Judikatūras krājums

ĢENERĀLADVOKĀTA M. KAMPOSA SANČESA-BORDONAS [*M. CAMPOS SÁNCHEZ-BORDONA*]
SECINĀJUMI,
sniegti 2016. gada 12. maijā [1]

Lieta C-582/14

Patrick Breyer
pret
Bundesrepublik Deutschland

(Bundesgerichtshof (Federālā Augstākā tiesa, Vācija) lūgums sniegt prejudiciālu nolēmumu)

Personas datu apstrāde — Direktīva 95/46/EK — 2. panta a) punkts un 7. panta f) punkts — Jēdziens "personas dati" — IP adreses — Saglabāšana, ko veic elektronisko sakaru pakalpojumu sniedzējs — Valsts tiesiskais regulējums, kas liedz ņemt vērā datu apstrādātāja likumīgās intereses

1. Interneta protokola adrese (turpmāk tekstā – "IP adrese") ir ierīcei (dators, planšetdators, viedtālrunis) piešķirta binārā sistēmā pierakstītu ciparu secība, kas ļauj to identificēt un ļauj tai piekļūt elektronisko sakaru tīklam. Lai pieslēgtos internetam, ierīcei ir jāizmanto ciparu secība, ko piešķīruši interneta piekļuves pakalpojumu sniedzēji. IP adrese tiek nosūtīta serverim, kurā atrodas meklētā tīmekļa vietne.

2. Konkrēti, interneta piekļuves pakalpojumu sniedzēji (galvenokārt telekomunikāciju uzņēmumi) brīdī, kad notiek pieslēgšanās internetam, piešķir saviem klientiem tā sauktās "dinamiskās IP adreses", kas ir izmantojamas ierobežotā laikā un mainās, nākamreiz pieslēdzoties tīklam. Šiem uzņēmumiem ir reģistrs, kurā tiek konstatēts, kāda IP adrese katrreiz tikusi piešķirta konkrētajai ierīcei [2].

3. To tīmekļa vietņu īpašnieki, kurām piekļuve notiek ar dinamisko IP adrešu palīdzību, arī mēdz saglabāt ierakstus, kuros tiek konstatēts, kādas vietnes tikušas apmeklētas, kad tas noticis un no kādas dinamiskās IP adreses. Tehniski šie ieraksti var tikt saglabāti bez laika ierobežojumiem pēc katra lietotāja atvienošanās no interneta.

4. Lai pakalpojumu sniedzējs varētu identificēt tīmekļa vietnes lietotāju, ar dinamisko IP adresi vien nepietiek. Tomēr viņam tas ir iespējams, ja viņš izmanto dinamisko IP adresi kopā ar citu papildinformāciju, kas ir interneta piekļuves pakalpojumu sniedzēja rīcībā.

1 — Oriģinālvaloda – spāņu.

2 — Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīvas 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK (OV 2006, L 105, 54. lpp.) 5. pantā kā viens no pienākumiem smagu noziegumu izmeklēšanas, atklāšanas un sodīšanas nolūkā tika noteikts tas, ka jāsaglabā "interneta piekļuves pakalpojuma pieteikuma un atteikuma datums un laiks, [..] kopā ar IP dinamisko vai statisko adresi, kuru komunikācijai piešķīris interneta piekļuves pakalpojumu sniedzējs, un reģistrētā lietotāja vai abonenta lietotāja identifikators".

5. Lietā ir strīds par to, vai dinamiskās IP adreses ir personas dati Direktīvas 95/46/EK 2. panta a) punkta izpratnē[3]. Lai atbildētu uz jautājumu, sākumā ir jānosaka, kāda nozīme šajā ziņā ir tam, ka lietotāja identificēšanai nepieciešamā papildinformācija nav tīmekļa vietnes īpašnieka, bet trešās personas (konkrētāk, interneta piekļuves pakalpojumu sniedzēja) rīcībā.

6. Šo jautājumu Tiesa vēl nav skatījusi, jo sprieduma *Scarlet Extended*[4] 51. punktā tā ir lēmusi, ka IP adreses "ir aizsargātie personas dati, kuri ļauj precīzi identificēt minētos lietotājus", bet tādā kontekstā, kurā IP adrešu iegūšanu un identificēšanu ir veicis interneta piekļuves pakalpojumu sniedzējs[5], nevis satura nodrošinātājs, kā tas ir šajā gadījumā.

7. Ja būtu jāuzskata, ka dinamiskās IP adreses interneta pakalpojumu sniedzējam ir personas dati, vēlāk būtu jāpārbauda, vai to apstrāde ietilpst Direktīvas 95/46 piemērošanas jomā.

8. Ir iespējams, ka, pat ja tie būtu uzskatāmi par personas datiem, tiem nebūtu piemērojama Direktīvā 95/46 paredzētā aizsardzība, ja, piemēram, tie tiktu apstrādāti, lai veiktu krimināltiesisku vajāšanu pret iespējamiem uzbrucējiem tīmekļa vietnei. Šajā gadījumā Direktīva 95/46 saskaņā ar tās 3. panta 2. punkta pirmo ievilkumu nav piemērojama.

9. Turklāt ir jānoskaidro, vai pakalpojumu sniedzējs, kas ieraksta dinamiskās IP adreses laika brīdi, kad tā tīmekļa vietnēm piekļūst lietotājs (šajā lietā Vācijas Federatīvā Republika), rīkojas kā valsts iestāde vai kā privātpersona.

10. Visbeidzot, ja būtu piemērojama Direktīva 95/46, būtu jāprecizē, vai ar tās 7. panta f) punktu ir saderīgs valsts tiesiskais regulējums, kas ierobežo viena no tajā paredzētajiem nosacījumiem attiecībā uz personas datu apstrādi apjomu.

I – Atbilstošās tiesību normas

A – *Savienības tiesības*

11. Direktīvas 95/46 preambulas 26. apsvērums ir formulēts šādi:

"(26) tā kā aizsardzības principus jāpiemēro jebkurai informācijai par identificētu vai identificējamu personu; tā kā, lai noteiktu, vai persona ir identificējama, būtu jāņem vērā visi līdzekļi, kurus, iespējams, pamatoti izmantotu vai nu personas datu apstrādātājs, vai jebkura cita persona, lai identificētu minēto personu; tā kā aizsardzības principus nepiemēro anonīmi iesniegtiem datiem, ja datu subjekts vairs nav identificējams; tā kā 27. pantā paredzētie profesionālās ētikas kodeksi var būt noderīgs līdzeklis norādījumu sniegšanā par veidiem, kādos datus var iesniegt anonīmi un saglabāt tos veidā, kurā datu subjekta identifikācija vairs nav iespējama."

12. Saskaņā ar Direktīvas 95/46/EK 1. pantu:

"1. Saskaņā ar šo direktīvu dalībvalstis aizsargā fizisku personu pamattiesības un brīvības un jo īpaši viņu tiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi.

2. Dalībvalstis neierobežo un neaizliedz personas datu brīvu plūsmu starp dalībvalstīm, pamatojoties uz 1. punktā paredzēto aizsardzību."

3 — Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.).

4 — 2011. gada 24. novembra spriedums (C-70/10, EU:C:2011:771), 51. punkts.

5 — Tas ir attiecināms arī uz 2012. gada 19. aprīļa spriedumu *Bonnier Audio* u.c. (C-461/10, EU:C:2012:219), 51. un 52. punkts.

13. Saskaņā ar Direktīvas 95/46 2. pantu:

"Šajā direktīvā:

a) "personas dati" ir jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu ("datu subjektu"); identificējama persona ir tā, kuru var identificēt tieši vai netieši, norādot reģistrācijas numuru vai vienu vai vairākus šai personai raksturīgus fiziskās, fizioloģiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktorus;

b) "personu datu apstrāde" ("apstrāde") ir jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem – kā vākšana, reģistrēšana, organizēšana, uzglabāšana, piemērošana vai pārveidošana, labošana, konsultēšana, izmantošana, atklāšana, pielietojot pārsūtīšanu, izplatīšanu vai darot tos pieejamus citādā veidā, grupēšana vai savienošana, piekļuves noslēgšana, dzēšana vai iznīcināšana;

[..]

d) "personas datu apstrādātājs" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita institūcija, kura viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja apstrādes nolūkus un līdzekļus nosaka valsts vai Kopienas tiesību akti vai noteikumi, personas datu apstrādātāju vai viņa iecelšanas konkrētos kritērijus var noteikt valsts vai Kopienas tiesību akti;

[..]

f) "trešās personas" ir jebkura fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita struktūra, kura nav datu subjekts, personas datu apstrādātājs, apstrādātājs un personas, kuras ir pilnvarotas apstrādāt datus personas datu apstrādātāja vai apstrādātāja tiešā vadībā;

[..]."

14. Direktīvas 95/46 3. pantā "Darbības joma" ir noteikts:

"1. Šī direktīva attiecas uz personas datu apstrādi pilnībā vai daļēji ar automatizētiem līdzekļiem un uz personas datu, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, apstrādi, kura netiek veikta ar automatizētiem līdzekļiem.

2. Šī direktīva neattiecas uz personas datu apstrādi:

— tādu pasākumu gaitā, uz kuru neattiecas Kopienas tiesību akti, kā Līguma par Eiropas Savienību V un VI sadaļā paredzētie pasākumi un, jebkurā gadījumā, uz apstrādes operācijām attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību (ieskaitot valsts ekonomisko labklājību, ja apstrādes operācija attiecas uz valsts drošības jautājumiem) un uz valsts pasākumiem krimināltiesību jomā;

[..]."

15. Direktīvas 95/46 II nodaļa "Vispārīgi noteikumi par personas datu apstrādes likumību" sākas ar 5. pantu, atbilstoši kuram "dalībvalstis saskaņā ar šīs nodaļas noteikumiem precīzāk nosaka apstākļus, kādos personas datu apstrāde ir likumīga".

