TEISINGUMO TEISMO (antroji kolegija) SPRENDIMAS

2016 m. spalio 19 d.*

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

Byloje C-582/14

dėl *Bundesgerichtshof* (Federalinis Aukščiausiasis Teismas, Vokietija) 2014 m. spalio 28 d. nutartimi, kurią Teisingumo Teismas gavo 2014 m. gruodžio 17 d., pagal SESV 267 straipsnį pateikto prašymo priimti prejudicinį sprendimą byloje

Patrick Breyer

prieš

Vokietijos Federacinę Respubliką

TEISINGUMO TEISMAS (antroji kolegija),

kurį sudaro kolegijos pirmininkas M. Ilešič, teisėjai A. Prechal, A. Rosas (pranešėjas), C. Toader ir E. Jarašiūnas,

generalinis advokatas M. Campos Sánchez-Bordona,

posėdžio sekretorė V. Giacobbo-Peyronnel, administratorė,

atsižvelgęs į rašytinę proceso dalį ir įvykus 2016 m. vasario 25 d. posėdžiui,

išnagrinėjęs pastabas, pateiktas:

— P. Breyer, atstovaujamo advokato M. Starostik,

— Vokietijos vyriausybės, atstovaujamos A. Lippstreu ir T. Henze,

— Austrijos vyriausybės, atstovaujamos G. Eberhard,

— Portugalijos vyriausybės, atstovaujamos L. Inez Fernandes ir C. Vieira Guerra,

— Europos Komisijos, atstovaujamos P. J. O. Van Nuffel, H. Krämer, P. Costa de Oliveira ir J. Vondung,

* Proceso kalba: vokiečių.

susipažinęs su 2016 m. gegužės 12 d. posėdyje pateikta generalinio advokato išvada,

priima šį

Sprendimą

1 Prašymas priimti prejudicinį sprendimą pateiktas dėl 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 (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k., 13 sk., 15 t., p. 355) 2 straipsnio a punkto ir 7 straipsnio f punkto išaiškinimo.

2 Šis prašymas pateiktas nagrinėjant Patrick Breyer ir Vokietijos Federacinės Respublikos ginčą dėl to, kad pastaroji įrašinėjo ir saugojo P. Breyer interneto protokolo adresą (toliau – IP adresas) šiam lankantis Vokietijos federalinių institucijų interneto puslapiuose.

Teisinis pagrindas

Sąjungos teisė

3 Direktyvos 95/46 26 konstatuojamoji dalis suformuluota taip:

„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“.

4 Šios direktyvos 1 straipsnyje nustatyta:

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

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

5 Tos pačios direktyvos 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;

<...>“

6 Direktyvos 95/46 3 straipsnyje „Taikymo sritis“ numatyta:

„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;

<...>“

7 Šios direktyvos 5 straipsnyje nustatyta:

„Kiek leidžia šio skyriaus nuostatos, valstybės narės tiksliau apibrėžia sąlygas, kuriomis asmens duomenų tvarkymas yra teisėtas.“

8 Tos pačios direktyvos 7 straipsnis suformuluotas taip:

„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;

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.“

9 Direktyvos 95/46 13 straipsnio 1 dalyje nurodyta:

„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:

<...>

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

<...>“

Vokietijos teisė

10 2007 m. vasario 26 d. Elektroninių paslaugų įstatymo (*Telemediengesetz*, *BGBl*. 2007 I, p. 179, toliau – TMG) 12 straipsnyje nustatyta:

„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.“

11 TMG 15 straipsnyje numatyta:

„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.

2. Paslaugų teikėjas gali sisteminti 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 užblokuoti duomenis. <...>“

12 Pagal 1990 m. gruodžio 20 d. Federalinio duomenų apsaugos įstatymo (*Bundesdatenschutzgesetz*, *BGBl.* 1990 I, p. 2954, toliau – BDSG) 3 straipsnio 1 dalį „asmens duomenys yra konkretūs duomenys apie fizinio asmens, kurio tapatybė nustatyta arba gali būti nustatyta (duomenų subjektas), asmeninius ar profesinius ryšius <...>“.

Pagrindinė byla ir prejudiciniai klausimai

13 P. Breyer lankėsi keliuose Vokietijos federalinių institucijų interneto portaluose. Šiuose viešai prieinamuose portaluose šios institucijos pateikia aktualią informaciją.

