TIESAS SPRIEDUMS (otrā palāta)

2016. gada 19. oktobrī*

Lūgums sniegt prejudiciālu nolēmumu — Personas datu apstrāde — Direktīva 95/46/EK — 2. panta a) punkts — 7. panta f) punkts — Jēdziens "personas dati" — Interneta protokola adrese — Saglabāšana, ko veic tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs — Valsts tiesiskais regulējums, kas liedz ņemt vērā datu apstrādātāja likumīgās intereses

Lieta C-582/14

par lūgumu sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *Bundesgerichtshof* (Federālā Augstākā tiesa, Vācija) iesniedza ar lēmumu, kas pieņemts 2014. gada 28. oktobrī un kas Tiesā reģistrēts 2014. gada 17. decembrī, tiesvedībā

Patrick Breyer

pret

Vācijas Federatīvo Republiku.

TIESA (otrā palāta)

šādā sastāvā: palātas priekšsēdētājs M. Ilešičs [*M. Ilešič*], tiesneši A. Prehala [*A. Prechal*], A. Ross [*A. Rosas*] (referents), K. Toadere [*C. Toader*] un E. Jarašūns [*E. Jarašiūnas*],

ģenerāladvokāts M. Kamposs Sančess-Bordona [*M. Campos Sánchez-Bordona*],

sekretāre V. Džakobo-Peironnela [*V. Giacobbo-Peyronnel*], administratore,

ņemot vērā rakstveida procesu un 2016. gada 25. februāra tiesas sēdi,

ņemot vērā apsvērumus, ko sniedza:

— *P. Breyer* vārdā – *M. Starostik*, *Rechtsanwalt*,

— Vācijas valdības vārdā – *A. Lippstreu* un *T. Henze*, pārstāvji,

— Austrijas valdības vārdā – *G. Eberhard*, pārstāvis,

— Portugāles valdības vārdā – *L. Inez Fernandes* un *C. Vieira Guerra*, pārstāvji,

— Eiropas Komisijas vārdā – *P. J. O. Van Nuffel* un *H. Krämer*, kā arī *P. Costa de Oliveira* un *J. Vondung*, pārstāvji,

* Tiesvedības valoda – vācu.

noklausījusies ģenerāladvokāta secinājumus 2016. gada 12. maija tiesas sēdē,

pasludina šo spriedumu.

Spriedums

1 Lūgums sniegt prejudiciālu nolēmumu ir par to, kā interpretēt 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 (OV 1995, L 281, 31. lpp.) 2. panta a) punktu un 7. panta f) punktu.

2 Šis lūgums tika iesniegts tiesvedībā starp *Patrick Breyer* un *Bundesrepublik Deutschland* (Vācijas Federatīvā Republika) jautājumā par pēdējās minētās veikto *P. Breyer* interneta protokola adreses (turpmāk tekstā – "IP adrese") ierakstīšanu un saglabāšanu, viņam aplūkojot vairākas Vācijas federālo dienestu interneta vietnes.

Atbilstošās tiesību normas

Savienības tiesības

3 Direktīvas 95/46 preambulas 26. apsvērums ir izteikts šādā redakcijā:

"tā kā aizsardzības principi 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".

4 Saskaņā ar minētās direktīvas 1. panta formulējumu:

"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."

5 Šīs pašas direktīvas 2. pantā ir paredzēts:

"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;

[..].”

6 Direktīvas 95/46 3. pantā “Darbības joma” ir paredzēts:

“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;

[..].”

7 Minētās direktīvas 5. pantā ir noteikts:

“Dalībvalstis saskaņā ar šīs nodaļas noteikumiem precīzāk nosaka apstākļus, kādos personas datu apstrāde ir likumīga.”

8 Šīs pašas direktīvas 7. pants ir izteikts šādā redakcijā:

“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 juridiskās 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."

9 Direktīvas 95/46 13. panta 1. punktā ir noteikts:

"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:

[..]

d) krimināls odāmu noziedzīgu nodarījumu vai reglamentētu profesiju ētikas pārkāpumu profilaksei, izziņai, atklāšanai un krimināl vajāšanai;

[..]."

Vācijas tiesību akti

10 2007. gada 26. februāra *Telemediengesetz* (Tiešsaistes plašsaziņas līdzekļu likums) (*BGBl.* 2007 I, 179. lpp.; turpmāk tekstā – "*TMG*") 12. pantā ir noteikts:

"1) Tiešsaistes plašsaziņas 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 tiešsaistes plašsaziņas līdzekļiem, vai ja lietotājs ir devis savu piekrišanu.

2) Tiešsaistes plašsaziņas 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 tiešsaistes plašsaziņas līdzekļiem, vai ja lietotājs ir devis savu piekrišanu.

