar tam pakanka vien abstrakčios galimybės sužinoti tokią informaciją, o gal, priešingai, reikalinga, kad tokią informaciją turėtų dinamišką IP adresą jau žinantis asmuo arba trečioji šalis?

12 — Pateiktas šios išvados 13 punkte.

13 — Pateiktas šios išvados 11 punkte.

14 — Kaip generalinis advokatas P. Cruz Villalón nurodė savo išvados byloje *Scarlet Extended* (C-70/10, EU:C:2011:255) 76 punkte ir kaip tai supranta Europos duomenų apsaugos priežiūros pareigūnas savo 2010 m. vasario 22 d. nuomonėje dėl šiuo metu vykstančių Europos Sąjungos derybų dėl Kovos su klastojimu prekybos susitarimo (ACTA) (OL C 147, 2010, p. 1, 24 punktas) ir 2010 m. gegužės 10 d. Nuomonėje dėl Europos Parlamento ir Tarybos direktyvos dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria panaikinamas Pamatinis sprendimas 2004/68/TVR (OL C 323, 2010, p. 6, 11 punktas).

15 — Šiuo klausimu žr. 2003 m. gegužės 20 d. Sprendimo *Österreichischer Rundfunk* (C-465/00, C-138/01 ir C-139/01, EU:C:2003:294) 68 punktą ir generalinės advokatės J. Kokott išvados byloje *Promusicae* (C-275/06, EU:C:2007:454) 51 ir paskesnius punktus.

16 — Darytina prielaida, kad, nesant priešingų įrodymų, minėtas asmuo yra tas asmuo, kuris naršė internete ir lankėsi atitinkamame interneto puslapyje. Nepaisant šios prielaidos, informacija apie lankymosi interneto puslapyje datą, laiką ir skaitmeninę kilmę leistų susieti šį apsilankymą su įrenginio savininku ir netiesiogiai – su jo elgesio tinkle įpročiais. Išimtimi galėtų būti laikomi IP adresai, priskirti tokių vietų kaip *ciber cafés* kompiuteriams, kurių anonimiškų naudotojų negalima nustatyti, o toje vietoje sugeneruotų duomenų srautas nesuteikia jokios asmeninės informacijos apie jų savininkus. Be to, tai yra vienintelė principo, kad IP adresai yra asmens duomenys, išimtis, kurią pripažino Direktyva 95/46 sukurta Darbo grupė asmenų apsaugai tvarkant asmens duomenis (vadinamoji 29 straipsnio grupė). Žr. 2007 m. birželio 20 d. Nuomonę 4/2007 dėl asmens duomenų sąvokos, WP 136, prieinamą adresu: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

60. Savo pastabose šalys daugiausiai dėmesio skyrė Direktyvos 95/46 26 konstatuojamosios dalies, kurioje yra žodžių junginys „priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti“ aiškinimui. Prašymą priimti prejudicinį sprendimą pateikusio teismo klausimas nesusijęs su papildoma informacija, kurią turi pagrindinėje byloje dalyvaujantys paslaugų teikėjai. Jis nesusijęs ir su bet kuria trečiąja šalimi, turinčia tokios papildomos informacijos (kuri kartu su dinamišku IP adresu padeda nustatyti naudotoją), o mintyje turimas prieigos prie tinklo teikėjas.

61. Taigi nebūtina, kad šiuo atveju Teisingumo Teismas išanalizuotų visas priemones, kurias atsakovė procese *a quo* galėtų „pagrįstai“ naudoti tam, kad dinamiškus IP adresus būtų galima pripažinti asmens duomenimis. Kadangi *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nurodo tik trečiosios šalies turimą papildomą informaciją, galima daryti išvadą, kad: a) atsakovė neturi tinkamos papildomos informacijos, kuri leistų nustatyti naudotoją; arba b) jeigu turi tokią informaciją, negali pagrįstai šiuo tikslu jos naudoti, nes yra jos valdytoja, kaip tai suprantama pagal Direktyvos 95/46 26 konstatuojamąją dalį.

62. Abi situacijos priklauso nuo faktinio pobūdžio vertinimo, kurį gali atlikti tik prašymą priimti prejudicinį sprendimą pateikęs teismas. Teisingumo Teismas galėtų nurodyti bendro pobūdžio kriterijus, kaip aiškinti žodžių junginį „priemones, kuriomis galėtų pasinaudoti duomenų valdytojas“, jeigu *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) abejotų atsakovės gebėjimu pagrįstai naudotis tinkama papildoma informacija. Kadangi taip nėra, manau, kad Teisingumo Teismas neturi pateikti aiškinimo kriterijų, kurie prašymą priimti prejudicinį sprendimą pateikusiam teismui nėra būtini ir kurių jis neprašė.