14 Siekiant išvengti atakų ir sudaryti galimybę vykdyti „piratų“ baudžiamąjį persekiojimą, daugumoje iš šių portalų visi apsilankymai išsaugomi rinkmenų sistemose. Pasibaigus apsilankymui, išsaugomi rinkmenos arba interneto puslapio pavadinimas, į paieškos laukelį įvesti žodžiai, apsilankymo laikas, perduotų duomenų kiekis, pranešimas, ar duomenys gauti sėkmingai, ir kompiuterio, iš kurio atliktas apsilankymas, IP adresas.

15 IP adresai yra skaitmenų sekos, priskiriamos prie tinklo prijungtiems kompiuteriams, kad būtų sudaryta galimybė jais keistis duomenimis internetu. Atsivertus interneto puslapį, kompiuterio, kuriuo naudojamasi, IP adresas perduodamas į serverį, kuriame išsaugotas prašomas puslapis. Tai būtina tam, kad duomenys būtų perduodami teisingam gavėjui.

16 Be to, iš nutarties pateikti prašymą priimti prejudicinį sprendimą ir iš Teisingumo Teismui pateiktos bylos medžiagos matyti, kad interneto prieigos teikėjai interneto naudotojams suteikia „statinį“ arba „dinaminį“, t. y. kintantį kaskart jungiantis prie interneto, IP adresą. Kitaip nei statiniai IP adresai, dinaminiai IP adresai neleidžia pasitelkti viešai prieinamų rinkmenų ir taip susieti konkretų kompiuterį su fizine prieiga prie tinklo, kurią naudoja interneto tiekėjas.

17 P. Breyer pateikė skundą Vokietijos administraciniams teismams, šiuo skundu siekė, kad Vokietijos Federacinei Respublikai būtų uždrausta saugoti arba leisti tretiesiems asmenims saugoti *host* sistemos, kuria naudojosi P. Breyer, IP adresus pasibaigus apsilankymui viešai prieinamuose Vokietijos federalinių institucijų elektroninių paslaugų portaluose, jei toks saugojimas nėra būtinas, siekiant sutrikimų atvejais atkurti galimybę vėl naudotis tokiomis elektroninėmis paslaugomis.

18 Po to, kai pirmosios instancijos teismas atmetė P. Breyer skundą, jis pateikė apeliacinį skundą dėl tokio sprendimo.

19 Apeliacinės instancijos teismas iš dalies pakeitė tą sprendimą. Jis įpareigojo Vokietijos Federacinę Respubliką nebesaugoti ar nebeleisti tretiesiems asmenims saugoti *host* sistemos, kuria naudojosi P. Breyer, IP adresų, perduotų lankantis viešai prieinamuose Vokietijos federalinių institucijų elektroninių paslaugų portaluose, pasibaigus tokiam apsilankymui, jei šis adresas saugomas kartu su apsilankymo data ir jei P. Breyer apsilankęs nurodė savo tapatybę, taip pat ir ją patvirtinančiu elektroniniu laišku, ir jei saugojimas nėra būtinas, siekiant sutrikimų atvejais atkurti galimybę vėl naudotis elektroninėmis paslaugomis.

20 Anot apeliacinio teismo, dinaminis IP adresas kartu su apsilankymo data tuo atveju, kai atitinkamame interneto puslapyje apsilankęs asmuo nurodė savo tapatybę, yra asmens duomenys, nes šio puslapio operatorius gali nustatyti šio naudotojo tapatybę, susiejęs jo pavardę su jo kompiuterio IP adresu.

21 Apeliacinis teismas manė, kad kitais atvejais vis dėlto nereikia patenkinti P. Breyer skundo. Iš tiesų tuo atveju, jei per prisijungimo operaciją P. Breyer nenurodo savo tapatybės, tik interneto prieigos teikėjas gali susieti IP adresą ir konkretų abonentą. Vokietijos Federacinės Respublikos, kaip elektroninių paslaugų teikėjos, atžvilgiu, priešingai, IP adresas nėra asmens duomenys net ir tada, kai jis pateikiamas kartu su prisijungimo data, nes ši valstybė narė negali nustatyti konkrečių interneto portalų naudotojo tapatybės.