16. Saskaņā ar Direktīvas 95/46 6. pantu:

"1. Dalībvalstis nosaka to, ka personas datiem jābūt:

a) apstrādātiem godīgi un likumīgi;

b) vāktiem konkrētiem, precīzi formulētiem un likumīgiem nolūkiem, un tos nedrīkst tālāk apstrādāt ar šiem nolūkiem nesavienojamā veidā. Turpmāka datu apstrāde vēsturiskiem, statistiskiem vai zinātniskiem nolūkiem nav uzskatāma par nesavienojamu, ar noteikumu, ka dalībvalstis sniedz atbilstošas garantijas;

c) adekvātiem, attiecīgiem un ne pārmērīgā apjomā attiecībā uz nolūkiem, kādiem tie savākti un/vai tālāk apstrādāti;

d) precīziem un nepieciešamības gadījumā atjauninātiem; jāveic visi reālie pasākumi, lai nodrošinātu, ka neprecīzus vai nepilnīgus datus, ņemot vērā to vākšanas vai turpmākās apstrādes nolūkus, dzēš vai izlabo;

e) saglabātiem veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk, kā tas nepieciešams nolūkiem, kuriem datus vāca vai kuriem tos turpmāk apstrādā. Dalībvalstis nosaka atbilstošas garantijas personas datiem, kurus uzglabā ilgāku laiku, lai izmantotu vēsturiskiem, statistiskiem vai zinātniskiem nolūkiem.

2. Personas datu apstrādātājam jānodrošina 1. punkta izpilde."

17. Saskaņā ar Direktīvas 95/46 7. pantu:

"Dalībvalstis paredz to, ka personas datus var apstrādāt tikai, ja:

a) datu subjekts nepārprotami devis savu piekrišanu;

b) vai apstrāde vajadzīga līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;

c) vai apstrāde vajadzīga, lai izpildītu uz personas datu apstrādātāju attiecināmas juridiskas saistības; vai

d) apstrāde vajadzīga, lai aizsargātu datu subjekta būtiskas intereses;

e) vai apstrāde vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai personas datu apstrādātājam vai trešajai personai, kurai dati tiek atklāti, piešķirto oficiālo pilnvaru realizācijai;

f) vai apstrāde vajadzīga personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgo interešu ievērošanai, izņemot, ja šīs intereses ignorē, ņemot vērā datu subjekta pamattiesību un brīvību intereses, kurām nepieciešama aizsardzība saskaņā ar 1. panta 1. punktu."

18. Saskaņā ar Direktīvas 95/46 13. pantu:

"1. Dalībvalstis var pieņemt tiesību aktus, lai ierobežotu 6. panta 1. punktā, 10. pantā, 11. panta 1. punktā, 12. pantā un 21. pantā paredzēto pienākumu un tiesību jomu, ja šāds ierobežojums ir nepieciešams aizsargpasākums:

a) valsts drošībai;

b) aizsardzībai;

c) sabiedrības drošībai;

d) kriminālsodāmu noziedzīgu nodarījumu vai reglamentētu profesiju ētikas pārkāpumu profilaksei, izziņai, atklāšanai un kriminālvajāšanai;

e) dalībvalsts vai Eiropas Savienības svarīgās ekonomiskās vai finansiālās interesēs, ieskaitot monetāros, budžeta un nodokļu jautājumus;

f) ar oficiālo pilnvaru realizāciju c), d) un e) apakšpunktā minētajos gadījumos pat laiku pa laikam saistītajai uzraudzībai, pārbaudei un reglamentējošām funkcijām;

g) datu subjekta aizsardzībai vai citu personu tiesību un brīvību aizsardzībai.

[..]"

B – *Valsts tiesības*

19. *Telemediengesetz* (Telekomunikāciju līdzekļu likums, turpmāk tekstā – "*TMG*")[6] 12. pantā ir noteikts:

"1. Telekomunikāciju līdzekļu pieejamības nodrošināšanas nolūkā pakalpojumu sniedzējs drīkst iegūt un izmantot personas datus tikai tiktāl, ciktāl to atļauj šis likums vai cita tiesību norma, kas tieši attiecas uz telekomunikāciju līdzekļiem, vai ja lietotājs ir devis savu piekrišanu.

2. Telekomunikāciju līdzekļu pieejamības nodrošināšanas nolūkā iegūtos personas datus pakalpojumu sniedzējs drīkst izmantot citiem nolūkiem tikai tiktāl, ciktāl to atļauj šis likums vai cita tiesību norma, kas tieši attiecas uz telekomunikāciju līdzekļiem, vai ja lietotājs ir devis savu piekrišanu.

3. Ciktāl nav noteikts citādi, attiecīgi spēkā esošās tiesību normas attiecībā uz personas datu aizsardzību ir piemērojamas arī tad, ja dati netiek apstrādāti automatizētā veidā."

20. Saskaņā ar *TMG* 15. pantu:

"1. Lietotāja personas datus pakalpojumu sniedzējs drīkst iegūt un izmantot tikai tad, ja tas ir nepieciešams, lai padarītu par iespējamu telekomunikāciju līdzekļu lietošanu un norēķinus par to (lietošanas dati). Lietošanas dati tostarp ir:

1. ° pazīmes lietotāja identifikācijai;

2. ° dati par attiecīgas lietošanas sākumu un beigām, kā arī apjomu; un

3. ° dati par lietotāja izmantotajiem telekomunikāciju līdzekļiem.

2. Pakalpojumu sniedzējs drīkst apkopot lietotāja lietošanas datus saistībā ar dažādu telekomunikāciju līdzekļu izmantošanu, ciktāl tas ir nepieciešams norēķinu ar lietotāju vajadzībām.

[..]

6 — 2007. gada 26. februāra likums (*BGBl* 2007 I, 179. lpp.).

4. Pakalpojumu sniedzējs drīkst uzglabāt lietošanas datus ilgāk par lietošanas procesu, ciktāl tas ir nepieciešams norēķinu ar lietotāju vajadzībām (norēķinu dati). Pakalpojumu sniedzējs drīkst bloķēt datus, lai ievērotu likumiskus, statūtu vai līgumiskus uzglabāšanas termiņus. [..]"

21. Saskaņā ar *Bundesdatenschutzgesetz* (Federālais datu aizsardzības likums, turpmāk tekstā – "*BDSG*")[7] 3. panta 1. punktu "personas dati ir konkrētas norādes par identificētas vai identificējamas fiziskas personas (datu subjekts) personīgo vai materiālo stāvokli. [..]"

II – Fakti

22. *P. Breyer* ir cēlis prasību pret Vācijas Federatīvo Republiku par IP adrešu ierakstīšanas pārtraukšanu.

23. Daudzas valsts iestādes uztur vispārēji pieejamus interneta portālus, kuros tās piedāvā atjauninātu informāciju. Lai novērstu uzbrukumus un darītu iespējamu krimināltiesiskas vajāšanas uzsākšanu pret uzbrucējiem, vairākos portālos visi piekļuves gadījumi tiek saglabāti datnēs vai protokola datos. Tajos – arī pēc [lietošanas] darbības pabeigšanas – tiek saglabāts aplūkotās datnes vai tīmekļa vietnes nosaukums, meklētāja laukā ievadītie jēdzieni, piekļuves laika brīdis, pārraidīto datu apjoms, ziņojums, vai piekļuve ir bijusi veiksmīga, un datora, no kura tika veikta piekļuve, IP adrese.

24. *P. Breyer*, kas apmeklēja vairākas minētās vietnes, savā prasībā lūdza, lai Vācijas Federatīvajai Republikai piespriež pārtraukt ierakstīt vai likt ierakstīt trešajām personām saimniekdatora, no kura tiek veikta piekļuve, IP adresi, ciktāl ierakstīšana nebija nepieciešama telekomunikāciju līdzekļu pieejamības atjaunošanai traucējuma gadījumā.

25. *P. Breyer* prasība pirmās instances tiesā tika noraidīta. Tomēr viņa apelācijas sūdzība tika daļēji apmierināta, piespriežot Vācijas Federatīvajai Republikai pārtraukt veikt ierakstus, kas tiek saglabāti pēc katra piekļuves procesa beigām. Ierakstīšana bija jāpārtrauc, ja piekļuves procesa laikā prasītājs sniedza personas datus, tostarp elektroniskā pasta adreses formā, un ja tā nebija nepieciešama, lai atjaunotu telekomunikāciju pakalpojuma pieejamību.

III – Uzdotie jautājumi

26. Tā kā abas puses iesniedza kasācijas sūdzību, *Bundesgerichtshof* (Federālā Augstākā tiesa) VI palāta ir formulējusi šos prejudiciālos jautājumus, kas tika iesniegti 2014. gada 17. decembrī:

"1) Vai [..] Direktīvas 95/46/EK [..] 2. panta a) punkts ir jāinterpretē tādējādi, ka interneta protokola adrese (IP adrese), ko pakalpojumu sniedzējs ieraksta saistībā ar piekļuvi tā interneta vietnei, attiecībā uz šo pakalpojumu sniedzēju ir uzskatāma par personas datiem jau tad, ja trešajai personai (šajā gadījumā tai, kas nodrošina pieslēgumu) ir datu subjekta identificēšanai nepieciešamā papildinformācija?

2) Vai ar Datu aizsardzības direktīvas 7. panta f) punktu netiek pieļauta valsts tiesību norma, atbilstoši kurai pakalpojumu sniedzējs lietotāja personas datus bez viņa piekrišanas var iegūt un izmantot tikai tad, kad tas ir nepieciešams, lai nodrošinātu telekomunikāciju līdzekļa konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un atbilstoši kurai mērķis nodrošināt vispārēju telekomunikāciju līdzekļa funkcionēšanas spēju nevar attaisnot izmantošanu pēc attiecīga lietošanas procesa beigām?"