63. Pateikto klausimo esmė yra išsiaiškinti, ar tam, kad dinamiški IP adresai būtų pripažinti asmens duomenimis, svarbi aplinkybė, jog labai konkreti trečioji šalis, t. y. prieigos prie interneto teikėjas, turi papildomos informacijos, kurią suderinus su tokiais adresais galima nustatyti naudotoją, kuris lankėsi konkrečiame interneto puslapyje.

64. Vėl reikia nurodyti Direktyvos 95/46 26 konstatuojamąją dalį: žodžių junginys „priemones, kuriomis galėtų [pagrįstai] pasinaudoti <...> *bet kuris kitas asmuo*“ [17] galėtų pagrįsti aiškinimą, jog tam, kad dinamišką IP adresą būtų galima laikyti *eo ipso* asmens duomenimis, pakanka, kad bet kuri trečioji šalis galėtų gauti papildomos informacijos (kurią, siekiant nustatyti asmenį, galima suderinti su dinamišku IP adresu).

65. Dėl tokio plataus aiškinimo asmens duomenimis būtų laikoma visų rūšių informacija, kuri pati savaime būtų nepakankama naudotojui nustatyti. Niekada nebūtų galima visiškai užtikrintai paneigti, kad nėra trečiosios šalies, turinčios papildomos informacijos, kurią galima derinti su minėta informacija ir dėl kurios dėl to būtų galima atskleisti asmens tapatybę.

66. Mano nuomone, galimybė, kad technologinių priemonių tobulėjimas netolimoje ateityje atvers plačias galimybes naudotis vis pažangesniais informacijos gavimo ir tvarkymo įrankiais, pagrindžia priemones, kurių norima imtis privatumui apsaugoti. Buvo stengtasi užtikrinti, kad į duomenų apsaugos sričiai svarbių teisinių kategorijų apibrėžtį patektų pakankamai plačios bei lanksčios elgesio situacijos tam, kad ji apimtų bet kurią įsivaizduojamą situaciją [18].

67. Manau, kad dėl tokio, be kita ko, labai pagrįsto susirūpinimo negali būti neatsižvelgiama į teisės aktų leidėjo ketinimus ir kad sisteminis Direktyvos 95/46 26 konstatuojamosios dalies aiškinimas turi apsiriboti „priemon[ėmis], kuriomis [pagrįstai] galėtų pasinaudoti“ *konkrečios trečiosios šalys*.

17 — Originale neišskirta.

18 — Tokiu apsaugos ir prevencijos tikslu grindžiama 29 straipsnio grupės pozicija, kad, kaip buvo nurodyta, reikia vadovautis principu, jog IP adresai yra asmens duomenys, ir pripažinti, kad išimtis galima tik tuo atveju, kai paslaugos teikėjas gali visiškai užtikrintai nustatyti, kad tai yra adresai, atitinkantys asmenis, kurių tapatybė gali būti nustatyta, o tokie gali būti *ciber café* naudotojai. Žr. 16 išnašą *in fine*.

68. 26 konstatuojamojoje dalyje nurodytos ne bet kokios priemonės, kurias naudoja duomenų valdytojas (šiuo atveju interneto paslaugų teikėjas), o tik tokios, kurias jis gali naudoti „pagrįstai“; atitinkamai reikėtų suprasti, kad teisės aktų leidėjas nurodo tokias „trečiąsias šalis“, kurios *taip pat pagrįstai* gali kreiptis į duomenų valdytoją, nustatymo tikslais siekiantį gauti papildomos informacijos. Taip nebūtų, jeigu susisiekimas su tokiomis trečiosiomis šalimis faktiškai reikalautų labai daug žmogiškųjų ir ekonominių išteklių, būtų praktiškai neįmanomas arba draudžiamas pagal įstatymą. Kita vertus, kaip jau minėta, būtų praktiškai neįmanoma atskirti vienų priemonių nuo kitų, nes visada reikėtų įsivaizduoti situaciją, kurioje atsidurtų trečioji šalis, dabar arba ateityje galinti turėti naudotojui nustatyti svarbios papildomos informacijos, kuri neprieinama interneto paslaugų teikėjui.