22 P. Breyer ir Vokietijos Federacinė Respublika pateikė kasacinius skundus *Bundesgerichtshof* (Federalinis Aukščiausiasis Teismas, Vokietija) dėl apeliacinio teismo sprendimo. P. Breyer prašo visiškai patenkinti prašymą dėl uždraudimo. Vokietijos Federacinė Respublika prašo atmesti šį prašymą.

23 Prašymą priimti prejudicinį sprendimą pateikęs teismas patikslina, kad P. Breyer kompiuterio dinaminiai IP adresai, kuriuos saugo Vokietijos Federacinė Respublika, kaip elektroninių paslaugų teikėja, bent palyginti su kitais rinkmenų sistemose išsaugotais duomenimis, yra konkretūs duomenys apie profesinius ryšius, nes iš šių duomenų matyti, kad tam tikru laiku šis asmuo lankėsi tam tikruose interneto portaluose ir parsisiuntė tam tikrus duomenis.

24 Vis dėlto taip išsaugoti duomenys neleidžia iškart nustatyti P. Breyer tapatybės. Iš tiesų pagrindinėje byloje aptariamų interneto portalų operatoriai galėtų nustatyti P. Breyer tapatybę tik tuomet, jeigu jo interneto prieigos teikėjas suteiktų jiems informacijos apie šio naudotojo tapatybę. Taigi tai, ar šie duomenys laikytini „asmens duomenimis“, priklauso nuo to, ar buvo galima nustatyti P. Breyer tapatybę.

25 *Bundesgerichtshof* (Federalinis Aukščiausiasis Teismas) konstatuoja, kad doktrinoje yra prieštaringų nuomonių dėl to, kuriuo kriterijumi – „objektyviu“ ar „santykiniu“ – reikia remtis vertinant, ar galima nustatyti asmens tapatybę. Taikant „objektyvų“ kriterijų tokie duomenys, kaip pagrindinėje byloje nagrinėjami IP adresai, pasibaigus apsilankymui tam tikruose interneto portaluose galėtų būti laikomi asmens duomenimis, net jei atitinkamo asmens tapatybę gali nustatyti tik trečioji šalis; nagrinėjamu atveju tokia trečioji šalis yra P. Breyer interneto prieigos teikėjas, saugojęs papildomus duomenis, leidžiančius nustatyti šio asmens tapatybę pagal minėtus IP adresus. Pagal „santykinį“ kriterijų tokie duomenys galėtų būti laikomi asmens duomenimis tokios įstaigos, kaip antai P. Breyer interneto prieigos teikėjo, atžvilgiu, nes šie duomenys leidžia konkrečiai nustatyti naudotojo tapatybę (šiuo klausimu žr. 2011 m. lapkričio 24 d. Sprendimo *Scarlet Extended*, C-70/10, EU:C:2011:771, 51 punktą), tačiau nelaikomi asmens duomenimis kitos įstaigos, kaip antai interneto portalų, kuriuose lankėsi P. Breyer, operatoriaus atžvilgiu, nes, jei apsilankęs šiuose portaluose P. Breyer nenurodė savo tapatybės, šis operatorius neturėjo informacijos, būtinos tapatybei nustatyti be neproporcingai didelių pastangų.

26 Tuo atveju, jei P. Breyer kompiuterio dinaminiai IP adresai kartu su apsilankymo data turi būti laikomi asmens duomenimis, prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, ar IP adresų saugojimas pasibaigus apsilankymui leidžiamas pagal tos pačios direktyvos 7 straipsnio f punktą.

27 Šiuo klausimu *Bundesgerichtshof* (Federalinis Aukščiausiasis Teismas) patikslina, kad, pirma, pagal TMG 15 straipsnio 1 dalį elektroninių paslaugų teikėjai gali rinkti ir panaudoti naudotojo asmens duomenis tik tais atvejais, kai tai būtina siekiant suteikti galimybę naudotis šiomis paslaugomis ir atsiskaityti už jas. Antra, prašymą priimti prejudicinį sprendimą pateikęs teismas nurodo, kad, anot Vokietijos Federacinės Respublikos, šių duomenų saugojimas būtinas siekiant užtikrinti jos teikiamų viešai prieinamų elektroninių paslaugų portalų saugumą ir funkcionalumą, nes taip visų pirma

suteikiama galimybė atpažinti kibernetines atakas, vadinamas „atsisakymo aptarnauti atakomis“, kuriomis siekiama sustabdyti šių portalų veikimą tikslingai ir koordinuotai siunčiant didelį užklausų srautą į tam tikrus interneto serverius, taip pat kovoti su šiomis atakomis.