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

11 *TMG* 15. pantā ir paredzēts:

"1) Lietotāja personas datus pakalpojumu sniedzējs drīkst iegūt un izmantot tikai tad, ja tas ir nepieciešams, lai padarītu iespējamu tiešsaistes plašsaziņas 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;

3. dati par lietotāja izmantotiem tiešsaistes plašsaziņas līdzekļiem.

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

[..]

4) Pakalpojumu sniedzējs drīkst izmantot lietošanas datus pēc lietošanas procesa beigām, ciktāl tas ir nepieciešams norēķinu ar lietotāju par sniegtajiem pakalpojumiem vajadzībām (norēķinu dati). Pakalpojumu sniedzējs drīkst bloķēt datus, lai ievērotu likumiskus, statūtu vai līgumiskus uzglabāšanas termiņus. [..]"

12 Saskaņā ar 1990. gada 20. decembra *Bundesdatenschutzgesetz* (Federālais datu aizsardzības likums) (*BGBl*. 1990 I, 2954. lpp.) 3. panta 1. punktu "personas dati ir konkrētas norādes par identificētas vai identificējamas fiziskas personas (datu subjekts) personīgo vai materiālo stāvokli [..]".

Pamatlieta un prejudiciālie jautājumi

13 *P. Breyer* aplūkoja vairākas Vācijas federālo dienestu interneta vietnes. Šajās sabiedrībai pieejamajās vietnēs minētie dienesti sniedz aktualizētu informāciju.

14 Lai novērstu uzbrukumus un darītu iespējamu krimināltiesiskas vajāšanas uzsākšanu pret "uzbrucējiem", šajās vietnēs lielākoties visi piekļuves gadījumi tiek saglabāti protokola datos. Tajos – arī pēc minēto vietņu aplūkošanas – tiek saglabāts aplūkotās datnes vai tīmekļa vietnes nosaukums, meklētāja laukā ievadītie jēdzieni, piekļuves datums un laiks, pārraidīto datu apjoms, ziņojums, vai piekļuve ir bijusi veiksmīga, un datora, no kura ir veikta piekļuve, IP adrese.

15 IP adreses ir ciparu secības, kas tiek piešķirtas ar internetu savienotiem datoriem, lai padarītu iespējamu to savstarpējo komunikāciju, izmantojot šo tīklu. Piekļūšanas interneta vietnei gadījumā datora, kas nosūta piekļuves pieprasījumu, IP adrese tiek nosūtīta uz serveri, kurā ir saglabāta vietne, kurai tiek piekļūts. Šī nosūtīšana ir vajadzīga, lai nosūtītu pieprasītos datus pareizajam saņēmējam.

16 Turklāt no lūguma sniegt prejudiciālu nolēmumu un Tiesas rīcībā esošajiem lietas materiāliem izriet, ka interneta piekļuves pakalpojumu sniedzēji interneta lietotāju datoriem piešķir vai nu "statisku" IP adresi, vai "dinamisku" IP adresi, tas ir, IP adresi, kas mainās līdz ar katru jaunu savienojumu ar internetu. Atšķirībā no statiskajām IP adresēm, dinamiskās IP adreses nedod iespēju noteikt saikni, izmantojot sabiedrībai pieejamas datnes, starp konkrētu datoru un interneta piekļuves pakalpojumu sniedzēja izmantotu fizisku pieslēgumu tīklam.

17 *P. Breyer* cēla Vācijas administratīvajās tiesās prasību par to, lai Vācijas Federatīvajai Republikai tiktu aizliegts pēc katras Vācijas federālo dienestu tiešsaistes plašsaziņas līdzekļu publiski pieejamu vietņu aplūkošanas saglabāt vai likt trešajām personām saglabāt *P. Breyer* saimniekdatora, no kura tiek veikta piekļuve, IP adresi, jo šī saglabāšana neesot vajadzīga šo elektronisko plašsaziņas līdzekļu izplatīšanas atjaunošanai traucējuma gadījumā.

18 Tā kā *P. Breyer* prasība pirmajā instancē tika noraidīta, viņš par noraidošo spriedumu iesniedza apelācijas sūdzību.

19 Apelācijas instance daļēji grozīja šo spriedumu. Tā piesprieda Vācijas Federatīvajai Republikai pārtraukt ilgāk par attiecīgu [vietnes] aplūkošanas laiku ierakstīt vai likt trešajām personām ierakstīt *P. Breyer* saimniekdatora, no kura tiek veikta piekļuve, IP adresi, kas tiek pārraidīta saistībā ar viņa veiktu Vācijas federālo dienestu tiešsaistes plašsaziņas līdzekļu publiski pieejamu vietņu aplūkošanu, ja šī adrese ir saglabāta kopā ar vietnes aplūkošanas reizes, uz kuru attiecas šī adrese, datumu un ja *P. Breyer* šajā vietnes aplūkošanas reizē ir atklājis savu identitāti, tostarp elektroniskās adreses, kurā ir minēta viņa identitāte, formā, ja vien šī saglabāšana nav vajadzīga tiešsaistes plašsaziņas līdzekļu izplatīšanas atjaunošanai traucējuma gadījumā.