69. Kaip minėta, *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nurodoma trečioji šalis yra prieigos prie tinklo teikėjas. Neabejotinai labiausiai pagrįsta manyti, kad būtent jis yra ta trečioji šalis, į kurią paslaugų teikėjas kreipsis konkrečios papildomos informacijos, norėdamas kuo veiksmingiau, praktiškiau ir tiesiogiai nustatyti naudoją, kuris, pasinaudodamas dinamišku IP adresu, lankėsi jo interneto puslapyje. Tai yra ne hipotetinė, nežinoma ir neprieinama trečioji šalis, o vienas pagrindinių interneto tinklo dalyvių, apie kurį žinoma, kad jis tikrai turi informacijos, paslaugų teikėjui reikalingos naudotojui nustatyti. Faktiškai ir, kaip tai nurodė prašymą priimti prejudicinį sprendimą pateikęs teismas, būtent į šią konkrečią trečiąją šalį ketina kreiptis atsakovė pagrindinėje byloje, siekdama gauti jai reikalingos papildomos informacijos.

70. Prieigos prie interneto teikėjas paprastai yra trečioji šalis, apie kurią kalbama Direktyvos 95/46 26 konstatuojamojoje dalyje ir į kurią labiausiai „pagrįstai“ gali kreiptis procese *a quo* dalyvaujantis paslaugų teikėjas. Dar reikia išsiaiškinti, ar tokios trečiosios šalies turimos papildomos informacijos gavimas laikytinas „pagrįstai“ praktiškai įgyvendinamu ir praktikuotinu.

71. Vokietijos vyriausybė tvirtina: kadangi prieigos prie interneto teikėjo turima informacija yra asmens duomenys, ji gali būti pateikiama tik pagal tokių duomenų tvarkymą reglamentuojančius teisės aktus [19].

72. Taigi norint pasinaudoti tokia informacija reikia laikytis asmens duomenims taikytinų teisės aktų. Informacija laikoma gauta „pagrįstai“, jeigu įvykdytos susipažinti su tokios rūšies duomenimis taikomos sąlygos; pirmoji iš jų yra teisinė galimybė šiuos duomenis saugoti ir perduoti juos kitiems. Akivaizdu, kad prieigos prie interneto teikėjas gali atsisakyti pateikti atitinkamą informaciją, tačiau gali būti ir kitaip. Dėl visiškai „pagrįsto“ informacijos perdavimo galimybės dinamiškas IP adresas, remiantis Direktyvos 95/46 26 konstatuojamąja dalimi, interneto paslaugų teikėjui savaime tampa asmens duomenimis.

73. Tai yra teisės aktuose numatyta ir dėl to „pagrįsta“ galimybė. Direktyvoje 95/46 nurodytos informacijos gavimo priemonės turi būti teisėtos [20]. Vokietijos vyriausybė primena, kad tokia savaime suprantama prielaida remiasi prašymą priimti prejudicinį sprendimą pateikęs teismas [21]. Dėl to smarkiai sumažėja teisiškai galimų duomenų gavimo būdų skaičius, nes galimi tik teisėti duomenų gavimo būdai. Tačiau kol jie egzistuoja, kad ir kaip būtų ribojamas praktinis taikymas, jie laikytini „pagrįsta priemone“, kaip tai suprantama pagal Direktyvą 95/46.

74. Todėl manau, kad į pirmąjį klausimą – taip, kaip jį suformulavo *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija), turi būti atsakyta teigiamai. Dinamiškas IP adresas interneto paslaugų teikėjui turėtų būti laikomas asmens duomenimis, atsižvelgiant į tai, kad egzistuoja trečioji šalis (prieigos prie tinklo teikėjas), į kurią galima pagrįstai kreiptis dėl kitos papildomos informacijos, o ši, suderinta su minėtu adresu, leistų nustatyti naudotoją.

19 — Jos rašytinių pastabų 40 ir 45 punktai.

20 — Tokiomis aplinkybėmis nesvarbu, kad gauti asmens duomenis įmanoma *de facto* pažeidžiant duomenų apsaugą reglamentuojančius teisės aktus.

21 — Jos rašytinių pastabų 47 ir 48 punktai.

75. Manau, kad rezultatas, kurį lemtų priešingas sprendimas, tik dar labiau pagrįstų mano siūlomą sprendimą. Jeigu dinamiški IP adresai interneto paslaugų teikėjui nėra asmens duomenys, jis gali juos išsaugoti neapibrėžtu būdu ir bet kuriuo momentu galėtų prašyti prieigos prie interneto teikėjo papildomos informacijos, kad suderinęs ją su dinamišku IP adresu galėtų nustatyti naudotoją. Tokiomis aplinkybėmis, kaip pripažįsta Vokietijos vyriausybė [22], dinamiškas IP adresas taptų asmens duomenimis, kai jame būtų papildomos informacijos, tinkamos nustatyti naudotojui, dėl tuo tikslu jam taikomų duomenų apsaugą reglamentuojančių teisės aktų.