28 Anot prašymą priimti prejudicinį sprendimą pateikusio teismo, jei ir tiek, kiek būtina elektroninių paslaugų teikėjui imtis priemonių kovoti su tokiomis atakomis, šios priemonės gali būti laikomos būtinomis, siekiant „suteikti galimybę naudotis elektroninėmis paslaugomis“ pagal TMG 15 straipsnį. Vis dėlto doktrinoje daugiausia laikomasi požiūrio, kad, pirma, interneto portalo naudotojo asmens duomenų rinkimas ir panaudojimas galimas tik siekiant suteikti galimybę naudotis tuo konkrečiu portalu ir, antra, šie duomenys turi būti ištrinti pasibaigus atitinkamam apsilankymui, jei nėra būtini siekiant, kad naudotojas atsiskaitytų už paslaugą. Vis dėlto pagal tokį siaurą TMG 15 straipsnio 1 dalies supratimą būtų draudžiama saugoti IP adresus siekiant bendrai užtikrinti elektroninių paslaugų saugumą ir funkcionalumą.

29 Prašymą priimti prejudicinį sprendimą pateikęs teismas kelia klausimą, ar toks aiškinimas, kurį palaikė apeliacinis teismas, suderinamas su Direktyvos 95/46 7 straipsnio f punktu, atsižvelgiant į kriterijus, kuriuos Teisingumo Teismas suformulavo 2011 m. lapkričio 24 d. Sprendimo *ASNEF ir FECEMD* (C-468/10 ir C-469/10, EU:C:2011:777) 29 ir paskesniuose punktuose.

30 Tokiomis aplinkybėmis *Bundesgerichtshof* (Federalinis Aukščiausiasis Teismas) nutarė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar Direktyvos 95/46 2 straipsnio a punktą reikia aiškinti taip, kad IP adresas, kurį [elektroninės] 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?

2. Ar pagal [šios] direktyvos 7 straipsnio f punktą draudžiama nacionalinės teisės nuostata, pagal kurią [elektroninės] 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?

Dėl prejudicinių klausimų

Dėl pirmojo klausimo

31 Pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 95/46 2 straipsnio a punktą reikia aiškinti taip, kad dinaminis IP adresas, kurį elektroninių paslaugų teikėjas išsaugo asmeniui apsilankius viešai prieinamame šio teikėjo interneto puslapyje, šio paslaugų teikėjo atžvilgiu yra asmens duomenys, kaip jie suprantami pagal šią nuostatą, jei trečioji šalis (šiuo atveju to asmens interneto prieigos teikėjas) turi papildomos informacijos, būtinos šio asmens tapatybei nustatyti.

32 Pagal minėtą nuostatą „asmens duomenys“ reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta“. Pagal šią nuostatą 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.

33 Visų pirma pažymėtina, kad 2011 m. lapkričio 24 d. Sprendimo *Scarlet Extended* (C-70/10, EU:C:2011:771), susijusio būtent su tos pačios direktyvos išaiškinimu, 51 punkte Teisingumo Teismas iš esmės teigė, kad interneto vartotojų IP adresai yra saugomi asmens duomenys, nes leidžia tiksliai nustatyti tokius vartotojus.

34 Vis dėlto šis Teisingumo Teismo teiginys buvo susijęs su situacija, kai interneto vartotojų IP adresus renka ir identifikuoja interneto prieigos teikėjas.

35 Nagrinėjamu atveju pirmasis klausimas susijęs su situacija, kai interneto puslapio vartotojų IP adresus išsaugo elektroninių paslaugų teikėjas, padaręs tą puslapį viešai prieinamą, t. y. Vokietijos Federacinė Respublika, tačiau šis teikėjas neturi papildomos informacijos, būtinos šių vartotojų tapatybei nustatyti.

36 Be to, neginčijama, kad prašymą priimti prejudicinį sprendimą pateikusio teismo minimi IP adresai yra „dinaminiai“, t. y. laikini, suteikiami kiekvieną kartą prisijungus prie interneto ir keičiami per vėlesnius prisijungimus, o ne „statiniai“ IP adresai, kurie nekinta ir leidžia ilgam laikui identifikuoti prie tinklo prijungtą įrenginį.