20 Šī apelācijas instance uzskatīja, ka dinamiskā IP adrese kopā ar vietnes aplūkošanas reizes, uz kuru attiecas šī adrese, datumu, ja interneta vietnes lietotājs šajā procesā ir atklājis savu identitāti, ir personas dati, jo šīs vietnes operators var identificēt šo lietotāju, savienojot viņa vārdu ar viņa datora IP adresi.

21 Minētā apelācijas instance nolēma, ka *P. Breyer* prasība attiecībā uz citām iespējamām situācijām tomēr nav jāapmierina. Gadījumā, ja *P. Breyer* vietnes aplūkošanas reizē neatklāj savu identitāti, vienīgi interneta piekļuves pakalpojumu sniedzējs varot saistīt IP adresi ar identificētu abonentu. Turpretim tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējas statusā esošās Vācijas Federatīvās Republikas rīcībā IP adrese pat kopā ar vietnes aplūkošanas reizes, uz kuru attiecas šī adrese, datumu neesot personas dati, jo šī dalībvalsts nevarot identificēt attiecīgo interneta vietņu lietotāju.

22 Gan *P. Breyer*, gan arī Vācijas Federatīvā Republika par apelācijas instances spriedumu iesniedza sūdzību "Revision" kārtībā *Bundesgerichtshof* (Federālā Augstākā tiesa, Vācija). *P. Breyer* lūdz, lai viņa aizlieguma prasījums tiktu apmierināts pilnībā. Vācijas Federatīvā Republika lūdz šo prasījumu noraidīt.

23 Iesniedzējtiesa precizē, ka *P. Breyer* datora dinamiskās IP adreses, ko saglabā Vācijas Federatīvā Republika, kura rīkojas kā tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēja, vismaz citu protokola datos saglabāto datu kontekstā esot konkrēti dati par ar *P. Breyer* saistītām situācijām, jo tie sniedzot norādes par to, ka viņš noteiktos datumos internetā ir aplūkojis noteiktas vietnes vai datnes.

24 Tomēr šādi saglabātie dati neļaujot tieši noteikt *P. Breyer* identitāti. Pamatlietā aplūkojamie interneta vietņu pārvaldītāji *P. Breyer* varot identificēt tikai tad, ja viņa interneta piekļuves pakalpojumu sniedzējs tiem nodotu informāciju par šī lietotāja identitāti. Šo datu kvalificēšana par "personas" datiem tātad esot atkarīga no tā, vai *P. Breyer* ir identificējams.

25 *Bundesgerichtshof* (Federālā Augstākā tiesa) norāda uz doktrinālo domstarpību par jautājumu, vai, lai noteiktu, vai persona ir identificējama, ir jāpamatojas uz "objektīvo" vai "relatīvo" kritēriju. "Objektīvā" kritērija piemērošanas rezultātā tādi dati kā pamatlietā aplūkojamās IP adreses pēc attiecīgo interneta vietņu apskatīšanas beigām varot tikt uzskatīti par tādiem, kuriem ir personas datu raksturs, lai gan attiecīgās personas identitāti var noteikt vienīgi trešā persona, kas šajā gadījumā ir *P. Breyer* interneta piekļuves pakalpojumu sniedzējs, kura ir saglabājusi papildu datus, kas ļauj identificēt *P. Breyer* ar minēto IP adrešu palīdzību. Saskaņā ar "relatīvo" kritēriju šādi dati varot tikt uzskatīti par personas datiem saistībā ar noteiktu struktūru, tādu kā *P. Breyer* interneta piekļuves pakalpojumu sniedzējs, jo tie ļauj veikt precīzu lietotāja identifikāciju (šajā ziņā skat. spriedumu, 2011. gada 24. novembris, *Scarlet Extended*, C-70/10, EU:C:2011:771, 51. punkts), tomēr saistībā ar citu struktūru, tādu kā *P. Breyer* aplūkoto interneta vietņu pārvaldītājs, tiem nebūtu personas datu rakstura, jo šim pārvaldītājam, neveicot nesamērīgus centienus, nebūtu viņa identificēšanai nepieciešamās informācijas, ja vien šo interneta vietņu aplūkošanas procesā *P. Breyer* nav atklājis savu identitāti.