7 — 1990. gada 20. decembra likums (*BGBl* 1990 I, 2954. lpp.).

27. Kā paskaidro iesniedzējtiesa, saskaņā ar Vācijas tiesībām prasītājs varētu lūgt pārtraukt IP adrešu ierakstīšanu, ja atbilstoši tiesību aktiem par datu aizsardzību to saglabāšana būtu prettiesiska iejaukšanās tā vispārējās personiskajās tiesībās, it īpaši, viņa tiesībās pašam noteikt personas datu izmantošanu (*Bürgerliches Gesetzbuch* (Vācijas Civillikums) 1004. panta 1. punkts un 823. panta 1. punkts, aplūkojot kopsakarā ar *Grundgesetz* (Pamatlikums) 1. un 2. pantu).

28. Tā tas būtu, ja a) IP adrese (jebkurā gadījumā kopā ar piekļuves tīmekļa vietnei laika brīdi) varētu tikt kvalificēta kā "personas dati" Direktīvas 95/46 2. panta a) punkta, aplūkojot kopsakarā ar preambulas 26. apsvēruma otro teikumu, vai *TMG* 12. panta 1. un 3. punkta, aplūkojot kopsakarā ar *BDSG* 3. panta 1. punktu, izpratnē un, b) ja nav izpildīts neviens atļaujas nosacījums Direktīvas 95/46 7. panta f) punkta vai *TMG* 12. panta 1. un 3. punkta un 15. panta 1. un 4. punkta izpratnē.

29. *Bundesgerichtshof* (Federālā Augstākā tiesa) uzskata, ka, lai interpretētu valsts tiesības (*TMG* 12. panta 1. punkts), ir jāzina, kā ir jāsaprot personas dati, uz kuriem ir atsauce Direktīvas 95/46 2. panta a) punktā.

30. Turklāt tiesa *a quo* norāda, ka, tā kā saskaņā ar *TMG* 15. panta 1. punktu pakalpojumu sniedzējs drīkst iegūt un izmantot lietotāja personas datus tikai tad, ja tas ir vajadzīgs, lai nodrošinātu telekomunikāciju pakalpojumu izmantošanu un norēķinu par tiem (lietošanas dati) [8], šīs valsts tiesību normas interpretācija ir saistīta ar Direktīvas 95/46 7. panta f) punktu.

IV – Tiesvedība Tiesā un lietas dalībnieku argumenti

31. Rakstveida apsvērumus iesniedza Vācijas, Austrijas un Portugāles valdības, kā arī Komisija. Tikai šī iestāde, kā arī *P. Breyer* piedalījās tiesas sēdē, kas notika 2016. gada 25. februārī, kurā Vācijas valdība atteicās piedalīties.

A – *Lietas dalībnieku argumenti saistībā ar pirmo jautājumu*

32. *P. Breyer* uzskata, ka personas dati ir arī tie, kurus var apkopot tikai no teorētiskā viedokļa, proti, pamatojoties uz abstrakti iespējamām briesmām, un nav nozīmes tam, vai šāda apkopošana praksē faktiski ir notikusi. Viņa skatījumā tas, ka iestāde drīzāk nespētu identificēt personu pēc IP adreses, nenozīmē, ka šī persona nav pakļauta briesmām. Turklāt viņš uzskata, ka nozīme ir tam, ka Vācija saglabā viņa IP datus, lai vajadzības gadījumā identificētu iespējamos uzbrukumus vai uzsāktu krimināltiesisku vajāšanu, kā tas ir atļauts *Telekommunikationsgesetz* (Telekomunikāciju likums) 113. pantā un kas jau ir noticis vairākkārt.

33. Vācijas valdība uzskata, ka uz pirmo jautājumu ir jāsniedz noraidoša atbilde. Pēc tās domām, dinamiskās IP adreses neatklāj "identificēto" personu Direktīvas 95/46 2. panta a) punkta izpratnē. Lai izlemtu, vai tie sniedz informāciju par "identificējamo" personu šīs tiesību normas izpratnē, *identificējamības* pārbaude ir jāveic, piemērojot "relatīvo" kritēriju. Pēc tās domām, tas izriet no Direktīvas 95/46 preambulas 26. apsvēruma saskaņā ar kuru būtu jāņem vērā tikai tie līdzekļi, kurus, iespējams, "pamatoti" izmantotu vai nu personas datu apstrādātājs, vai trešā persona, lai identificētu minēto personu. Šāds skaidrojums norādot, ka Savienības likumdevējs Direktīvas 95/46 piemērošanas jomā nav vēlējies iekļaut tādas situācijas, kurās jebkurai trešajai personai būtu objektīvi iespējams veikt identificēšanu.

8 — Saskaņā ar *Bundesgerichtshof* (Federālā Augstākā tiesa) viedokli lietošanas dati ir pazīmes lietotāja identifikācijai, dati par attiecīgas izmantošanas sākumu un beigām, kā arī apjomu, un dati par lietotāja izmantotajiem telekomunikāciju līdzekļiem.

34. Vācijas valdība arī uzskata, ka jēdziens "personas dati" Direktīvas 95/46 2. panta a) punkta izpratnē ir jāinterpretē, ņemot vērā šīs direktīvas mērķi, proti, nodrošināt pamattiesību ievērošanu. Nepieciešamību nodrošināt fizisko personu aizsardzību varot aplūkot atšķirīgi, atkarībā no tā, kam pieder dati, un vai tā rīcībā ir personu identificēšanai nepieciešamie līdzekļi.

35. Vācijas valdība apgalvo, ka *P. Breyer* nav identificējams pēc IP adreses, skatot to kopsakarā ar citiem satura nodrošinātāju saglabātajiem datiem. Tāpēc to rīcībā būtu jābūt informācijai, kas ir interneta piekļuves nodrošinātājam, kurš nevar to nodot satura nodrošinātājiem, ja tam nav tiesiska pamata.

36. Austrijas savukārt valdība uzskata, ka ir sniedzama apstiprinoša atbilde. Direktīvas 95/46 preambulas 26. apsvērumā nav skaidri noteikts, ka, lai personu varētu uzskatīt par identificējamu, visiem identificēšanai nepieciešamajiem datiem būtu jābūt viena subjekta rīcībā. Tādējādi IP adrese varot būt personas dati, ja trešajai personai (piemēram, interneta piekļuves nodrošinātājam) ir līdzekļi, lai bez pārmērīgas piepūles identificētu šīs adreses īpašnieku.

37. Portugāles vadība arī piedāvā sniegt apstiprinošu atbildi, uzskatot, ka IP adrese, kopā ar apmeklējuma datumu, ir personas dati, ciktāl subjekts, kas nav tas subjekts, kurš saglabājis IP adresi, var ļaut identificēt lietotāju.

38. Komisija arī ierosina atbildēt apstiprinoši, pamatojoties uz risinājumu, ko Tiesa ir izmantojusi spriedumā *Scarlet Extended*[9]. Komisijas skatījumā, ņemot vērā to, ka IP adreses tiek saglabātas tieši tāpēc, lai identificētu lietotājus kiberuzbrukumu gadījumā, interneta piekļuves nodrošinātāja ierakstītās papildinformācijas izmantošana nozīmētu līdzekli, ko var "pamatoti" izmantot Direktīvas 95/46 preambulas 26. apsvēruma izpratnē. Visbeidzot, ņemot vērā gan Direktīvā 95/46 izvirzīto mērķi, gan Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 7. un 8. pantu, Direktīvas 95/46 2. panta a) punkts, pēc Komisijas domām, ir jāinterpretē plaši.

B – *Lietas dalībnieku argumenti saistībā ar otro jautājumu*

39. *P. Breyer* uzskata, ka Direktīvas 95/46 7. panta f) punkts ir vispārējs noteikums, kura īstenošanai ir jāsniedz precizējumi. Tāpēc atbilstoši Tiesas judikatūrai būtu jāizvērtē katras lietas konkrētie apstākļi un jānosaka, vai ir grupas, kurām ir likumīgas intereses šīs tiesību normas izpratnē, un, ja tādas ir, šī panta piemērošanas nolūkā ir ne tikai atļauts šādām grupām paredzēt īpašus noteikumus, bet arī tie ir jāparedz. Šajā gadījumā *P. Breyer* uzskata, ka valsts tiesiskais regulējums ir saderīgs ar Direktīvas 95/46 7. panta f) punktu, jo nepastāv portāla publiska interese saglabāt personas datus vai lielāka nozīme ir piešķirta interesei saglabāt anonimitāti. Viņa ieskatā sistemātiska personas datu saglabāšana tomēr nav saderīga ar demokrātisko sabiedrību un nav nedz vajadzīga, nedz samērīga, lai nodrošinātu elektronisko līdzekļu funkcionēšanas spēju, kas ir iespējams, neierakstot personas datus, kā to pierādot dažu federālo ministriju tīmekļa vietnes.

40. Vācijas valdība apgalvo, ka otrais jautājums, kas uzdots tikai gadījumā, ja uz pirmo jautājumu būtu jāsniedz apstiprinoša atbilde, nav jāaplūko, jo iepriekš minēto iemeslu dēļ, pēc tās domām, šāda atbilde nav jāsniedz.