37 Pirmasis prašymą priimti prejudicinį sprendimą pateikusio teismo pateiktas klausimas grindžiamas prielaida, kad, pirma, duomenys, kuriuos sudaro dinaminis IP adresas ir prisijungimo prie interneto puslapio iš šio IP adreso data ir laikas, o įrašo elektroninių paslaugų teikėjas, patys savaime nesuteikia šiam paslaugų teikėjui galimybės nustatyti naudotojo, kuris lankėsi tame interneto puslapyje per tą prisijungimo operaciją, ir, antra, interneto prieigos teikėjas turi papildomos informacijos, kuri, susieta su IP adresu, leistų nustatyti tokio naudotojo tapatybę.

38 Šiuo klausimu pirmiausia pažymėtina, jog neginčijama, kad dinaminis IP adresas nėra su fiziniu „asmeniu, kurio tapatybė nustatyta“, susijusi informacija, nes toks adresas tiesiogiai neatskleidžia fizinio asmens, kompiuterio, iš kurio lankytasi interneto puslapyje, savininko, ar kito asmens, kuris galėtų pasinaudoti tuo kompiuteriu, tapatybės.

39 Siekiant nustatyti, ar šio sprendimo 37 punkte nurodytu atveju dinaminis IP adresas elektroninių paslaugų teikėjo atžvilgiu yra asmens duomenys, kaip jie suprantami pagal Direktyvos 96/45 2 straipsnio a punktą, reikia patikrinti, ar toks IP adresas, kurį išsaugo toks paslaugų teikėjas, gali būti laikomas informacija, susijusia su „asmeniu, kurio tapatybė yra nustatyta“, jei papildomos informacijos, būtinos interneto puslapio, kurį viešai prieinamą padarė šis paslaugų teikėjas, naudotojo tapatybei nustatyti, turi šio naudotojo interneto prieigos teikėjas.

40 Šiuo klausimu pasakytina, jog iš Direktyvos 95/46 2 straipsnio a punkto teksto matyti, kad asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta ne tik tiesiogiai, bet ir netiesiogiai.

41 Sąjungos teisės aktų leidėjo vartojamas žodis „netiesiogiai“ rodo, jog tam, kad informacija būtų laikoma asmens duomenimis, nebūtina, kad ji pati savaime leistų nustatyti atitinkamo asmens tapatybę.

42 Be to, Direktyvos 95/46 26 konstatuojamojoje dalyje nurodyta, kad norint įvertinti, 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.

43 Kadangi šioje konstatuojamojoje dalyje nurodytos priemonės, kuriomis gali pasinaudoti duomenų valdytojas ar „kitas asmuo“, remiantis jos tekstu galima manyti, jog tam, kad duomenys būtų laikomi „asmens duomenimis“, kaip jie suprantami pagal minėtos direktyvos 2 straipsnio a punktą, nereikalaujama, kad visą informaciją, leidžiančią nustatyti atitinkamo asmens tapatybę, turėtų vienas asmuo.

44 Taigi dėl aplinkybės, kad papildomos informacijos, būtinos interneto puslapio naudotojo tapatybei nustatyti, turi ne elektroninių paslaugų teikėjas, o šio naudotojo interneto prieigos teikėjas, negalima atmesti galimybės, kad elektroninių paslaugų teikėjo išsaugoti dinaminiai IP adresai jo atžvilgiu yra asmens duomenys, kaip jie suprantami pagal Direktyvos 95/46 2 straipsnio a punktą.

45 Vis dėlto reikia nustatyti, ar galimybė susieti dinaminį IP adresą su tokia interneto prieigos teikėjo turima papildoma informacija yra priemonė, kuria galima pasinaudoti atitinkamo asmens tapatybei nustatyti.

46 Kaip savo išvados 68 punkte iš esmės nurodė generalinis advokatas, taip nebūtų tuo atveju, jeigu nustatyti atitinkamo asmens tapatybę būtų draudžiama pagal įstatymą arba praktiškai neįmanoma, nes, pavyzdžiui, reikalautų neproporcingai daug laiko ir žmogiškųjų bei ekonominių išteklių, ir dėl to tapatybės nustatymas faktiškai būtų nereikšmingas.