26 Gadījumā, ja *P. Breyer* datora dinamiskās IP adreses kopā ar vietnes aplūkošanas reizes, uz kuru šīs adreses attiecas, datumu būtu uzskatāmas par personas datiem, iesniedzējtiesa vēlas noskaidrot, vai šo IP adrešu saglabāšana pēc šīs vietnes aplūkošanas reizes atbilstoši šīs direktīvas 7. panta f) punktam ir atļauta.

27 Šajā ziņā *Bundesgerichtshof* (Federālā Augstākā tiesa) precizē, pirmkārt, ka saskaņā ar TMG 15. panta 1. punktu tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēji lietotāja personas datus drīkst iegūt un izmantot tikai tiktāl, ciktāl tas ir nepieciešams, lai nodrošinātu šo plašsaziņas līdzekļu lietošanu un norēķinus par to. Otrkārt, iesniedzējtiesa norāda, ka saskaņā ar Vācijas Federatīvās Republikas viedokli minēto datu saglabāšana esot nepieciešama, lai nodrošinātu tiešsaistes plašsaziņas līdzekļu pakalpojumu interneta vietņu, ko tā padara pieejamas sabiedrībai, drošību un nepārtrauktu labu funkcionēšanu, it īpaši ļaujot atpazīt tādus datoruzbrukumus kā "pakalpojuma atteikuma uzbrukumi", kas ir vērsti uz šo vietņu darbības paralizēšanu, mērķtiecīgi un koordinēti pārplūdinot noteiktus interneta serverus ar lielu pieprasījumu skaitu, un apkarot šos uzbrukumus.

28 Iesniedzējtiesa uzskata, ka, ja un ciktāl ir nepieciešams, ka tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs veic pasākumus, lai apkarotu šādus uzbrukumus, šie pasākumi varot tikt uzskatīti par nepieciešamiem, lai "padarītu [iespējamu] elektronisko plašsaziņas līdzekļu lietošanu" *TMG* 15. panta

izpratnē. Tomēr doktrīnā pārsvarā esot pārstāvēts viedoklis, ka, pirmkārt, interneta vietnes lietotāja personas datu iegūšana un izmantošana ir atļauta tikai tam, lai padarītu iespējamu šīs vietnes konkrētu lietošanu, un, otrkārt, šie dati, ja tie nav vajadzīgi norēķinu vajadzībām, ir jāizdzēš līdz ar attiecīgās vietnes aplūkošanas reizes beigām. Tomēr šī *TMG* 15. panta 1. punkta ierobežojošā izpratne neļautu veikt IP adrešu saglabāšanu, lai vispārīgi nodrošinātu tiešsaistes plašsaziņas līdzekļu drošību un nepārtrauktu labu funkcionēšanu.

29 Iesniedzējtiesai rodas jautājums, vai šī pēdējā minētā interpretācija, kas ir interpretācija, kuru atbalsta apelācijas instance, atbilst Direktīvas 95/46 7. panta f) punktam, ievērojot tostarp Tiesas 2011. gada 24. novembra sprieduma *ASNEF* un *FECEMD* (C-468/10 un C-469/10, EU:C:2011:777) 29. un nākamajos punktos izklāstītos kritērijus,

30 Šādos apstākļos *Bundesgerichtshof* (Federālā Augstākā tiesa) nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

"1) Vai Direktīvas 95/46 2. panta a) punkts ir jāinterpretē tādējādi, ka IP adrese, ko [tiešsaistes plašsaziņas līdzekļu] 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 [šīs direktīvas] 7. panta f) punktu netiek pieļauta valsts tiesību norma, atbilstoši kurai [tiešsaistes plašsaziņas līdzekļu] pakalpojumu sniedzējs lietotāja personas datus bez viņa piekrišanas var iegūt un izmantot tikai tad, kad tas ir nepieciešams, lai nodrošinātu tiešsaistes plašsaziņas līdzekļa konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un atbilstoši kurai mērķis nodrošināt vispārēju tiešsaistes plašsaziņas līdzekļa funkcionēšanas spēju nevar attaisnot izmantošanu pēc attiecīgā lietošanas procesa beigām?"

Par prejudiciālajiem jautājumiem

Par pirmo jautājumu

31 Ar savu pirmo jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai Direktīvas 95/46 2. panta a) punkts ir jāinterpretē tādējādi, ka dinamiskā IP adrese, ko tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs ieraksta saistībā ar personas piekļuvi šī pakalpojumu sniedzēja publiskai lietošanai paredzētai interneta vietnei, attiecībā uz šo pakalpojumu sniedzēju ir uzskatāma par personas datiem šīs tiesību normas izpratnē, ja vienīgi trešajai personai, kas šajā gadījumā ir minētās personas interneta piekļuves pakalpojumu sniedzējs, ir tās identificēšanai nepieciešamā papildinformācija?