41. Austrijas valdība ierosina atbildēt, ka Direktīvai 95/46 vispārīgi nav pretrunā tādu datu kā pamatlietā aplūkotie strīdīgie dati saglabāšana, ja tā ir nepieciešama, lai nodrošinātu elektronisko līdzekļu labu funkcionēšanas spēju. Šīs valdības ieskatā IP adreses pagaidu saglabāšana, kas ir ilgāka par tīmekļa vietnes lietošanas ilgumu, var būt likumīga, ja personas datu apstrādātājs ievēro pienākumu īstenot šo datu aizsardzības pasākumus, kas paredzēti Direktīvas 95/46 17. panta 1. punktā. Kiberuzbrukumu apkarošanas nolūkā datu analīze attiecībā uz iepriekšējiem uzbrukumiem

9 — 2011. gada 24. novembra spriedums (C-70/10, EU:C:2011:771), 51. punkts.

var būt likumīga un atsevišķām IP adresēm var liegt piekļuvi tīmekļa vietnei. No elektronisko līdzekļu labas funkcionēšanas spējas nodrošināšanas objektīvā skatupunkta tādu datu kā pamatlietā aplūkotie saglabāšanas samērīgums būtu jāvērtē katrā gadījumā atsevišķi, ņemot vērā Direktīvas 95/46 6. panta 1. punktā minētos principus.

42. Portugāles valdība uzskata, ka Direktīvas 95/46 7. panta f) punktam nav pretrunā pamatlietā aplūkotās valsts tiesību normas, jo Vācijas likumdevējs jau esot veicis šajā tiesību normā paredzēto izsvēršanu starp personas datu apstrādātāja likumīgajām interesēm, no vienas puses, un minēto datu subjektu tiesībām un brīvībām, no otras puses.

43. Komisijas skatījumā valsts tiesiskajā regulējumā, ar kuru ir transponēts Direktīvas 95/46 7. panta f) punkts, personas datu apstrādes mērķi ir jādefinē attiecīgajai privātpersonai paredzamā veidā. Pēc tās domām, Vācijas tiesiskajā regulējumā šī prasība nav ievērota, norādot *TMG* 15. panta 1. punktā, ka IP adrešu saglabāšana ir atļauta, "ja tas ir vajadzīgs, lai nodrošinātu telekomunikāciju pakalpojumu izmantošanu [..]".

44. Tāpēc Komisija uz otro jautājumu ierosina atbildēt, ka šai tiesību normai ir pretrunā valsts tiesību normas interpretācija, saskaņā ar kuru valsts iestāde, kas darbojas kā pakalpojumu sniedzēja, var iegūt un izmantot lietotāja personas datus bez viņa piekrišanas arī tad, ja tās mērķis ir nodrošināt elektroniskā līdzekļa vispārēju labu funkcionēšanas spēju, ja šis mērķis minētajā valsts tiesību normā nav noteikts pietiekami skaidri un precīzi.

V – Vērtējums

A – *Pirmais jautājums*

1) Uzdotā jautājuma robežas noteikšana

45. Saskaņā ar *Bundesgerichtshof* (Federālā Augstākā tiesa) formulējumu ar pirmo prejudiciālo jautājumu tā vēlas noskaidrot, vai IP adrese, no kuras ir piekļūts tīmekļa vietnei, šīs vietnes īpašniecei – valsts iestādei – ir personas dati [Direktīvas 95/46 2. panta a) punkta izpratnē], ja interneta piekļuves nodrošinātāja rīcībā ir papildinformācija, kas ļauj identificēt datu subjektu.

46. Šāds jautājuma formulējums ir pietiekami precīzs, lai pašā sākumā noraidītu citus jautājumus, kas varētu rasties *in abstracto* par IP adrešu juridisko statusu saistībā ar personas datu aizsardzību.

47. Pirmkārt, *Bundesgerichtshof* (Federālā Augstākā tiesa) atsaucas tikai uz "dinamiskajām IP adresēm", proti, tām, kas tiek piešķirtas uz laiku, katrreiz pieslēdzoties tīklam, un mainās turpmākiem pieslēgumiem. Tādējādi netiek aplūkotas "statiskās vai fiksētās IP adreses", kas ir nemainīgas un ļauj pastāvīgi identificēt tīklam pieslēgto ierīci.

48. Otrkārt, iesniedzējtiesa pamatojas uz pieņēmumu, ka tiesvedībā *a quo* iesaistītā tīmekļa vietnes īpašniece ar dinamiskās IP adreses palīdzību nespēj identificēt personas, kas apmeklē vietnes, un tās rīcībā arī nav papildinformācija, kas kopā ar šo IP adresi ļauj viņu identificēt. *Bundesgerichtshof* (Federālā Augstākā tiesa), šķiet, uzskata, ka šajā kontekstā dinamiskā IP adrese *tīmekļa vietnes īpašniekam* nav personas dati Direktīvas 95/46 2. panta a) punkta izpratnē.

49. Iesniedzējtiesa šaubās, vai tīmekļa vietnes īpašniekam dinamiskā IP adrese var tikt uzskatīta par personas datiem, *ja trešās personas rīcībā ir papildinformācija*, kas kopā ar to ļauj identificēt personas, kuras apmeklē tā tīmekļa vietnes. Taču ir jāmin viens svarīgs precizējums, ka *Bundesgerichtshof* (Federālā Augstākā tiesa) neatsaucas uz jebkuru trešo personu – papildinformācijas īpašnieku, bet tikai uz interneta piekļuves nodrošinātāju (tādējādi tā izslēdz citus, kuru rīcībā, iespējams, ir šādi dati).

50. Tādējādi tostarp netiek apspriesti šādi aspekti: a) vai statiskās IP adreses ir personas dati saskaņā ar Direktīvu 95/46 [10]; b) vai dinamiskās IP adreses vienmēr un jebkādos apstākļos ir personas dati šīs direktīvas izpratnē un visbeidzot c) vai dinamiskās IP adreses obligāti ir jāuzskata par personas datiem, līdzko ir kāda trešā persona, kas spēj tos izmantot, lai identificētu tīkla lietotājus.

51. Tādējādi runa ir tikai par to, vai dinamiskā IP adrese interneta pakalpojumu sniedzējam ir personas dati, kad telekomunikāciju uzņēmumam, kurš sniedz piekļuvi tīklam (piekļuves nodrošinātājs), ir papildinformācija, kas kopā ar šo adresi ļauj identificēt personu, kura piekļuvusi tīmekļa vietnei, ko pārvalda pakalpojumi sniedzējs.

2) Par lietas būtību

52. Šajā lūgumā sniegt prejudiciālu nolēmumu ietvertais jautājums ir plaši apspriests Vācijas judikatūrā un doktrīnā, attiecībā uz kuru ir divi atšķirīgi viedokļi [11]. Saskaņā ar vienu viedokli (kas izvēlas "objektīvo" vai "absolūto" kritēriju) lietotājs ir identificējams – un tāpēc IP adrese ir aizsargājami personas dati – katrreiz, kad neatkarīgi no interneta pakalpojumu sniedzēja rīcībā esošajiem līdzekļiem un spējām viņu ir iespējams identificēt, ja šo dinamisko IP adresi aplūko kopā ar trešo personu (piemēram, tīkla piekļuves nodrošinātāja) sniegtajiem datiem.

53. Otrā virziena piekritēji (kas aizstāv "relatīvo" kritēriju) uzskata, ka iespēja rēķināties ar trešās puses palīdzību lietotāja identificēšanā nav pietiekama, lai dinamisko IP adresi uzskatītu par personas datiem. Nozīme ir tās personas, kurai ir piekļuve datiem, spējai tos izmantot ar saviem līdzekļiem un tādējādi identificēt personu.

54. Neatkarīgi no šī strīda formulējuma valsts tiesībās, sniedzot atbildi, Tiesai ir jāinterpretē divi Direktīvas 95/46 noteikumi, uz kuriem ir norādījusi tiesa *a quo*, kā arī lietas dalībnieki, proti, tās 2. panta a) punkts [12] un tās preambulas 26. apsvērums [13].

55. Dinamiskās IP adreses tikai tāpēc vien, ka tās sniedz informāciju par datumu un laika brīdi, kurā notika piekļuve tīmekļa vietnei no datora (vai citas ierīces), atklāj konkrētus interneta lietotāju uzvedības paradumus un tādējādi ietver iespējamu iejaukšanos tiesībās uz privātās dzīves neaizskaramību [14], kas ir garantētas Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas 8. pantā un Hartas 7. pantā, saskaņā ar kuru, kā arī ar tās 8. pantu ir jāinterpretē Direktīva 95/46 [15]. Faktiski lietas dalībnieki neapstrīd šo pieņēmumu, uz ko arī pats par sevi neattiecas prejudiciālais jautājums.

10 — Tiesa aplūkoja problēmu 2011. gada 24. novembra spriedumā *Scarlet Extended* (C-70/10, EU:C:2011:771), 51. punkts, un 2012. gada 19. aprīļa spriedumā *Bonnier Audio* u.c. (C-461/10, EU:C:2012:219). Šī pēdējā minētā sprieduma 51. un 52. punktā Tiesa ir secinājusi, ka informācija "nolūkā to identificēt – [attiecībā uz] tā [..] interneta lietotāja vārdu vai nosaukumu un adresi, kas lieto IP adresi, no kuras, iespējams, prettiesiski ir izplatītas datnes, kas satur aizsargātus darbus [..], ir uzskatāma par personas datu apstrādi Direktīvas 2002/58 2. panta pirmās daļas, skatot to kopsakarā ar Direktīvas 95/46 2. panta b) punktu, izpratnē".

11 — Par abām doktrinārām nostājām skat., piemēram, Schreibauer, M., no: *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P. un von Lewinski, K. (red.), Ķelne: *Carl Heymanns Verlag/Wolters Kluwer*, 2014, 4. izd., 11. punkts *Telemediengesetz* (4.–10.). Nink, J. un Pohle, J., "Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze", no: *Multimedia und Recht*, 9/2015, 563.–567. lpp. Heidrich, J. un Wegener, C., "Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging", no: *Multimedia und Recht*, 8/2015, 487.–492. lpp. Leisterer, H., "Die neuen Pflichten zur Netz- und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr", no: *Computer und Recht*, 10/2015, 665.–670. lpp.

12 — Minēts 13. punktā.