47 Nors prašymą priimti prejudicinį sprendimą pateikęs teismas savo nutartyje nurodo, kad pagal Vokietijos teisę interneto prieigos teikėjui neleidžiama tiesiogiai elektroninių paslaugų teikėjui perduoti papildomos informacijos, būtinos atitinkamo asmens tapatybei nustatyti, vis dėlto tikriausiai yra teisėtų būdų, kaip elektroninių paslaugų teikėjas visų pirma kibernetinių atakų atvejais gali kreiptis į kompetentingą instituciją, kad ši imtųsi veiksmų, reikalingų šiai informacijai gauti iš interneto prieigos teikėjo ir pradėti baudžiamąjį persekiojimą, bet tai turi patikrinti prašymą priimti prejudicinį sprendimą pateikęs teismas.

48 Taigi elektroninių paslaugų teikėjas gali pasinaudoti tam tikromis priemonėmis, kad padedamas kitų subjektų, t. y. kompetentingos institucijos ir interneto prieigos teikėjo, nustatytų atitinkamo asmens tapatybę pagal išsaugotus IP adresus.

49 Atsižvelgiant į tai, kas išdėstyta, į pirmąjį klausimą reikia atsakyti, kad Direktyvos 95/46 2 straipsnio a punktas aiškintinas taip, jog dinaminis IP adresas, kurį elektroninių paslaugų teikėjas išsaugo asmeniui apsilankius viešai prieinamame šio teikėjo interneto puslapyje, šio paslaugų teikėjo atžvilgiu yra asmens duomenys, kaip jie suprantami pagal šią nuostatą, jeigu jis turi teisėtų priemonių atitinkamo asmens tapatybei nustatyti, remdamasis papildoma informacija, kurios turi šio asmens interneto prieigos teikėjas.

Dėl antrojo klausimo

50 Antruoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia sužinoti, ar Direktyvos 95/46 7 straipsnio f punktas turi būti aiškinamas taip, kad pagal jį draudžiamos valstybės narės teisės nuostatos, pagal kurias elektroninių paslaugų teikėjas gali rinkti ir panaudoti šių paslaugų naudotojo asmens duomenis be jo sutikimo tik tiek, kiek toks rinkimas ir panaudojimas būtinas siekiant leisti tam naudotojui pasinaudoti konkrečia paslauga ir atsiskaityti už ją, ir pagal kurias tikslas užtikrinti bendrą tokių paslaugų veikimą negali pateisinti duomenų naudojimo pasibaigus konkrečiai naudojimosi paslaugomis operacijai.

51 Siekiant atsakyti į šį klausimą, reikia nustatyti, ar pagrindinėje byloje nagrinėjamų asmens duomenų, t. y. tam tikrų Vokietijos federalinių tarnybų interneto portalų naudotojų dinaminių IP adresų, tvarkymas patenka, ar nepatenka į Direktyvos 95/46 taikymo sritį, remiantis jos 3 straipsnio 2 dalies pirma įtrauka, pagal kurią ši direktyva netaikoma tvarkant asmens duomenis, kai tvarkymo operacija susijusi su valstybės veiksmais baudžiamosios teisės srityje.

52 Šiuo klausimu primintina, kad šioje nuostatoje kaip pavyzdžiai nurodytos veiklos rūšys visais atvejais priskirtinos valstybės ar valstybės institucijų, o ne privačių subjektų veiklos sritims (žr. 2003 m. lapkričio 6 d. Sprendimo *Lindqvist*, C-101/01, EU:C:2003:596, 43 punktą ir 2008 m. gruodžio 16 d. Sprendimo *Satakunnan Markkinapörssi ir Satamedia*, C-73/07, EU:C:2008:727, 41 punktą).

53 Vis dėlto pagrindinėje byloje Vokietijos federalinės tarnybos, teikiančios elektronines paslaugas ir tvarkančios dinaminius IP adresus, nepaisant to, kad yra valdžios institucijos, veikia kaip privatūs asmenys ir jų veikla nesusijusi su valstybės veiksmais baudžiamosios teisės srityje, bet tai turi patikrinti prašymą priimti prejudicinį sprendimą pateikęs teismas.

54 Taigi reikia nustatyti, ar tokios valstybės narės teisės nuostatos, kaip nagrinėjamos pagrindinėje byloje, suderinamos su Direktyvos 95/46 7 straipsnio f punktu.