32 Atbilstoši minētās tiesību normas redakcijai "personas dati" ir "jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu ("datu subjektu")". Šajā tiesību normā ir noteikts, ka 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.

33 Vispirms ir jānorāda, ka 2011. gada 24. novembra sprieduma *Scarlet Extended* (C-70/10, EU:C:2011:771) 51. punktā, kas attiecas tostarp uz tās pašas direktīvas interpretāciju, Tiesa būtībā ir uzskatījusi, ka interneta lietotāju IP adreses ir aizsargāti personas dati, jo tie ļauj precīzi identificēt minētos lietotājus.

34 Tomēr šis Tiesas apgalvojums bija saistīts ar situāciju, kad interneta lietotāju IP adrešu iegūšanu un identificēšanu veica interneta piekļuves pakalpojumu sniedzēji.

35 Taču šajā lietā pirmais jautājums attiecas uz situāciju, kurā tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēja, tas ir, Vācijas Federatīvā Republika, reģistrē tās interneta vietnes lietotāju IP adreses, kuru šī pakalpojumu sniedzēja ir padarījusi pieejamu sabiedrībai, un tās rīcībā nav šo lietotāju identificēšanai vajadzīgās papildu informācijas.

36 Turklāt nav strīda par to, ka IP adreses, uz kurām atsaucas iesniedzējtiesa, ir "dinamiskas", tas ir, tās pagaidu adreses, kas tiek piešķirtas līdz ar katru savienojumu ar internetu un aizstātas līdz ar vēlākiem savienojumiem, nevis "statiskas" IP adreses, kas ir nemainīgas un ļauj pastāvīgi identificēt tīklam pievienotu ierīci.

37 Tātad pirmais iesniedzējtiesas uzdotais jautājums ir balstīts uz pieņēmumu, saskaņā ar kuru, pirmkārt, dati, ko veido dinamiskā IP adrese, kā arī interneta vietnes aplūkošanas no šīs IP adreses reizes datums un laiks, ko ir ierakstījis tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs, paši par sevi nedod šim pakalpojumu sniedzējam iespēju identificēt lietotāju, kas lietošanas reizē ir aplūkojis šo interneta vietni, un, otrkārt, interneta piekļuves pakalpojumu sniedzējam savukārt ir papildu informācija, kura, ja tā tiktu savienota ar šo IP adresi, ļautu identificēt minēto lietotāju.

38 Šajā ziņā vispirms ir jānorāda, ka nav strīda par to, ka dinamiskā IP adrese nav informācija, kas attiecas uz "identificētu fizisku personu", jo šāda adrese tieši neatklāj nedz fiziskās personas – datora, no kura ir notikusi interneta vietnes aplūkošana, īpašnieces – identitāti, nedz citas personas, kas varētu izmantot šo datoru, identitāti.

39 Turpmāk, lai noskaidrotu, vai šī sprieduma 37. punktā norādītajos apstākļos dinamiskā IP adrese attiecībā uz tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēju ir personas dati Direktīvas 95/46 2. panta a) punkta izpratnē, ir jāpārbauda, vai šī IP adrese, ko ieraksta šāds pakalpojumu sniedzējs, var tikt kvalificēta kā informācija, kas attiecas uz "identificējamu fizisku personu", ja papildu informācija, kas ir vajadzīga, lai identificētu interneta vietnes, ko šis pakalpojumu sniedzējs padara pieejamu sabiedrībai, lietotāju, ir šī lietotāja interneta piekļuves pakalpojumu sniedzēja rīcībā.

40 Šajā ziņā no Direktīvas 95/46 2. panta a) punkta formulējuma izriet, ka par identificējamu ir uzskatāma persona, kura var tikt identificēta ne vien tieši, bet arī netieši.

41 Tas, ka Savienības likumdevējs ir izmantojis vārdu "netieši", liecina par to, ka, lai kvalificētu informāciju par tādu, kas ir uzskatāma par personas datiem, nav vajadzīgs, lai šī informācija pati par sevi ļautu identificēt attiecīgo personu.

42 Turklāt Direktīvas 95/46 preambulas 26. apsvērumā ir noteikts, ka, lai noteiktu, vai persona ir identificējama, ir jāņem vērā visi līdzekļi, kurus var saprātīgi izmantot vai nu personas datu apstrādātājs, vai jebkura cita persona, lai identificētu minēto personu.

43 Ņemot vērā, ka šajā apsvērumā ir paredzēta atsauce uz līdzekļiem, ko var saprātīgi izmantot gan personas datu apstrādātājs, gan arī "cita persona", tā formulējums norāda uz to, ka, lai datus varētu kvalificēt kā "personas datus" minētās direktīvas 2. panta a) punkta izpratnē, netiek prasīts, lai visa informācija, kas ļauj identificēt attiecīgo personu, atrastos tikai vienas personas rīcībā.