76. Taigi tai yra duomenys, kuriuos išsaugoti galima tol, kol paslaugų teikėjui jie netapo asmens duomenimis. Todėl dinamišką IP adresą teisiškai kvalifikuoti kaip asmens duomenis turėtų paslaugų teikėjas, atsižvelgdamas į galimybę, kad ateityje jis gali nuspręsti naudoti šį adresą tam, kad, suderinęs jį su papildoma informacija, kurią turėtų gauti iš trečiosios šalies, nustatytų naudotoją. Manau, kad pagal Direktyvą 95/46 lemiama yra – pagrįsta – galimybė, kad egzistuoja „prieinama“ trečioji šalis, turinti asmeniui nustatyti būtinų priemonių, o ne realus pasinaudojimas galimybe kreiptis į tokią trečiąją šalį.

77. Net būtų galima pritarti Vokietijos vyriausybės tvirtinimui, kad dinamiškas IP adresas asmens duomenimis tampa tik tada, kai jį gauna prieigos prie interneto paslaugos teikėjas. Tačiau reikėtų sutikti, kad, atsižvelgiant į IP adreso saugojimo laikotarpį, toks kvalifikavimas būtų atliekamas atgaline data ir reikėtų jį laikyti neegzistavusiu, jeigu adresas saugotas ilgesnį laiką nei tas, per kurį tokį adresą buvo galima kvalifikuoti kaip asmens duomenis. Tokiomis aplinkybėmis galimas teisės aktų asmens duomenų apsaugos srityje esmės neatitinkantis rezultatas. Priežastis, pagrindžianti tik laikiną tokių duomenų išsaugojimą, būtų paneigta dėl to, kad galimai per vėlai būtų nustatyta svarbi savybė, kuri buvo būdinga nuo pat pradžių: jų pačių arba kartu su kita informacija galimas panaudojimas kaip priemonės fiziniam asmeniui nustatyti. Taip pat ir dėl šios visiškai praktinės priežasties būtų pagrįsta tokį pobūdį pripažinti nuo pat pradžių.

78. Todėl pirmoji išvada yra tokia, kad Direktyvos 95/46 2 straipsnio a punktą reikia aiškinti taip, jog IP adresas, kurį paslaugų teikėjas išsaugo apsilankius jo interneto puslapyje, jam yra asmens duomenys tiek, kiek prieigos prie (interneto) tinklo teikėjas turi papildomos informacijos, leidžiančios nustatyti duomenų subjektą.

B – *Antrasis klausimas*

79. Antruoju prejudiciniu klausimu *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) nori išsiaiškinti, ar pagal Direktyvos 95/46 7 straipsnio f punktą draudžiama nacionalinės teisės nuostata, pagal kurią naudotojo asmens duomenis be jo sutikimo galima rinkti ir naudoti tik tada, kai tai būtina siekiant leisti tam naudotojui pasinaudoti konkrečia elektronine paslauga ir atsiskaityti už ją, o tikslas užtikrinti paslaugos veikimą negali pateisinti tokių duomenų naudojimo pasibaigus kiekvienai naudojimosi operacijai.

80. Prieš pateikiant atsakymą reikia sukonkretinti *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) pateiktą informaciją, pagal kurią duomenys, dėl kurių kilo ginčas, išsaugomi siekiant užtikrinti gerą pagrindinėje byloje nagrinėjamų interneto puslapių veikimą ir kartu suteikti galimybę vykdyti baudžiamąjį persekiojimą dėl galimų kibernetinių minėtų puslapių atakų.

81. Visų pirma reikia išsiaiškinti, ar tvarkant IP adresus, apie kuriuos kalbama prašyme priimti prejudicinį sprendimą, taikoma Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje numatyta išimtis [23].

22 — Jos rašytinių pastabų 36 punktas.

23 — Į Direktyvos 95/46 taikymo sritį nepatenka „duomenų tvarkymas, susijęs su visuomenės saugumu, gynyba, valstybės saugumu <...> *ir su valstybės veiksmais baudžiamosios teisės srityje*“ (originale neišskirta).

1. Dėl Direktyvos 95/46 taikymo tvarkant duomenis, dėl kurių kilo ginčas

82. Atrodo, kad pagrindinėje byloje Vokietijos Federacinė Respublika veikia tik kaip interneto paslaugų teikėjas, t. y. kaip privatus asmuo (ir, be to, *sine imperio*). Tai reiškia, kad iš principo duomenų, kurie yra šio ginčo dalykas, tvarkymas patenka į Direktyvos 95/46 taikymo sritį.