13 — Minēts 11. punktā.

14 — Kā to ir atgādinājis ģenerāladvokāts P. Kruss Viljalons [*P. Cruz Villalón*] savos secinājumos lietā *Scarlet Extended* (C-70/10, EU:C:2011:255), 76. punkts, un kā to ir apstiprinājis Eiropas Datu aizsardzības uzraudzītājs savā 2010. gada 22. februāra atzinumā par notiekošajām Eiropas Savienības sarunām saistībā ar Nolīgumu par viltotu preču tirdzniecības apkarošanu (*ACTA*) (OV, C 147, 1. lpp., 24. punkts), un 2010. gada 10. maija atzinumā par priekšlikumu Eiropas Parlamenta un Padomes Direktīvai par seksuālās vardarbības pret bērniem, bērnu seksuālās izmantošanas un bērnu pornogrāfijas apkarošanu, ar ko atceļ Pamatlēmumu 2004/68/TI (OV 2010, C 323, 6. lpp., 11. punkts).

15 — Šajā ziņā skat. 2003. gada 20. maija spriedumu *Österreichischer Rundfunk* (C-465/00, C-138/01 un C-139/01, EU:C:2003:294), 68. punkts, un ģenerāladvokātes J. Kokotes [*J. Kokott*] secinājumus lietā *Promusicae* (C-275/06, EU:C:2007:454), 51. un nākamie punkti.

56. Persona, ko uz kuru attiecas minētie apstākļi, nav "identificēta fiziska persona". Pieslēgšanās datums un laika brīdis, kā arī ar ciparu palīdzību atveidotā adrese nedz tieši, nedz nepastarpināti nenorāda uz fizisko personu, kam pieder ierīce, ar kuras palīdzību tā apmeklē tīmekļa vietni, nedz arī uz lietotāja, kas ar to rīkojas, identitāti (tā var būt jebkura fiziska persona).

57. Tomēr, ciktāl dinamiskā IP adrese – gan pati par sevi, gan kopā ar citiem datiem – palīdz noteikt, kam pieder ierīce, kura tiek lietota, lai piekļūtu tīmekļa vietnei, var uzskatīt, ka tā ir informācija par "identificējamu personu" [16].

58. Saskaņā ar *Bundesgerichtshof* (Federālā Augstākā tiesa) lūgumu sniegt prejudiciālu nolēmumu dinamiskā IP adrese pati par sevi nav pietiekama, lai identificētu lietotāju, kas ar tās starpniecību ir piekļuvis tīmekļa vietnei. Savukārt, ja interneta pakalpojumu sniedzējs ar dinamiskās IP adreses palīdzību varētu identificēt lietotāju, neapšaubāmi, runa būtu par personas datiem Direktīvas 95/46 izpratnē. Tomēr nešķiet, ka šāda būtu prejudiciālā jautājuma jēga, kurā ir uzsvērts, ka tiesvedībā *a quo* iesaistītie interneta pakalpojumu sniedzēji nevar identificēt lietotāju tikai ar dinamiskās IP adreses palīdzību.

59. Dinamiskā IP adrese kopā ar citiem datiem ļauj "netieši" identificēt lietotāju – tam piekrīt visi. Vai dinamisko IP adresi var uzskatīt par personas datiem saskaņā ar direktīvu, ja ir iespēja, ka pastāv ar šo adresi saistīta papildinformācija? Būs jārod risinājums tam, vai šajā nolūkā pietiek ar abstraktu iespēju uzzināt šos datus vai, gluži pretēji, tiem ir jābūt pieejamiem personām, kas jau zina dinamisko IP adresi, vai trešajai personai.

60. Lietas dalībnieki savos apsvērumos galvenokārt pievērsās Direktīvas 95/46 preambulas 26. apsvēruma interpretācijai, kurā tie norādīja uz izteicienu "līdzekļi, kurus, iespējams, pamatoti izmantotu vai nu personas datu apstrādātājs, vai jebkura cita persona, lai identificētu minēto personu". Iesniedzējtiesas jautājums neattiecas uz papildinformāciju, kas ir pamatlietā iesaistīto pakalpojuma sniedzēju rīcībā. Tāpat tajā nav norādes uz kādu trešo personu, kuras rīcībā ir šī papildinformācija (kura kopā ar dinamisko IP adresi ļauj identificēt lietotāju), bet uz interneta piekļuves nodrošinātāju.

61. Tāpēc Tiesai nav jāanalizē visi līdzekļi, kurus atbildētāja tiesvedībā *a quo* "pamatoti" varētu izmantot, lai varētu uzskatīt, ka dinamiskās IP adreses ir personas dati. Tā kā *Bundesgerichtshof* (Federālā Augstākā tiesa) atsaucas tikai uz trešās personas rīcībā esošu papildinformāciju, var secināt: a) vai nu atbildētājai nav īpašas papildinformācijas, kas ļauj veikt lietotāja identifikāciju, b) vai arī, ka, ja šie dati tai ir pieejami, tā nespēj tos pamatoti izmantot šajā nolūkā kā to apstrādātājs saskaņā ar Direktīvas 95/46 preambulas 26. apsvērumu.

62. Abi pieņēmumi ir atkarīgi no faktu konstatējuma, kas ir jāveic tikai iesniedzējtiesai. Tiesa gan varētu noteikt vispārējos kritērijus, lai interpretētu izteicienu "līdzekļi, kurus, iespējams, pamatoti izmantotu [..] personas datu apstrādātājs", ja *Bundesgerichtshof* (Federālā Augstākā tiesa) rastos kādas šaubas par atbildētājas spēju pamatoti izmantot īpašu papildinformāciju. Tā kā tas tā nav, Tiesai, manuprāt, nav jānosaka daži interpretācijas kritēriji, kas iesniedzējtiesai nav vajadzīgi un ko tā arī nav lūgusi sniegt.

16 — Ja vien nav pierādījuma atspēkojuma, ir jāpieņem, ka minētā persona ir lietojusi internetu un piekļuvusi attiecīgajai tīmekļa vietnei. Tādējādi, ņemot vērā šo pēdējo pieņēmumu, informācija par piekļuves tīmekļa vietnei datumu, laika brīdi un ar ciparu palīdzību atveidotu adresi ļautu piedēvēt šo piekļuvi ierīces īpašniekam un netieši saistīt to ar viņa uzvedības tīklā paradumiem. Izņēmums, iespējams, būtu IP adreses, kas tiek piešķirtas interneta kafejnīcās izvietotajiem datoriem, kuru anonīmie lietotāji nav identificējami un par kuriem to īpašniekiem nav nekādas atbilstīgas personiskās informācijas. Turklāt tas ir vienīgais izņēmums no principa, ka IP adreses ir personas dati, ko ir pieņēmusi ar Direktīvu 95/46 izveidotā darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi (saukta par "29. panta grupu"). Tās 2007. gada 20. jūnija Atzinums 4/2007 par personas datu jēdzienu, WP 136 ir pieejams http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

63. Uzdotā jautājuma mērķis ir atrisināt jautājumu, vai, lai dinamiskās IP adreses uzskatītu par personas datiem, ir nozīme apstāklim, ka ļoti specifiskas trešās personas –interneta piekļuves nodrošinātāja – rīcībā ir papildinformācija, kas kopā ar šīm adresēm ļauj identificēt lietotāju, kurš ir apmeklējis konkrētu tīmekļa vietni.

64. Atkal ir jāatsaucas uz Direktīvas 95/46 preambulas 26. apsvērumu. Izteiciens "līdzekļi, kurus, iespējams, pamatoti izmantotu [..] *jebkura cita persona*" [17], varētu pamatot interpretāciju, saskaņā ar kuru pietiktu, ka jebkura trešā persona varētu iegūt papildinformāciju (ko var izmantot kopā ar dinamisko IP adresi, lai identificētu personu), lai uzskatītu, ka šī adrese ir *eo ipso* personas dati.

65. Piemērojot šo plašo interpretāciju, par personas datiem praksē varētu uzskatīt jebkādu informāciju pašu par sevi, lai cik nepietiekama tā būtu, kas ļauj identificēt lietotāju. Nekad pilnīgi droši nevarētu noteikt, vai ir trešā persona, kuras rīcībā ir papildinformācija, ko var izmantot kopā šo informāciju, un tādējādi tas ļautu noteikt personas identitāti.

66. Manuprāt, iespēja, ka tehnisko līdzekļu attīstība jūtami bruģē ceļu arvien sarežģītākiem informācijas iegūšanas un apstrādes instrumentiem, kas būs izmantojami tuvākā vai tālākā nākotnē, pamato tādu piesardzības pasākumu ieviešanu, ar kuriem priekšlaikus ir jāaizsargā privātums. Definējot attiecīgās juridiskās kategorijas datu aizsardzības jomā, ir mēģināts iekļaut pietiekami plašus un elastīgus pieņēmumus attiecībā uz rīcību, lai tos varētu piemērot jebkuram iespējamam gadījumam [18].

67. Tomēr es uzskatu, ka šo bažu dēļ – kas citādi ir ļoti pamatotas – nevar neņemt vērā likumdevēja nodomu un pieļaut tādu Direktīvas 95/46 preambulas 26. apsvēruma sistēmisku interpretāciju, kas būtu ierobežota tikai ar "līdzekļ[iem], kurus, iespējams, pamatoti izmantotu" *konkrētas trešās personas*.