44 Tātad ar to, ka papildu informācija, kas ir vajadzīga, lai identificētu interneta vietnes lietotāju, ir nevis tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēja, bet šī lietotāja interneta piekļuves pakalpojumu sniedzēja rīcībā, nevar izslēgt, ka tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēja ierakstītās dinamiskās IP adreses attiecībā uz to ir personas dati Direktīvas 95/46 2. panta a) punkta izpratnē.

45 Tomēr ir jānosaka, vai iespēja savienot dinamisko IP adresi ar minēto papildu informāciju, kura ir šī interneta piekļuves pakalpojumu sniedzēja rīcībā, ir līdzeklis, kas saprātīgi var tikt izmantots, lai identificētu attiecīgo personu.

46 Kā ģenerāladvokāts būtībā ir norādījis savu secinājumu 68. punktā, tas tā nebūtu, ja attiecīgās personas identifikācija būtu aizliegta ar tiesību aktiem vai praktiski neīstenojama, piemēram, tādēļ, ka tā nozīmētu nesamērīgu piepūli laika, izmaksu un darbaspēka ziņā, kā rezultātā identifikācijas risks patiesībā būtu nenozīmīgs.

47 Lai gan iesniedzējtiesa savā lūgumā sniegt prejudiciālu nolēmumu norāda, ka Vācijas tiesībās interneta piekļuves pakalpojumu sniedzējam esot aizliegts tieši nodot tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējam papildu informāciju, kas ir nepieciešama, lai identificētu attiecīgo personu, tomēr, neskarot šīs tiesas šajā ziņā veicamo pārbaudi, ir jākonstatē, ka ir tiesiskās iespējas, kas tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējam, piemēram, kiberuzbrukumu gadījumā, ļauj vērsties pie kompetentās iestādes, lai tā veiktu nepieciešamos pasākumus, lai iegūtu šo informāciju no interneta piekļuves pakalpojumu sniedzēja, un uzsāktu kriminālvajāšanu.

48 Tātad ir jākonstatē, ka tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējam ir līdzekļi, kas saprātīgi var tikt izmantoti, lai, pamatojoties uz saglabātām IP adresēm, ar citu personu, proti, kompetentas iestādes un interneta piekļuves pakalpojumu sniedzēja, palīdzību identificētu attiecīgo personu.

49 Ņemot vērā iepriekš norādītos apsvērumus, uz pirmo jautājumu ir jāatbild, ka Direktīvas 95/46 2. panta a) punkts ir jāinterpretē tādējādi, ka dinamiskā IP adrese, ko tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs ieraksta saistībā ar personas piekļuvi šī pakalpojumu sniedzēja publiskai lietošanai paredzētai interneta vietnei, attiecībā uz minēto pakalpojumu sniedzēju ir uzskatāma par personas datiem šīs tiesību normas izpratnē, ja tā rīcībā ir tiesiski līdzekļi, kas tam ļauj likt identificēt attiecīgo personu, izmantojot šīs personas interneta piekļuves pakalpojumu sniedzēja rīcībā esošo papildu informāciju.

Par otro jautājumu

50 Ar savu otro jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai Direktīvas 95/46 7. panta f) punkts ir jāinterpretē tādējādi, ka ar to netiek pieļauts dalībvalsts regulējums, atbilstoši kuram tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs šo pakalpojumu lietotāja personas datus bez viņa piekrišanas var iegūt un izmantot tikai tad, ja šī iegūšana un izmantošana ir nepieciešama, lai nodrošinātu minēto pakalpojumu konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un mērķis nodrošināt minēto pakalpojumu vispārēju funkcionēšanas spēju nevar attaisnot minēto datu izmantošanu pēc konkrēta pakalpojumu izmantošanas procesa beigām.

51 Pirms atbildes uz šo jautājumu sniegšanas ir jānosaka, vai pamatlietā aplūkojamā personas datu, tas ir, noteiktu Vācijas federālajiem dienestiem piederošu interneta vietņu lietotāju dinamisko IP adrešu, apstrāde nav izslēgta no Direktīvas 95/46 piemērošanas jomas, piemērojot tās 3. panta 2. punkta pirmo ievilkumu, saskaņā ar kuru minētā direktīva neattiecas uz personas datu apstrādi, kuras priekšmets tostarp ir valsts pasākumi krimināltiesību jomā.

