Kohtulahendite kogumik

KOHTUJURISTI ETTEPANEK
MANUEL CAMPOS SÁNCHEZ-BORDONA
esitatud 12. mail 2016*

Kohtuasi C-582/14

Patrick Breyer
versus
Saksamaa Liitvabariik

(eelotsusetaotlus, mille on esitanud Bundesgerichtshof (Saksamaa Liitvabariigi kõrgeim üldkohus))

Isikuandmete töötlemine — Direktiiv 95/46/EÜ — Artikli 2 punkt a ja artikli 7 punkt f — Mõiste „isikuandmed“ — IP-aadressid — Säilitamine elektroonilise meedia teenuse pakkuja poolt — Siseriiklik õigusnorm, mis ei luba arvesse võtta vastutava töötleja õiguspärast huvi

1. Interneti-protokolli aadress (edaspidi „IP-aadress“) on binaararvude jada, mis seadmele (arvuti, tahvelarvuti, nutitelefon) eraldatult tuvastab seadet ja võimaldab selle juurdepääsu elektronsidevõrgule. Internetti ühendamiseks peab seade kasutama võrguteenuse pakkuja antud numbrijada. IP-aadress edastatakse serverile, kus hoitakse külastatavat veebisaiti.

2. Konkreetselt eraldavad võrguühenduse pakkujad (üldjuhul telefoniettevõtjad) oma klientidele ajutiselt iga internetiühenduse jaoks niinimetatud IP-aadressid ja muudavad neid hilisemate ühenduste puhul. Need samad ettevõtjad peavad registrit, milles on märgitud, millised IP-aadressid nad on igal ajal konkreetsele seadmele eraldanud.**

3. Ka nende veebisaitide omanikud, mida dünaamilistelt IP-aadressidelt külastatakse, peavad harilikult registreid, kus on märgitud, milliseid saite, millal ja milliselt dünaamiliselt IP-aadressilt on vaadatud. Neid registreid võib pärast iga kasutaja internetiühenduse lõpetamist tehniliselt säilitada ilma ajalise piiranguta.

4. Ainuüksi dünaamilisest IP-aadressist teenusepakkujale ei piisa oma veebisaidi kasutaja tuvastamiseks. Ta saab seda aga teha, kui ta kombineerib dünaamilise IP-aadressi teiste võrguühenduse pakkuja käsutuses olevate lisaandmetega.

5. Kohtuasjas vaieldakse, kas dünaamilised IP-aadressid on direktiivi 95/46/EÜ*** artikli 2 punkti a tähenduses isikuandmed. Vastamiseks tuleb enne kindlaks määrata, millist tähtsust omab selleks asjaolu, et kasutaja tuvastamiseks vajalikud lisaandmed ei ole veebisaidi omaniku, vaid kolmanda isiku (konkreetselt võrguühenduse teenusepakkuja) valduses.

* Algkeel: hispaania.

** Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiivi 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (ELT 2006, L 105, lk 54), artiklis 5 oli muude kohustuste hulgas sätestatud kohustus säilitada raskete rikkumiste uurimise, tuvastamise ja karistamise eesmärgil „Interneti-seansi alguse ja lõpu kuupäev ja kellaaeg […] koos dünaamilise või staatilise Interneti-protokolli aadressiga, mille on kasutajale eraldanud Interneti-teenuse pakkuja, ja abonendi või registreeritud kasutaja kasutajatunnusega“.

*** Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT 1995, L 281, lk 31; ELT eriväljaanne 13/15, lk 355).

6. See on Euroopa Kohtu jaoks seni käsitlemata küsimus, sest kohtuotsuse Scarlet Extended**** punktis 51 ta tuvastas, et IP-aadressid „on kaitstud isikuandmed, sest nende identifitseerimine võimaldab selliste kasutajate täpse tuvastamise“, kuid kontekstis, kus IP-aadresse kogus ja identifitseeris võrguühenduse pakkuja,***** mitte sisupakkuja, nagu see on käesolevas kohtuasjas.

7. Kui IP-aadressid oleksid internetiteenuse pakkuja jaoks isikuandmed, tuleks seejärel kontrollida, kas nende töötlemine kuulub direktiivi 95/46 kohaldamisalasse.

8. On võimalik, et isegi kui tegu on isikuandmetega, ei ole need direktiiviga 95/46 kaitstud, kui näiteks nende töötlemise eesmärk on kriminaalasja algatamine veebisaidi võimalike ründajate vastu. Sel juhul ei ole direktiiv 95/46 selle artikli 3 lõike 2 kolmanda taande kohaselt kohaldatav.

9. Lisaks tuleb välja selgitada, kas teenusepakkuja, kes registreerib dünaamilised IP-aadressid, kui kasutaja pöördub tema veebisaidile (käesolevas kohtuasjas Saksamaa Liitvabariik), toimib avaliku võimu organina või pigem üksikisikuna.

10. Kui direktiiv 95/46 on kohaldatav, tuleks lõpuks täpsustada, mil määral on selle artikli 7 punktiga f kooskõlas siseriiklik õigusnorm, millega piiratakse selles punktis isikuandmete töötlemise põhjendamiseks kehtestatud tingimustest ühe tingimuse ulatust.