68. Preambulas 26. apsvērumā arī nav nekādas atsauces uz jebkādiem datu apstrādātāja (šajā gadījumā interneta pakalpojumu sniedzējs) izmantojamiem līdzekļiem, bet tikai uz tiem, kurus tas var "pamatoti" izmantot, tāpat ir jāsaprot, ka likumdevējs atsaucas uz "trešām personām", pie kurām *arī pamatoti* var vērsties datu apstrādātājs, kas vēlas iegūt papildinformāciju identificēšanas nolūkā. Tas nenotiktu, ja saskare ar šīm trešajām personām faktiski būtu ļoti sarežģīta no cilvēciskā vai ekonomiskā viedokļa vai ja tā būtu praktiski neīstenojama vai aizliegta tiesību aktos. Kā minēts iepriekš, citādi praktiski būtu neiespējami izvēlēties kādu no līdzekļiem, jo vienmēr būtu jāiztēlojas, ka, iespējams, ir trešā persona, kura, būdama nepieejama interneta pakalpojumu sniedzējam, var iegūt – tagad un nākotnē – attiecīgu informāciju, kas varētu palīdzēt identificēt lietotāju.

69. Saskaņā ar iepriekš izklāstīto trešā persona, uz kuru atsaucas *Bundesgerichtshof* (Federālā Augstākā tiesa), ir interneta piekļuves nodrošinātājs. Protams, ir saprātīgāk uzskatīt, ka pakalpojumu sniedzējs vēršas pie trešās personas, lai saņemtu precīzu papildinformāciju, ja tas vēlas efektīvi, praktiski un tieši identificēt lietotāju, kas piekļuvis tīmekļa vietnei ar dinamiskās IP adreses palīdzību. Nekādā ziņā tā nav hipotētiska, nezināma un nepieejama trešā persona, bet galvenā dalībniece interneta kontekstā, par kuru ir droši zināms, ka tās rīcībā ir pakalpojumu sniedzējam nepieciešamie dati, lai identificētu lietotāju. Faktiski, kā norāda iesniedzējtiesa, atbildētāja pamatlietā vēlas vērsties pie šīs konkrētās trešās personas, lai saņemtu tai nepieciešamo papildinformāciju.

70. Interneta piekļuves nodrošinātājs parasti ir trešā persona, uz kuru ir atsauce Direktīvas 95/46 preambulas 26. apsvērumā un pie kuras pēc iespējas "pamatoti" var vērsties pakalpojumu sniedzējs tiesvedībā *a quo*. Tomēr ir jānoskaidro, vai šīs trešās personas rīcībā esošas papildinformācijas iegūšana var tikt uzskatīta par "pamatoti" ticamu vai izmantojamu.

17 — Mans izcēlums.

18 — Šis piesardzības un preventīvais mērķis ir 29. panta grupas nostājas pamatā, kura, kā tika norādīts, uzskata, ka pamatā ir jābūt principam, ka IP adreses ir personas dati, pieņemot kā vienīgo izņēmumu gadījumu, kurā pakalpojuma sniedzējs pilnīgi droši var noteikt, ka runa ir par adresēm, kas atbilst neidentificējamām personām, kā tas var būt gadījumā ar lietotājiem interneta kafejnīcās. Skat. 16. zemsvītras piezīmes beigas.

71. Vācijas valdība apgalvo, ka, tā kā interneta piekļuves nodrošinātāja rīcībā esošā informācija ir personas dati, tas nevar to darīt zināmu tāpat vien, bet tikai saskaņā ar šo datu apstrādi regulējošo tiesisko regulējumu [19].

72. Neapšaubāmi, ka tas tā ir, jo, lai izmantotu šo informāciju, ir jāievēro personas datiem piemērojamie tiesību akti. Informāciju var "pamatoti" iegūt tikai tad, ja ir izpildīti nosacījumi par piekļuvi šādiem datiem; pirmais no tiem ir likumīga iespēja tos uzglabāt un nodot citiem. Ir acīmredzami, ka interneta piekļuves nodrošinātājam ir tiesības atteikties nodot attiecīgos datus, bet var būt arī otrādi. Pilnīgi "pamatota" datu nodošanas iespēja pati par sevi padara dinamisko IP adresi interneta pakalpojumu sniedzējam par personas datiem saskaņā ar Direktīvas 95/46 preambulas 26. apsvērumu.

73. Runa ir par īpašu iespēju *likuma ietvaros* un tāpēc "pamatotu" iespēju. Pamatotiem piekļuves līdzekļiem, uz kuriem ir atsauce Direktīvā 95/46, pēc definīcijas ir jābūt likumīgiem [20]. Tāds ir pieņēmums, uz kura dabiski pamatojas iesniedzējtiesa, kā to atgādina Vācijas valdība [21]. Tādējādi būtiski tiek ierobežoti juridiski atbilstīgi piekļuves veidi, jo tiem ir jābūt tikai un vienīgi likumīgiem. Taču, kamēr tie pastāv, lai cik ierobežojoši tie būtu, piemērojot tos praksē, tie ir "pamatots līdzeklis" Direktīvas 95/46 izpratnē.

74. Tāpēc es uzskatu, ka, ņemot vērā *Bundesgerichtshof* (Federālā Augstākā tiesa) lietoto formulējumu, uz pirmo tās jautājumu ir jāsniedz apstiprinoša atbilde. Dinamiskā IP adrese interneta pakalpojumu sniedzējam ir jāuzskata par personas datiem, ja ir trešā persona (interneta piekļuves nodrošinātājs), pie kuras pamatoti varētu vērsties, lai saņemtu papildinformāciju, kas kopā ar minēto adresi palīdz identificēt lietotāju.

75. Manuprāt, to apstiprina rezultāts, kas tiktu sasniegts, piemērojot risinājumu, kurš būtu pretējs manis ierosinātajam. Ja dinamiskās IP adreses interneta pakalpojumu sniedzējam nebūtu personas dati, tas varētu tos saglabāt nenoteiktu laiku un jebkurā brīdī varētu lūgt interneta piekļuves nodrošinātājam papildinformāciju, lai to izmantotu kopā ar [dinamiskajām IP adresēm] un identificētu lietotāju. Šajos apstākļos, kā to atzīst Vācijas valdība [22], piemērojot attiecīgos tiesību aktus par datu aizsardzību, dinamiskā IP adrese kļūtu par personas datiem ikreiz, kad būtu pieejama derīga papildinformācija, lai identificētu lietotāju.

76. Tomēr runa būtu par datiem, kurus saglabāt varētu tikai tik ilgi, kamēr pakalpojumu sniedzējam tie netiktu uzskatīti par personas datiem. Tādējādi, ja tā būtu šī pēdējā minētā rīcībā, dinamiskā IP adrese būtu juridiski jākvalificē kā personas dati, ja pastāvētu iespēja, ka nākotnē lietotāja identificēšanai tas izlemtu izmantot to kopā ar papildinformāciju, kas būtu jāsaņem no trešās personas. Tomēr saskaņā ar Direktīvu 95/46 izšķiroša nozīme, manuprāt, ir – pamatotai – iespējai, ka ir "pieejama" trešā persona, kurai ir nepieciešamie līdzekļi, lai identificētu datu subjektu, un nevis tas, ka iespēja vērsties pie šīs trešās personas tiek izmantota.

77. Kopā ar Vācijas valdību varētu pieņemt, ka dinamiskā IP adrese kļūst par personas datiem, tiklīdz to saņem interneta piekļuves pakalpojuma sniedzējs. Tātad, ņemot to vērā, būtu jāpieņem, ka attiecībā uz IP adreses saglabāšanas termiņu šī kvalifikācija būtu jāveic ar atpakaļejošu spēku un tādējādi tā jāuzskata par neesošu, ja ir beidzies termiņš, kurā tā varēja tikt saglabāta, ja no paša sākuma tā bija jāuzskata par personas datiem. Šajos apstākļos būtu jādod priekšroka risinājumam, kas neatbilst tiesību

19 — Rakstveida apsvērumu 40. un 45. punkts.

20 — Šajā kontekstā nav svarīgi, ka *de facto* ir iespējams piekļūt personas datiem, pārkāpjot likumus par datu aizsardzību.

21 — Tās rakstveida apsvērumu 47. un 48. punkts.

22 — Rakstveida apsvērumu 36. punkts.

aktu par personas datiem garam. Iemesls, kas pamato šo datu tikai pagaidu saglabāšanu, tiktu izkropļots, pieļaujot iespējamo kavēšanos, lai no paša sākuma atzītu tiem piemītošās īpašības nozīmi: tie var būt fiziskas personas identifikācijas līdzeklis – paši par sevi vai kopā ar citiem datiem. Tāpēc šī tīri ekonomiskā iemesla dēļ ir saprātīgāk piešķirt tiem šādu īpašību no paša sākuma.

78. Tādējādi mans pirmais secinājums ir, ka Direktīvas 95/46 2. panta a) punkts ir jāinterpretē tādējādi, ka IP adrese, ko pakalpojumu sniedzējs ieraksta saistībā ar piekļuvi tā interneta vietnei, šim pakalpojumu sniedzējam ir uzskatāma par personas datiem jau tad, ja (interneta) piekļuves nodrošinātājam ir datu subjekta identificēšanai nepieciešamā papildinformācija.

B – *Otrais jautājums*

79. Ar savu otro prejudiciālo jautājumu *Bundesgerichtshof* (Federālā Augstākā tiesa) vēlas noskaidrot, vai Direktīvas 95/46 7. panta f) punktam ir pretrunā valsts tiesību norma, atbilstoši kurai personas datus bez tās piekrišanas var iegūt un izmantot tikai tad, kad tas ir nepieciešams, lai nodrošinātu telekomunikāciju līdzekļa konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un atbilstoši kurai mērķis nodrošināt vispārēju telekomunikāciju līdzekļa funkcionēšanas spēju nevar attaisnot izmantošanu pēc attiecīga lietošanas procesa beigām.

80. Pirms atbildes ir jāsniedz paskaidrojums attiecībā uz *Bundesgerichtshof* (Federālā Augstākā tiesa) sniegto informāciju, saskaņā ar kuru strīdīgie dati ir saglabāti, lai nodrošinātu interneta vietņu, uz kurām attiecas pamatlieta, labu funkcionēšanas spēju un vajadzības gadījumā dotu iespēju uzsākt kriminālizmeklēšanu saistībā ar pret tām vērstajiem kiberuzbrukumiem.