52 Šajā ziņā ir jāatgādina, ka darbības, kuras kā piemēri ir norādītas šajā tiesību normā, katrā ziņā ir valsts vai valsts iestāžu darbības, kas neietilpst privātpersonu darbības lokā (skat. spriedumus, 2003. gada 6. novembris, *Lindqvist*, C-101/01, EU:C:2003:596, 43. punkts, un 2008. gada 16. decembris, *Satakunnan Markkinapörssi* un *Satamedia*, C-73/07, EU:C:2008:727, 41. punkts).

53 Pamatlietā, neskarot iesniedzējtiesas šajā ziņā veicamo pārbaudi, ir jāsecina, ka Vācijas federālie dienesti, kas sniedz tiešsaistes plašsaziņas līdzekļu pakalpojumus un kas ir atbildīgi par dinamisko IP adrešu apstrādi, rīkojas, neraugoties uz to publisko iestāžu statusu, kā privātpersonas un ārpus valsts pasākumu krimināltiesību jomā konteksta.

54 Tādējādi ir jānosaka, vai tāds dalībvalsts regulējums, kāds tiek aplūkots pamatlietā, ir saderīgs ar Direktīvas 95/46 7. panta f) punktu.

55 Šajā ziņā ir jāatgādina, ka saskaņā ar pamatlietā aplūkojamo dalībvalsts regulējumu, piemērojot tam iesniedzējtiesas izteikto ierobežoto interpretāciju, minēto pakalpojumu lietotāja personas datu iegūšanu un izmantošanu bez viņa piekrišanas var veikt tikai tad, ja tas ir nepieciešams, lai nodrošinātu tiešsaistes plašsaziņas līdzekļu konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un mērķis nodrošināt tiešsaistes plašsaziņas līdzekļu vispārēju funkcionēšanas spēju nevar attaisnot minēto datu izmantošanu pēc konkrēta pakalpojumu izmantošanas procesa beigām.

56 Saskaņā ar Direktīvas 95/46 7. panta f) punktu personas datu apstrāde ir likumīga, ja apstrāde ir "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 [šīs direktīvas] 1. panta 1. punktu".

57 Ir jāatgādina, ka Tiesa ir nospriedusi, ka minētās direktīvas 7. pantā ir paredzēts izsmeļošs un ierobežojošs tādu situāciju saraksts, kurās personas datu apstrādi var uzskatīt par likumīgu, un ka dalībvalstis nedrīkst ne pievienot minētajam pantam jaunus principus, kas attiektos uz personas datu apstrādes likumību, ne arī paredzēt papildu prasības, kas grozītu kāda no šajā pantā ietvertajiem sešiem principiem piemērošanas jomu (šajā ziņā skat. spriedumu, 2011. gada 24. novembris, *ASNEF* un *FECEMD*, C-468/10 un C-469/10, EU:C:2011:777, 30. un 32. punkts).

58 Lai gan ar Direktīvas 95/46 5. pantu dalībvalstīm ir dotas pilnvaras, ievērojot šīs direktīvas II nodaļas un tātad tās 7. panta ierobežojumus, precizēt nosacījumus, ar kādiem personas datu apstrāde ir likumīga, rīcības brīvība, kāda dalībvalstīm ir saskaņā ar minēto 5. pantu, var tikt izmantota tikai saskaņā ar minētās direktīvas izvirzīto mērķi, proti, saglabāt līdzsvaru starp personas datu brīvu apriti un privātās dzīves aizsardzību. Saskaņā ar šīs direktīvas 5. panta noteikumiem dalībvalstis drīkst noteikt tikai tos papildu principus attiecībā uz personas datu apstrādes likumību, kas ietverti šīs direktīvas 7. pantā, kā arī tās nedrīkst, nosakot papildu prasības, grozīt minētajā 7. pantā paredzēto sešu principu piemērošanas jomu (šajā ziņā skat. spriedumu, 2011. gada 24. novembris, *ASNEF* un *FECEMD*, C-468/10 un C-469/10, EU:C:2011:777, 30., 34. un 36. punkts).

59 Šajā lietā ir jākonstatē, ka *TMG* 15. panta, ja tas tiktu interpretēts šauri šī sprieduma 55. punktā minētajā veidā, piemērošanas joma būtu ierobežotāka nekā Direktīvas 95/46 7. panta f) punktā paredzētā principa piemērošanas joma.

60 Lai gan minētās direktīvas 7. panta f) punktā ir ietverta vispārīga atsauce uz "personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgo interešu ievērošan[u]", ar *TMG* 15. pantu pakalpojumu sniedzējam būtu tiesības iegūt un izmantot lietotāja personas datus tikai tiktāl, ciktāl tas ir nepieciešams, lai nodrošinātu telekomunikāciju līdzekļu konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus. Tādējādi ar *TMG* 15. pantu vispārīgi ir aizliegta personas datu saglabāšana pēc piekļuves tiešsaistes plašsaziņas līdzekļiem beigām, lai nodrošinātu šo plašsaziņas līdzekļu izmantošanu. Taču Vācijas federālajiem dienestiem, kas sniedz tiešsaistes plašsaziņas līdzekļu pakalpojumus, varētu būt likumīgas intereses arī nodrošināt savu sabiedrībai pieejamo interneta vietņu funkcionēšanas turpinātību pēc katras minēto vietņu konkrētas izmantošanas.