83. Kaip Teisingumo Teismas nurodė Sprendime *Lindqvist* [24], Direktyvos 95/46 3 straipsnio 2 dalyje nurodytos veiklos rūšys „visais atvejais priskirtinos valstybės ar valstybės institucijų, o ne privačių subjektų veiklos sritims“ [25]. Jeigu už duomenų tvarkymą atsakingas asmuo, kuris, nors ir yra viešosios valdžios subjektas, bet veikia kaip privatus asmuo, taikoma Direktyva 95/46.

84. Prašymą priimti prejudicinį sprendimą pateikęs teismas pabrėžia, kad išsaugodama dinamiškus IP adresus Vokietijos administracija iš esmės siekia „užtikrinti ir išlaikyti savo telekomunikacinių paslaugų saugumą ir veikimą“; konkrečiai tariant, ji siekia „atpažinti ir apsiginti nuo dažnai pasitaikančių „denial of service“ atakų, kai telekomunikacijų infrastruktūra paralyžiuojama dėl tikslingo ir koordinuoto konkrečių tinklo serverių didelio užklausų srauto“ [26]. Dinamiškų IP adresų išsaugojimas šiuo tikslu yra svarbus bet kuriam interneto puslapių savininkui ir tam nereikalingas – nei tiesiogiai, nei netiesiogiai – viešosios valdžios įgaliojimų vykdymas, dėl to jo įtraukimas į Direktyvos 95/46 taikymo sritį nesukelia per didelių problemų.

85. *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) pažymi, kad pagrindinėje byloje dalyvaujančių paslaugų teikėjų vykdomas dinamiškų IP adresų išsaugojimas svarbus ir siekiant prireikus vykdyti galimų kibernetinių atakų vykdytojų baudžiamąjį persekiojimą. Ar šio tikslo pakanka tam, kad tokių duomenų tvarkymas nepatektų į Direktyvos 95/46 taikymo sritį?

86. Mano nuomone, jeigu „baudžiamąjį persekiojimą“ reikia suprasti kaip paslaugų teikėjų, kurie yra atsakovai pagrindinėje byloje, vykdomą valstybės *ius puniendi*, susiduriame su „valstybės veiksmais baudžiamosios teisės srityje“ ir su viena iš Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje numatytų išimčių.

87. Šiomis aplinkybėmis, atsižvelgiant į Teisingumo Teismo praktiką byloje *Huber* [27], paslaugų teikėjų vykdomas asmens duomenų tvarkymas, siekiant užtikrinti jų telekomunikacijų paslaugų saugumą ir techninį veikimą, patenka į Direktyvos 95/46 taikymo sritį, tačiau ši direktyva netaikoma duomenų tvarkymui, susijusiam su valstybės veiksmais baudžiamosios teisės srityje.

88. Lygiai taip pat, net jeigu baudžiamąjį persekiojimą Vokietijos Federacinė Respublika vykdytų ne kaip viešosios valdžios įgaliojimų neturintis paslaugų teikėjas, bet kaip privatus asmuo, kuris baudžiamojo persekiojimo tikslu tik pateiktų IP adresus, dėl kurių kilo ginčas, viešosios valdžios įstaigai, dinamiškų IP adresų tvarkymo tikslas taip pat būtų veikla, nepatenkanti į Direktyvos 95/46 taikymo sritį.

24 — 2003 m. lapkričio 6 d. sprendimo (C-101/01, EU:C:2003:596) 43 punktas.

25 — Taip pat žr. 2008 m. gruodžio 16 d. Sprendimo *Satakunnan Markkinapörssi ir Satamedia* (C-73/07, EU:C:2008:727) 41 punktą.

26 — Prašymo priimti prejudicinį sprendimą 36 punktas.

27 — 2008 m. gruodžio 16 d. sprendimo (C-524/06, EU:C:2008:724) 45 punktas.

89. Kaip matyti iš teismo praktikos byloje *Parlamentas / Taryba ir Komisija* [28], Teisingumo Teismas patvirtino, kad tai, jog konkretūs asmens duomenys „komerciniais tikslais buvo surinkti privačių subjektų, organizuojančių jų perdavimą į trečiąją šalį“, nereiškia, kad nagrinėjamas perdavimas nepatenka į Direktyvos 95/46 3 straipsnio 2 dalies pirmos įtraukos taikymo sritį, jeigu perdavimo tikslas yra valstybės veiksmai baudžiamosios teisės srityje, ir jis, kaip ir šiuo atveju, „vyksta pagal valstybės institucijų nustatytą tvarką, susijusią su visuomenės saugumu“ [29].