81. Tāpēc vispirms ir jānoskaidro, vai lūgumā sniegt prejudiciālu nolēmumu minēto IP adrešu apstrāde iekļauta Direktīvas 95/46 3. panta 2. punkta pirmajā ievilkumā paredzētajā izņēmumā [23].

1) Par Direktīvas 95/46 piemērojamību strīdīgo datu apstrādei

82. Pamattiesvedībā Vācijas Federatīvā Republika, šķiet, ir interneta pakalpojumu sniedzēja, proti, privātpersona (un tādējādi *sine imperio*). No šī apstākļa var secināt, ka šajā lietā aplūkotā datu apstrāde principā nav izslēgta no Direktīvas 95/46 piemērošanas jomas.

83. Saskaņā ar Tiesas apgalvoto spriedumā *Lindqvist* [24] Direktīvas 95/46 3. panta 2. punktā minētās darbības "katrā ziņā ir valsts vai valsts iestāžu pasākumi, kas neietilpst privātpersonu darbības lokā" [25]. Ciktāl apstrīdēto datu apstrādi veic kāds, kas, neraugoties uz savu valsts iestādes statusu, faktiski rīkojas kā privātpersona, ir piemērojama Direktīva 95/46.

84. Iesniedzējtiesa, norādot Vācijas valsts iestāžu galveno dinamisko IP adrešu ierakstīšanas mērķi, uzsver, ka tā esot nepieciešama "tās telekomunikāciju līdzekļu drošības un funkcionēšanas spējas nodrošināšanai"; it īpaši, lai veicinātu "bieži izplatīto "denial of service" [pakalpojuma atteikuma] uzbrukumu, kuru gadījumā telekomunikāciju infrastruktūra tiek bloķēta, mērķtiecīgi un koordinēti pārslogojot atsevišķus interneta serverus ar lielu skaitu pieprasījumu, atpazīšanu un apkarošanu" [26]. Parasti ikvienas nozīmīgas tīmekļa vietnes īpašnieki saglabā dinamiskās IP adreses šajā nolūkā, un tas ne tieši, ne netieši neietver valsts varas īstenošanu, tāpēc to iekļaušana Direktīvas 95/46 nerada pārmērīgas grūtības.

23 — Direktīvas 95/46 piemērošanas jomā neietilpst "apstrādes operācij[as] attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību [..] un [..] *valsts pasākumi krimināltiesību jomā*" (mans izcēlums).

24 — 2003. gada 6. novembra spriedums (C-101/01, EU:C:2003:596), 43. punkts.

25 — Šajā ziņā skat. 2008. gada 16. decembra spriedumu *Satakunnan Markkinapörssi* un *Satamedia* (C-73/07, EU:C:2008:727), 41. punkts.

26 — Lūguma sniegt prejudiciālu nolēmumu 36. punkts.

85. *Bundesgerichtshof* (Federālā Augstākā tiesa) tomēr apgalvo, ka pamatlietā iesaistītie pakalpojumu sniedzēji saglabā dinamiskās IP adreses arī tāpēc, lai vajadzības gadījumā uzsāktu krimināltiesisku vajāšanu pret iespējamiem kiberuzbrukumu veicējiem. Vai ar šo mērķi pietiek, lai šos datus izslēgtu no Direktīvas 95/46 piemērošanas jomas?

86. Manuprāt, ja "darbība krimināllietās" nozīmē valsts *ius puniendi* īstenošanu, ko veic pakalpojumu sniedzēji – atbildētāja pamatlietā, runa ir par "valsts pasākumiem krimināltiesību jomā" un tādējādi arī par vienu no Direktīvas 95/46 3. panta 2. punkta pirmajā ievilkumā paredzētajiem izņēmumiem.

87. Šajos apstākļos saskaņā ar Tiesas judikatūru, kas noteikta spriedumā *Huber*[27], pakalpojumu sniedzēju veiktā personas datu apstrāde telekomunikāciju pakalpojumu drošības un tehniskās funkcionēšanas jomā ir iekļauta Direktīvas 95/46 piemērošanas jomā, tai pašā laikā tā neattiecas uz datu apstrādi saistībā ar valsts darbību krimināltiesību jomā.

88. Tādējādi, lai arī darbība krimināllietās pati par sevi nav jāveic Vācijas Federatīvajai Republikai, kurai kā konkrētu pakalpojumu sniedzējai tam nav pilnvaru, bet kura tāpat kā jebkura privātpersona tikai pārsūta strīdīgās IP adreses valsts iestādei represīvu pasākumu veikšanai, dinamisko IP adrešu apstrādes mērķis var būt arī darbība, kas izslēgta no Direktīvas 95/46 piemērošanas jomas.

89. Tas izriet no judikatūras, kas noteikta lietā Parlaments/Padome un Komisija[28], kurā Tiesa ir apstiprinājusi, ka fakts, ka "privātie uzņēmēji ir apkopojuši [konkrētus] datus komercdarbības nolūkā un organizē to pārsūtīšanu uz trešajām valstīm", nenozīmē, ka "šāda pārsūtīšana neietilpst" Direktīvas 95/46 3. panta 2. punkta pirmā ievilkuma piemērošanas jomā, ja nosūtīšanas mērķis ir valsts darbība krimināllietās, ja šajā gadījumā tā "ietilpst valsts varas noteiktajos ietvaros un attiecas uz sabiedrisko drošību"[29].

90. Gluži pretēji, ja, kā es uzskatu, "darbība krimināllietās" nozīmē, kā tas secināms no lūguma sniegt prejudiciālu nolēmumu, privātpersonas, kurai ir tiesības lūgt valsts *ius puniendi* darbību, rīcību, tad par dinamisko IP adrešu apstrādes mērķi nav jāuzskata dalībvalsts pasākumi krimināllietās, kas izslēgti no Direktīvas 95/46 piemērošanas jomas.

91. Šo datu ierakstīšana un saglabāšana būtu vēl viens pierādījums, kuru tīmekļa vietnes īpašnieks pēc puses pieprasījuma sniegtu, lai lūgtu valstij prettiesiskas rīcības sodīšanu. Visbeidzot tas būtu privātpersonai tiesību sistēmā atzīto tiesību aizsardzība krimināltiesiskā ceļā (šajā gadījumā valsts iestāde rīkojas privāttiesību režīmā). No šī viedokļa tā neatšķiras no kāda cita interneta pakalpojuma sniedzēja iniciatīvas, kas lūdz valsts aizsardzību, izmantojot tiesību sistēmā paredzētos krimināltiesiskos līdzekļus.

92. Tādējādi, ciktāl Vācijas iestādes rīkojas kā Interneta pakalpojumu sniedzēja, nebūdama valsts varas statusā, kas ir jāizvērtē iesniedzējtiesai, dinamisko IP adrešu kā personas datu apstrāde ietilpst Direktīvas 95/46 piemērošanas jomā.

27 — 2008. gada 16. decembra spriedums (C-524/06, EU:C:2008:725), 45. punkts.

28 — 2006. gada 30. maija spriedums (C-317/04 un C-318/04, EU:C:2006:346), 54.–59. punkts.

29 — Turpat, 59. punkts. Tā attiecās uz personas datiem, kuru apstrāde nebija nepieciešama pakalpojumu sniegšanai, kas bija attiecīgo privāto uzņēmumu (aviokompānijas) darījumi, bet tie uzskatīja par savu pienākumu tos pārsūtīt Amerikas Savienoto Valstu iestādēm, lai novērstu un apkarotu terorismu.

2) Par lietas būtību

93. *TMG* 15. panta 1. punktā ir atļauts iegūt un izmantot lietotāja personas datus tikai tad, ja tas ir vajadzīgs, lai nodrošinātu telekomunikāciju pakalpojuma konkrētu izmantošanu un norēķinu par to. Precīzāk, pakalpojumu sniedzējs var iegūt un izmantot tikai tā saucamos "lietošanas datus", proti, lietotāja datus, kas ir vajadzīgi, lai padarītu par iespējamu "telekomunikāciju līdzekļu lietošanu un norēķinus par to". Šie dati ir jāizdzēš, kad lietošanas process ir beidzies (proti, kad beidzas telekomunikāciju pakalpojuma konkrēta lietošana), izņemot gadījumu, kad saskaņā ar *TMG* 15. panta 4. punktu tie ir jāsaglabā "norēķina nolūkā".

94. Kad pieslēgšanās internetam ir pabeigta, *TMG* 15. pantā, šķiet, nedrīkst saglabāt lietošanas datus citu iemeslu dēļ, ne arī vispārējai "telekomunikāciju pakalpojumu lietošanas" nodrošināšanai. Atsaucoties tikai uz norēķina mērķiem kā datu saglabāšanas attaisnojošu iemeslu, šo *TMG* tiesību normu varētu interpretēt (pat ja tās galīgā interpretācija ir jāsniedz iesniedzējtiesai) tādējādi, ka tajā ir noteikta prasība, ka lietošanas dati ir jāizmanto tikai ar mērķi padarīt iespējamas konkrētas attiecības, un tie ir jādzēš, kad tās ir beigušās.

95. Direktīvas 95/46 [30] 7. panta f) punktā ir atļauts apstrādāt personas datus daudz plašākā nozīmē (datu apstrādātājam), nekā tas ir paredzēts *TMG* 15. panta formulējumā. Šajā gadījumā var uzskatīt, ka Vācijas tiesību normā ir noteikti lielāki ierobežojumi nekā Savienības normā, jo tajā principā nav paredzētas citas likumīgās intereses, kas nebūtu saistītas ar norēķinu par pakalpojumu, tomēr Vācijas Federatīvajai Republikai kā interneta pakalpojumu sniedzējai arī varētu būt likumīgas intereses nodrošināt savu tīmekļa vietņu labu funkcionēšanas spēju, un nevis tikai ar lietošanu saistītas attiecības [31].