61 Kā ģenerāladvokāts ir norādījis savu secinājumu 100. un 101. punktā, šāds valsts regulējums neaprobežojas ar to, lai saskaņā ar Direktīvas 95/46 5. pantu precizētu šīs direktīvas 7. panta f) punktā minēto jēdzienu "likumīgās intereses".

62 Šajā ziņā tāpat ir jāatgādina, ka ar minētās direktīvas 7. panta f) punktu netiek pieļauts, ka dalībvalsts kategoriski un vispārīgi izslēdz iespēju apstrādāt atsevišķas personu datu kategorijas, neļaujot veikt konkrētajā gadījumā iesaistītu pretstatītu tiesību un interešu izsvēršanu. Dalībvalsts tātad nedrīkst attiecībā uz šīm kategorijām galīgi paredzēt pretstatītu tiesību un interešu izsvēršanas rezultātu, nepieļaujot citu iznākumu atsevišķa gadījuma īpašu apstākļu dēļ (šajā ziņā skat. spriedumu, 2011. gada 24. novembris, *ASNEF* un *FECEMD*, C-468/10 un C-469/10, EU:C:2011:777, 47. un 48. punkts).

63 Ar tādu regulējumu kā tas, kas tiek aplūkots pamatlietā, tiek sašaurināta Direktīvas 95/46 7. panta f) punktā paredzētā principa piemērošanas joma attiecībā uz tiešsaistes plašsaziņas līdzekļu vietņu lietotāju personas datu apstrādi, izslēdzot iespēju veikt mērķa nodrošināt minētā tiešsaistes plašsaziņas līdzekļa vispārēju funkcionēšanas spēju izsvēršanu saistībā ar šo lietotāju interesēm vai pamattiesībām un pamatbrīvībām, kuras tiek aizsargātas atbilstoši šīs direktīvas 1. panta 1. punktam.

64 No visiem iepriekš minētajiem apsvērumiem izriet, ka uz otro jautājumu ir jāatbild, ka Direktīvas 95/46 7. panta f) punkts ir jāinterpretē tādējādi, ka ar to netiek pieļauts dalībvalsts regulējums, atbilstoši kuram tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs šo pakalpojumu lietotāja personas datus bez viņa piekrišanas var iegūt un izmantot tikai tad, ja šī iegūšana un izmantošana ir nepieciešama, lai nodrošinātu minēto pakalpojumu konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un mērķis nodrošināt minēto pakalpojumu vispārēju funkcionēšanas spēju nevar attaisnot minēto datu izmantošanu pēc konkrēta pakalpojumu izmantošanas procesa beigām.

Par tiesāšanās izdevumiem

65 Attiecībā uz pamatlietas pusēm šī tiesvedība ir stadija procesā, kuru izskata iesniedzējtiesa, un tā lemj par tiesāšanās izdevumiem. Izdevumi, kas radušies, iesniedzot apsvērumus Tiesai, un kas nav minēto pušu izdevumi, nav atlīdzināmi.

Ar šādu pamatojumu Tiesa (otrā palāta) nospriež:

1) 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) punkts ir jāinterpretē tādējādi, ka dinamiskā interneta protokola adrese, ko tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs ieraksta saistībā ar personas piekļuvi šī pakalpojumu sniedzēja publiskai lietošanai paredzētai interneta vietnei, attiecībā uz minēto pakalpojumu sniedzēju ir uzskatāma par personas datiem šīs tiesību normas izpratnē, ja tā rīcībā ir tiesiski līdzekļi, kas tam ļauj likt identificēt attiecīgo personu, izmantojot šīs personas interneta piekļuves pakalpojumu sniedzēja rīcībā esošo papildu informāciju;

2) Direktīvas 95/46 7. panta f) punkts ir jāinterpretē tādējādi, ka ar to netiek pieļauts dalībvalsts regulējums, atbilstoši kuram tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs šo pakalpojumu lietotāja personas datus bez viņa piekrišanas var iegūt un izmantot tikai tad, ja šī iegūšana un izmantošana ir nepieciešama, lai nodrošinātu minēto pakalpojumu konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un mērķis nodrošināt minēto pakalpojumu vispārēju funkcionēšanas spēju nevar attaisnot minēto datu izmantošanu pēc konkrēta pakalpojumu izmantošanas procesa beigām.

[Paraksti]