90. Tačiau jeigu, kaip manau, „baudžiamasis persekiojimas“ prašyme priimti prejudicinį sprendimą suprantamas kaip privataus asmens – teisės subjekto, turinčio teisę atitinkamai vykdyti valstybės *ius puniendi*, veiksmai, negalima tvirtinti, jog dinamiškų IP adresų tvarkymo tikslas yra valstybės veiksmai baudžiamosios teisės srityje, kurie nepatenka į Direktyvos 95/46 taikymo sritį.

91. Iš tikrųjų tokių duomenų išsaugojimas ir įrašymas laikytinas įrodymu, kuriuo remdamasis interneto puslapio savininkas gali prašyti valstybės pradėti baudžiamąjį persekiojimą dėl neteisėtų veiksmų. Galiausiai tai yra priemonė, kuri baudžiamosios teisės srityje naudojama konkrečiam subjektui teisės akte pripažintų teisių gynybai (šiuo atveju kalbama apie viešosios valdžios instituciją, veikiančią pagal privatinę teisę). Šiuo požiūriu toks elgesys nesiskiria nuo bet kurio kito interneto paslaugos teikėjo, kuris siekia valstybės apsaugos, laikydamasis teisės aktuose numatytos baudžiamojo persekiojimo procedūros, veiksmų.

92. Todėl tiek, kiek Vokietijos administracinė institucija veikia kaip viešosios valdžios įgaliojimų neturintis interneto paslaugų teikėjas, o tai turi įvertinti prašymą priimti prejudicinį sprendimą pateikęs teismas, jos atliekamas dinamiškų IP adresų tvarkymas kaip asmens duomenų patenka į Direktyvos 95/46 taikymo sritį.

2. Dėl esmės

93. Pagal TMG 15 straipsnio 1 dalį rinkti ir panaudoti naudotojo asmens duomenis galima tik tuo atveju, kai tai būtina siekiant suteikti jam galimybę naudotis telekomunikacijų paslaugomis ir atsiskaityti už jas. Konkrečiau kalbant, paslaugų teikėjas gali rinkti ir panaudoti „naudojimosi duomenis“, t. y. naudotojo asmeninius duomenis, tik tuo atveju, kai tai būtina siekiant suteikti jam galimybę „naudotis telekomunikacijų paslaugomis ir atsiskaityti už jas“. Šie duomenys turi būti ištrinami pasibaigus operacijai (t. y. kai baigiama naudotis telekomunikacijų paslauga), nebent jie turi būti saugomi „atsiskaitymo tikslais“, kaip numatyta TMG 15 straipsnio 4 dalyje.

94. Iš TMG 15 straipsnio matyti, kad atsijungus naudojimosi duomenys negali būti saugomi kitais tikslais; įskaitant ir tikslą apskritai „garantuoti telekomunikacijų paslaugų naudojimą“. Kadangi šioje TMG nuostatoje kaip duomenų išsaugojimą pateisinanti priežastis nurodomas atsiskaitymas, šią nuostatą galima suprasti taip (nors galutinį jos išaiškinimą turi pateikti prašymą priimti prejudicinį sprendimą pateikęs teismas), kad ja reikalaujama naudojimosi duomenis naudoti tik siekiant suteikti galimybę naudotis konkrečiu ryšiu, kuriam pasibaigus jie turėtų būti ištrinami.

28 — 2006 m. gegužės 30 d. sprendimo (C-317/04 ir C-318/04, EU:C:2006:346) 54–59 punktai.

29 — Ten pat, 59 punktas. Buvo kalbama apie asmens duomenis, kurių tvarkymas nebuvo būtinas paslaugoms, kurios yra susijusių privačių operatorių (vežėjų oro transportu) verslas, teikti, tačiau jie privalėjo juos pateikti JAV institucijoms dėl terorizmo prevencijos ir kovos su juo.

95. Mano nuomone, Direktyvos 95/46 7 straipsnio f punkto [30], kiek jis susijęs su leidimu tvarkyti asmens duomenis, formuluotė yra platesnė (duomenų tvarkytojo atžvilgiu) nei TMG 15 straipsnio formuluotė. Šiuo atveju Vokietijos teisės norma gali būti suprantama siauriau nei Sąjungos teisės norma, nes iš principo joje nenumatytas kito teisėto intereso, kuris nėra susijęs su atsiskaitymu už paslaugas, įgyvendinimas, nors Vokietijos Federacinė Respublika, kaip interneto paslaugų teikėja, galėtų turėti ir teisėtą interesą užtikrinti gerą savo interneto puslapių veikimą ne tik per kiekvieną atskirą prisijungimą [31].