96. Tiesas judikatūrā, kas izriet no sprieduma *ASNEF* un *FECEMD* [32], ir noteiktas pamatnostādnes, lai atbildētu uz otro prejudiciālo jautājumu. Tādējādi Tiesa ir apgalvojusi, ka no Direktīvas 95/46 mērķa "izriet, ka Direktīvas 95/46 7. pants paredz plašu un pilnīgu tādu situāciju sarakstu, kurās var uzskatīt, ka ir notikusi likumīga personas datu apstrāde" [33]. No tā izriet, "ka dalībvalstis nedrīkst ne pievienot Direktīvas 95/46 7. pantam jaunus kritērijus, kas attiektos uz likumīgu personas datu apstrādi, ne arī paredzēt papildu prasības, kas mainītu kāda no šajā pantā ietverto sešu kritēriju piemērošanu" [34].

97. *TMG* 15. pantā nav minēta papildu prasība par datu apstrādes likumīgumu – kā tas bija lietās *ASNEF* un *FECEMD* – [35] līdzās tām, kas ir paredzētas Direktīvas 95/46 7. pantā, bet, ja tā tiek interpretēta šauri, uz ko norāda tiesa *a quo*, tiek ierobežots minētās tiesību normas f) punktā paredzētā nosacījuma saturs: tad, kad Savienības likumdevējs vispārīgi atsaucas uz "personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgo interešu" ievērošanu, *TMG* 15. pantā runa ir tikai par nepieciešamību "padarīt [par iespējamu] telekomunikāciju līdzekļu lietošanu un norēķinus par to".

98. Tāpat kā lietās *ASNEF* un *FECEMD* [36] arī šajā lietā valsts pasākums – atkārtošu, ja to interpretē šauri, kā tas tika izskaidrots iepriekš – mainītu Direktīvas 95/46 7. pantā noteiktā principa tvērumu, turklāt ir jāprecizē, ka tas ir vienīgais [jautājums], attiecībā uz kuru saskaņā ar Direktīvas 95/46 5. pantu katrai dalībvalstij ir zināma rīcības brīvība.

30 — Minēts 17. punktā.

31 — Skat. 84. punktu. Neapšaubāmi, tīmekļa vietņu īpašniekiem ir likumīgas intereses novērst iesniedzējtiesas minētos pakalpojuma atteikumus ("denials of service"), proti, bieži izplatītos uzbrukumus, kas dažreiz tiek veikti koordinēti pret dažām tīmekļa vietnēm, lai tās pārslogotu un padarītu darboties nespējīgas, un tos apkarotu.

32 — 2011. gada 24. novembra spriedums (C-468/10 un C-469/10, EU:C:2011:777)

33 — Turpat, 30. punkts.

34 — Turpat, 32. punkts.

35 — Gadījums, kurā valsts tiesību aktos Direktīvas 95/46 7. panta f) punktā paredzētajām prasībām tika pievienota prasība, ka apstrādātajiem datiem jābūt iekļautiem sabiedrībai pieejamos avotos.

36 — 2011. gada 24. novembra spriedums (C-468/04 un C-469/10, EU:C:2011:777).

99. Atbilstoši pēdējai minētajai tiesību normai "dalībvalstis saskaņā ar šīs nodaļas noteikumiem [37] precīzāk nosaka apstākļus, kādos personas datu apstrāde ir likumīga". Tomēr, kā ir apgalvots apvienotajās lietās *ASNEF* un *FECEMD*[38], "saskaņā ar [minēto noteikumu] dalībvalstis vairs nedrīkst noteikt papildu kritērijus personas datu apstrādes likumīgumam, kā tikai tos, kas ietverti šīs direktīvas 7. pantā, kā arī tās nedrīkst, nosakot papildu prasības, grozīt 7. pantā paredzētos sešus kritērijus".

100. *TMG* 15. pantā saistībā ar Direktīvas 95/46 7. panta f) punktu esot būtiski ierobežots to likumīgo interešu apjoms, kas attaisno datu apstrādi, necenšoties to precizēt vai niansēt saskaņā ar šīs pašas direktīvas 5. punktā atļauto. Turklāt tā to darot pilnīgi un absolūti, nepiekrītot, ka telekomunikāciju pakalpojuma vispārīgas lietošanas aizsardzība un garantēšana var tikt izsvērtas, "ņemot vērā datu subjekta pamattiesību un brīvību intereses, kurām nepieciešama aizsardzība saskaņā ar 1. panta 1. punktu", kā tas ir noteikts Direktīvas 95/46 7. panta f) punktā.

101. Visbeidzot tāpat kā apvienotajās lietās *ASNEF* un *FECEMD*[39] Vācijas likumdevējs esot noteicis, ka "ar valsts tiesisko regulējumu tiek izslēgta iespēja apstrādāt [atsevišķas personu datu kategorijas], attiecībā uz šīm kategorijām noteikti paredzot rezultātu, kas tiks sasniegts, izvērtējot tiesības un intereses, nepieļaujot savādāka rezultāta iespējamību, ņemot vērā atsevišķa gadījuma īpašos apstākļus", tādējādi, ka runa nav "par precizējumu [Direktīvas 95/46] 5. panta izpratnē".

102. Šādos apstākļos uzskatu, ka *Bundesgerichtshof* (Federālā Augstākā tiesa) valsts tiesību akti ir jāinterpretē saskaņā ar Direktīvu 95/46, kas nozīmē, ka a) var tikt noteikts kā viens no tā saukto "lietošanas datu" apstrādes attaisnojošiem iemesliem telekomunikāciju pakalpojumu sniedzēja likumīgās intereses, lai aizsargātu to vispārīgo lietošanu, un b) šīs pakalpojumu sniedzēja intereses var tikt izsvērtas *ad casum* ar lietotāja pamattiesībām un brīvībām, lai secinātu, kuras no tām ir jāaizsargā saskaņā ar Direktīvas 95/46 1. panta 1. punktu[40].

103. Manuprāt, tikai būtu jāpiebilst, ka šī izsvēršana ir jāveic arī gadījumā, par kuru ir iesniegts lūgums sniegt prejudiciālu nolēmumu. *Bundesgerichtshof* (Federālā Augstākā tiesa) neuzdod jautājumus par šo īpašo problēmu, to interesē tikai jautājums pirms šīs izsvēršanas veikšanas, proti, vai minētā izsvēršana var tikt veikta.

104. Visbeidzot, šķiet, ir lieki norādīt, ka tiesa *a quo* varētu ņemt vērā dalībvalsts, iespējams, pieņemtās tiesību normas saistībā ar Direktīvas 95/46 13. panta 1. punkta d) apakšpunktā ietverto atļauju, lai mazinātu šīs direktīvas 6. pantā paredzēto tiesību un pienākumu apjomu, kad būtu jānodrošina arī "kriminālsodāmu noziedzīgu nodarījumu [..] profilakse, izziņa, atklāšana un kriminālvajāšana". Iesniedzējtiesa, kas neapšaubāmi zina par šo abu pantu esamību, neatsaucas arī uz šo gadījumu.

105. Tādējādi uz otro prejudiciālo jautājumu ierosinu atbildēt tā, ka Direktīvas 95/46 7. panta f) punktam ir pretrunā valsts tiesību norma, kuras interpretācija liedz pakalpojumu sniedzējam iegūt un apstrādāt lietotāja datus bez viņa piekrišanas, lai nodrošinātu telekomunikāciju pakalpojumu funkcionēšanas spēju pēc katras lietošanas darbības beigām.

37 — Direktīvas 95/46 II nodaļa "Vispārīgi noteikumi par personas datu apstrādes likumību", kurā iekļauts Direktīvas 95/46 5.–21. pants.

38 — 2011. gada 24. novembra spriedums (C-468/04 un C-469/10, EU:C:2011:777), 36. punkts.

39 — Turpat, 47. punkts.

40 — Tiesas sēdē *P. Breyer* advokāts noraidīja to, ka dinamiskā IP adrešu ierakstīšana esot nepieciešama, lai interneta pakalpojumu labu funkcionēšanas spēju pasargātu no iespējamiem uzbrukumiem. Es neuzskatu, ka var sniegt absolūtu atbildi saistībā ar šo problēmu, kuras atrisināšanai katrā konkrētajā gadījumā vispirms ir jāizsver tīmekļa vietnes īpašnieka intereses un lietotāju intereses.

VI – Secinājumi

106. Ņemot vērā iepriekš izklāstīto, es ierosinu Tiesai uz uzdotajiem prejudiciālajiem jautājumiem atbildēt šādi:

1) saskaņā ar Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti 2. panta a) punktu dinamiskā IP adrese, ar kuru lietotājs ir piekļuvis telekomunikāciju pakalpojumu sniedzēja tīmekļa vietnei, attiecībā uz šo pakalpojumu sniedzēju ir "personas dati", ciktāl interneta piekļuves nodrošinātāja rīcībā ir citi papildu dati, kas kopā ar dinamisko IP adresi palīdz identificēt lietotāju;

2) Direktīvas 95/46 7. panta f) punkts ir jāinterpretē tādējādi, ka mērķis nodrošināt telekomunikāciju pakalpojuma funkcionēšanas spēju principā var tikt uzskatīts par likumīgu interesi, kuras īstenošana pamato šo personas datu apstrādi, tomēr attiecībā uz to ir jāveic izsvēršana, vai tā ir pārāka pār datu subjekta pamattiesībām un brīvībām. Valsts tiesību norma, saskaņā ar kuru nav atļauts ņemt vērā šīs likumīgās intereses, būtu nesaderīga ar minēto pantu.