55 Šiuo tikslu primintina, kad pagal pagrindinėje byloje nagrinėjamas nacionalinės teisės nuostatas, kaip jas siaurai išaiškino prašymą priimti prejudicinį sprendimą pateikęs teismas, rinkti ir panaudoti tokių paslaugų naudotojo asmens duomenis be jo sutikimo galima tik tiek, kiek tai būtina siekiant leisti tam naudotojui pasinaudoti konkrečia elektronine paslauga ir atsiskaityti už ją, o tikslas užtikrinti bendrą tokių paslaugų veikimą negali pateisinti duomenų naudojimo pasibaigus konkrečiai naudojimosi šia paslauga operacijai.

56 Pagal Direktyvos 95/46 7 straipsnio f punktą asmens duomenų tvarkymas yra teisėtas, „jei tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto, kuriam pagal [šios direktyvos] 1 straipsnio 1 dalį reikalinga apsauga, teisės ir laisvės yra viršesnės nei šie interesai“.

57 Primintina, jog Teisingumo Teismas yra nusprendęs, kad šios direktyvos 7 straipsnyje pateiktas atvejų, kai asmens duomenų tvarkymas gali būti laikomas teisėtu, sąrašas yra išsamus ir baigtinis, ir kad valstybės narės negali papildyti tame straipsnyje nurodytų asmens duomenų tvarkymo teisėtumo principų naujais ar numatyti papildomų reikalavimų, kuriais būtų pakeista kurio nors iš šiame straipsnyje numatytų šešių principų apimtis (šiuo klausimu žr. 2011 m. lapkričio 24 d. Sprendimo *ASNEF ir FECEMD*, C-468/10 ir C-469/10, EU:C:2011:777, 30 ir 32 punktus).

58 Nors pagal Direktyvos 95/46 5 straipsnį, kiek leidžia II skyriaus, taigi ir jame esančio 7 straipsnio, nuostatos, valstybėms narėms suteikiama galimybė tiksliau apibrėžti sąlygas, kurioms esant asmens duomenų tvarkymas yra teisėtas, pagal šį 5 straipsnį valstybėms narėms suteikta diskrecija reikia naudotis tik paisant šia direktyva siekiamo tikslo išsaugoti laisvo asmens duomenų judėjimo ir privataus gyvenimo apsaugos pusiausvyrą. Pagal tos pačios direktyvos 5 straipsnį valstybės narės negali nei nustatyti kitų asmens duomenų tvarkymo teisėtumo principų, nei numatyti šios direktyvos 7 straipsnyje ar papildomais reikalavimais keisti šiame 7 straipsnyje numatytų šešių principų apimties (šiuo klausimu žr. 2011 m. lapkričio 24 d. Sprendimo *ASNEF ir FECEMD*, C-468/10 ir C-469/10, EU:C:2011:777, 33, 34 ir 36 punktus).

59 Nagrinėjamu atveju TMG 15 straipsnio, aiškinamo siaurai, kaip nurodyta šio sprendimo 55 punkte, apimtis būtų siauresnė, negu Direktyvos 95/46 7 straipsnio f punkte numatyto principo apimtis.

60 Minėtos direktyvos 7 straipsnio f punkte bendrai nurodyti „teisėti interesai, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys“, o pagal TMG 15 straipsnį paslaugų teikėjui leidžiama rinkti ir panaudoti naudotojo asmens duomenis tik tiek, kiek tai būtina siekiant suteikti galimybę pasinaudoti konkrečia elektronine paslauga ir už ją atsiskaityti. Taigi pagal TMG 15 straipsnį bendrai draudžiama pasibaigus naudojimosi elektroninėmis paslaugomis operacijai saugoti asmens duomenis, siekiant užtikrinti galimybę naudotis tokiomis paslaugomis. Vis dėlto Vokietijos federalinės tarnybos, teikiančios elektronines paslaugas, taip pat gali turėti teisėtų interesų užtikrinti, kad pasibaigus konkrečiai prisijungimo prie jų viešai prieinamų interneto portalų operacijai šie portalai ir toliau veiks.

61 Kaip savo išvados 100 ir 101 punktuose pažymėjo generalinis advokatas, tokiomis nacionalinės teisės nuostatomis ne tik patikslinama, kaip nurodyta Direktyvos 95/46 5 straipsnyje, jos 7 straipsnio f punkte esanti sąvoka „teisėti interesai“.