96. Sprendime *ASNEF* ir *FECEMD* [32] Teisingumo Teismas nurodė kriterijus, kuriais remiantis reikėtų atsakyti į antrąjį prejudicinį klausimą. Taigi Teisingumo Teismas nusprendė, kad iš Direktyvos 95/46 tikslo „matyti, kad šios direktyvos 7 straipsnyje pateiktas atvejų, kai asmens duomenų tvarkymas gali būti laikomas teisėtu, sąrašas yra išsamus ir baigtinis“ [33]. Darytina išvada, kad „valstybės narės negali nei papildyti Direktyvos 95/46 7 straipsnyje nurodytų asmens duomenų tvarkymo teisėtumo principų naujais, nei numatyti papildomų reikalavimų, kuriais būtų pakeista kurio nors iš šiame straipsnyje numatytų šešių principų apimtis“ [34].

97. TMG 15 straipsnyje nėra daugiau teisėto asmens duomenų tvarkymo sąlygų, nei numatyta Direktyvos 95/46 7 straipsnyje – kaip buvo bylose *ASNEF* ir *FECEMD* - [35], tačiau jeigu ją aiškinsime taip siaurai, kaip siūlo teismas *a quo*, būtų susiaurintas minėto straipsnio f punkte įtvirtintos sąlygos turinys: ten, kur Sąjungos teisės aktų leidėjas bendrai nurodo patenkinimą „<...> teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis arba šalys, kurioms atskleidžiami duomenys“, TMG 15 straipsnyje daroma nuoroda tik į galimybę „[konkrečiai] naudotis telekomunikacijų paslaugomis ir atsiskaityti už jas“.

98. Kaip ir bylose *ASNEF* ir *FECEMD* [36], taip ir šiuo atveju nacionalinė priemonė, jeigu būtų aiškinama siaurai, kaip nurodyta pirma, pakeistų Direktyvos 95/469 7 straipsnyje įtvirtinto principo apimtį, o ne ją patikslintų, nors pagal Direktyvos 95/46 5 straipsnį valstybių narių valdžios institucijoms suteiktas tik pastarasis įgaliojimas.

99. Pagal minėtą nuostatą, „kiek leidžia šio skyriaus nuostatos [37], valstybės narės tiksliau apibrėžia sąlygas, kuriomis asmens duomenų tvarkymas yra teisėtas“. Kaip nuspręsta bylose *ASNEF* ir *FECEMD* [38], „valstybės narės neturi nei teisės nustatyti kitų, nei numatyti šios direktyvos 7 straipsnyje asmens duomenų tvarkymo teisėtumo principų, nei papildomais reikalavimais keisti šiame 7 straipsnyje numatytų šešių principų apimties“.

100. Palyginti su Direktyvos 95/46 7 straipsnio f punktu, TMG 15 straipsnis iš esmės susiaurintų teisėto intereso, galinčio pateisinti duomenų tvarkymą, apimtį, užuot ją tiksliau ir aiškiau reglamentavęs, paisant to, kas leidžiama pagal tos pačios direktyvos 5 straipsnį. Be to, tai būtų daroma kategoriškai ir absoliučiai, neatsižvelgiant į tai, kad bendro telekomunikacijų paslaugų naudojimo apsaugos ir užtikrinimo interesai gali būti vertinami atsižvelgiant į „duomenų subjekto, kuriam pagal 1 straipsnio 1 dalį reikalinga apsauga, teises ir laisves“, kaip to reikalaujama pagal šios direktyvos 7 straipsnio f punktą.

30 — Pateiktas šios išvados 17 punkte.

31 — Žr. 84 punktą. Žinoma, interneto puslapių savininkai turi teisėtą interesą užkirsti kelią ir kovoti su prašymą priimti prejudicinį sprendimą pateikusio teismo minėtais „denials of service“ trukdžiais, t. y. didelio masto atakomis, kurios kartais koncentruotai vykdomos prieš kai kuriuos interneto puslapius siekiant, kad jie būtų per daug apkrauti ir neveiktų.

32 — 2011 m. lapkričio 24 d. sprendimas (C-468/10 ir C-469/10, EU:C:2011:777).

33 — Ten pat, 30 punktas.

34 — Ten pat, 32 punktas.

35 — Šiuo atveju Direktyvos 95/46 7 straipsnio f punkte įtvirtinti reikalavimai nacionalinės teisės aktuose buvo papildyti reikalavimu, kad tvarkomi duomenys turi būti pateikti visuomenei prieinamuose šaltiniuose.

36 — 2011 m. lapkričio 24 d. sprendimas (C-468/10 ir C-469/10, EU:C:2011:777).

37 — Direktyvos 95/46 II skyrius „Bendrosios asmens duomenų tvarkymo teisėtumo taisyklės“, kuris apima 5–21 straipsnius.

38 — 2011 m. lapkričio 24 d. sprendimo (C-468/10 ir C-469/10, EU:C:2011:777) 36 punktas.

101. Galiausiai, kaip ir bylose *ASNEF* ir *FECEMD*[39], jeigu Vokietijos teisės aktų leidėjas „bet kuriuo atveju reikalauja teisių ir interesų, dėl kurių kilo ginčas, palyginimo su [konkrečiomis asmens duomenų kategorijomis] rezultato, kuris negali skirtis atsižvelgiant į konkrečiam atvejui būdingas specifines aplinkybes“, „tai nebėra tikslesnis apibrėžimas, kaip jis suprantamas pagal Direktyvos 95/46 5 straipsnį“.

102. Tokiomis aplinkybėmis manau, kad *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija) privalo nacionalinės teisės aktus aiškinti pagal Direktyvą 95/46, o tai reiškia, kad: a) „naudojimosi duomenų“ tvarkymą pateisinančios priežastys apima telekomunikacijų paslaugų teikėjo teisėtą interesą apsaugoti bendrą tokių paslaugų naudojimą; ir b) kad *ad casum* galima palyginti šį paslaugų teikėjo interesą su naudotojo interesu arba pagrindinėmis teisėmis ir laisvėmis, kad būtų išsiaiškinta, kuris saugotinas pagal Direktyvos 95/46 1 straipsnio 1 dalį[40].

103. Manau, kad nereikia nurodyti, kaip palyginti interesus šiuo atveju, dėl kurio pateiktas prašymas priimti prejudicinį sprendimą. Nieko apie tai neklausia ir *Bundesgerichtshof* (Aukščiausiasis federalinis teismas, Vokietija), kuriam svarbesnis klausimas, į kurį reikia atsakyti prieš pradedant tokį palyginimą; t. y. ar apskritai reikia atlikti tokį palyginimą.

104. Manau, kad nereikia nurodyti ir to, kad teismas *a quo* gali atsižvelgti į teisės nuostatas, kurias valstybės narės gali priimti pagal Direktyvos 95/46 13 straipsnio 1 dalies d punktą ir kuriomis gali būti ribojama 6 straipsnyje numatytų teisių ir laisvių apimtis, kai toks apribojimas reikalingas norint užtikrinti „kriminalinių nusikaltimų <...> prevenciją, tyrimą, išaiškinimą ir persekiojimą“. Prašymą priimti prejudicinį sprendimą pateikęs teismas neužsimena ir apie šį aspektą, nors jam tikrai žinoma, kad šie du straipsniai egzistuoja.

105. Todėl į antrąjį prejudicinį klausimą siūlau atsakyti, kad pagal Direktyvos 95/46 7 straipsnio f punktą draudžiama nacionalinės teisės normą aiškinti taip, jog paslaugų teikėjui draudžiama rinkti ir tvarkyti naudotojo asmens duomenis be jo sutikimo pasibaigus naudojimosi operacijai tam, kad būtų užtikrintas telekomunikacijų paslaugos veikimas.

VI – Išvada

106. Remdamasis tuo, kas išdėstyta, siūlau Teisingumo Teismui taip atsakyti į pateiktus prejudicinius klausimus:

1. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 2 straipsnio a punktas aiškintinas taip, kad dinamiškas IP adresas, kuriuo naudodamasis naudotojas pateko į telekomunikacijų paslaugų teikėjo interneto puslapį, šiam teikėjui yra „asmens duomenys“, jeigu prieigos prie tinklo teikėjas turi papildomos informacijos, kuri, suderinta su dinamišku IP adresu, leidžia nustatyti naudotoją.

2. Direktyvos 95/46 7 straipsnio f punktas turi būti aiškinamas taip, kad tikslas užtikrinti telekomunikacijų paslaugos veikimą iš principo gali būti laikomas teisėtu interesu, kurio patenkinimas pateisina asmens duomenų tvarkymą, jeigu atliekant palyginimą jis nusveria duomenų subjekto interesą ar pagrindines teises. Nacionalinės teisės nuostata, pagal kurią neleidžiama atsižvelgti į tokį teisėtą interesą, nesuderinama su minėtu straipsniu.

39 — Ten pat, 47 punktas.

40 — Per posėdį P. Breyer atstovas nesutiko, kad dinamiškų IP adresų registravimas būtinas siekiant apsaugoti gerą interneto paslaugų veikimą nuo galimų atakų. Nemanau, kad į šį klausimą galima atsakyti abstrakčiai; atvirkščiai, prieš pateikiant atsakymą kiekvienu konkrečiu atveju reikia palyginti interneto puslapio savininko interesą ir naudotojų teises bei interesus.