62 Šiuo klausimu taip pat primintina, kad pagal minėtos direktyvos 7 straipsnio f punktą valstybei narei draudžiama kategoriškai ir visais atvejais panaikinti galimybę tvarkyti tam tikrų rūšių asmens duomenis, neleidžiant palyginti konkrečios situacijos priešingų teisių ir interesų. Taigi, kiek tai susiję su šių rūšių duomenimis, valstybė narė negali numatyti galutinio priešingų teisių ir interesų palyginimo rezultato ir neleisti konkrečiu atveju, kuriam būdingos specifinės aplinkybės, pasiekti kitokio rezultato (šiuo klausimu žr. 2011 m. lapkričio 24 d. Sprendimo *ASNEF ir FECEMD*, C-468/10 ir C-469/10, EU:C:2011:777, 47 ir 48 punktus).

63 Tokios nacionalinės teisės nuostatos, kaip nagrinėjamos pagrindinėje byloje, kiek tai susiję su elektroninių paslaugų naudotojų asmens duomenų tvarkymu, susiaurina Direktyvos 95/46 7 straipsnio f punkte numatyto principo apimtį, nes pagal jas atmetama galimybė, kad tikslas užtikrinti bendrą tokių elektroninių paslaugų veikimą gali būti palygintas su šių naudotojų interesais arba pagrindinėmis teisėmis ir laisvėmis, kurioms, kaip nurodyta šioje nuostatoje, reikalinga apsauga pagal šios direktyvos 1 straipsnio 1 dalį.

64 Atsižvelgiant į visa tai, kas išdėstyta, į antrąjį klausimą reikia atsakyti, kad Direktyvos 95/46 7 straipsnio f punktas turi būti aiškinamas taip, jog pagal jį draudžiamos valstybės narės teisės nuostatos, pagal kurias elektroninių paslaugų teikėjas gali rinkti ir panaudoti šių paslaugų naudotojo asmens duomenis be šio sutikimo tik tiek, kiek toks rinkimas ir panaudojimas būtinas siekiant leisti tam naudotojui pasinaudoti konkrečia paslauga ir atsiskaityti už ją, ir pagal kurias tikslas užtikrinti bendrą tokių paslaugų veikimą negali pateisinti duomenų naudojimo pasibaigus konkrečiai naudojimosi paslaugomis operacijai.

Dėl bylinėjimosi išlaidų

65 Kadangi šis procesas pagrindinės bylos šalims yra vienas iš etapų prašymą priimti prejudicinį sprendimą pateikusio teismo nagrinėjamoje byloje, bylinėjimosi išlaidų klausimą turi spręsti šis teismas. Išlaidos, susijusios su pastabų pateikimu Teisingumo Teismui, išskyrus tas, kurias patyrė minėtos šalys, nėra atlygintinos.

Remdamasis šiais motyvais, Teisingumo Teismas (antroji kolegija) nusprendžia:

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 turi būti aiškinamas taip, kad dinaminis interneto protokolo adresas, kurį elektroninių paslaugų teikėjas išsaugo asmeniui apsilankius viešai prieinamame šio teikėjo interneto puslapyje, šio paslaugų teikėjo atžvilgiu yra asmens duomenys, kaip jie suprantami pagal šią nuostatą, jeigu jis turi teisėtų priemonių atitinkamo asmens tapatybei nustatyti, remdamasis papildoma informacija, kurios turi šio asmens interneto prieigos teikėjas.**

2. **Direktyvos 95/46 7 straipsnio f punktas turi būti aiškinamas taip, kad pagal jį draudžiamos valstybės narės teisės nuostatos, pagal kurias elektroninių paslaugų teikėjas gali rinkti ir panaudoti šių paslaugų naudotojo asmens duomenis be jo sutikimo tik tiek, kiek toks rinkimas ir panaudojimas būtinas siekiant leisti tam naudotojui pasinaudoti konkrečia paslauga ir atsiskaityti už ją, ir pagal kurias tikslas užtikrinti bendrą tokių paslaugų veikimą negali pateisinti duomenų naudojimo pasibaigus konkrečiai naudojimosi paslaugomis operacijai.**

Parašai.