I. **Õiguslik raamistik**

A. *Liidu õigus*

11. Direktiivi 95/46 põhjendus 26 on järgmise sisuga:

„(26) [K]aitsmise põhimõtteid tuleb kohaldada igasuguse tuvastatud või tuvastatava isiku kohta käiva teabe suhtes; isiku tuvastatavuse kindlakstegemisel tuleb arvesse võtta kõiki vahendeid, mida volitatud töötleja või keegi muu võib andmesubjekti tuvastamiseks tõenäoliselt kasutada; kaitsmise põhimõtteid ei kohaldata teabe suhtes, mis on muudetud anonüümseks selliselt, et andmesubjekti ei ole enam võimalik tuvastada; tegevusjuhendid artikli 27 tähenduses võivad osutuda kasulikeks juhtnöörideks selle kohta, kuidas andmeid muuta anonüümseks ja kuidas neid säilitada kujul, mis ei võimalda andmesubjekti tuvastamist.“

12. Direktiivi 95/46 artiklis 1 on ette nähtud:

„1. Vastavalt käesolevale direktiivile kaitsevad liikmesriigid isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusele.

2. Liikmesriigid ei piira ega keela isikuandmete vaba liikumist liikmesriikide vahel põhjustel, mis on seotud lõikes 1 sätestatud kaitsega.“

**** Kohtuotsus, 24.11.2011 (C-70/10, EU:C:2011:771, punkt 51).

***** Nii oli see ka kohtuotsuses, 19.4.2012, Bonnier Audio jt (C-461/10, EU:C:2012:219, punktid 51 ja 52).

13. Direktiivi 95/46 artikli 2 kohaselt:

„Käesolevas [direktiivis] kasutatakse järgmisi mõisteid:

a) isikuandmed – igasugune teave tuvastatud või tuvastatava füüsilise isiku (edaspidi „andmesubjekt“) kohta. Tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal;

b) isikuandmete töötlemine (edaspidi „töötlemine“) – iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine;

[…]

d) vastutav töötleja – füüsiline või juriidiline isik, riigiasutus, esindused või mõni muu organ, kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui töötlemise eesmärgid ja vahendid on kindlaks määratud siseriiklike või ühenduse õigusnormidega, võib vastutava töötleja või tema ametissemääramise sätestada siseriiklikus või ühenduse õiguses;

[…]

f) kolmas isik – kõik füüsilised või juriidilised isikud, riigiasutused, esindused või muud organid, välja arvatud andmesubjekt, vastutav töötleja, volitatud töötleja ja isikud, kes võivad andmeid töödelda vastutava töötleja või volitatud töötleja otseses alluvuses;

[…]“.

14. Direktiivi 95/46 artiklis 3 „Reguleerimisala“ on sätestatud:

„1. Käesolevat direktiivi kohaldatakse isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad kataloogi või kui nad kavatsetakse hiljem sellesse kanda.

2. Käesolevat direktiivi ei kohaldata isikuandmete töötlemise suhtes:

— kui see toimub sellise tegevuse käigus, mis jääb väljapoole ühenduse õigust, nagu näiteks Euroopa Liidu lepingu V j[a] VI jaotises osutatud tegevused, ja igal juhul sellise töötlemise suhtes, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (sealhulgas riigi majanduslik heaolu, kui töötlemine on seotud riigi julgeoleku küsimustega) ja riigi toimingutega kriminaalõiguse valdkonnas;

[…]“.

15. Direktiivi 95/46 II peatükk „Üldised eeskirjad isikuandmete töötlemise seaduslikkuse kohta“ algab artikliga 5, mille kohaselt „[k]uivõrd see on lubatud käesoleva peatüki sätetega, määravad liikmesriigid täpsemalt kindlaks tingimused, mille puhul isikuandmete töötlemine on seaduslik“.

16. Direktiivi 95/46 artikkel 6 näeb ette:

„1. Liikmesriigid sätestavad selle, et:

a) isikuandmeid töödeldakse õiglaselt ja seaduslikult;

b) isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ega töödelda hiljem viisil, mis on vastuolus kõnealuste eesmärkidega. Täiendavat töötlemist ajaloo, statistika või teadusega seotud eesmärkidel ei peeta vastuolus olevaks tingimusel, et liikmesriigid kannavad hoolt vajalike tagatiste eest;

c) isikuandmed on piisavad, asjakohased ega ületa selle otstarbe piire, mille tarvis neid kogutakse ja/või hiljem töödeldakse;

d) andmed on täpsed ja vajaduse korral ajakohastatud; võetakse kõik mõistlikud meetmed, et kustutada või parandada andmete kogumise või hilisema töötlemise eesmärgi seisukohast ebaõiged või mittetäielikud andmed;

e) isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega. Liikmesriigid kehtestavad vajalikud tagatised nende isikuandmete jaoks, mida säilitatakse pikema aja jooksul, et neid kasutada seoses ajaloo, statistika või teadusega.

2. Lõike 1 järgimise tagab vastutav töötleja.“

17. Direktiivi 95/46 artikli 7 kohaselt:

„Liikmesriigid sätestavad, et isikuandmeid võib töödelda ainult juhul, kui:

a) andmesubjekt on selleks andnud oma ühemõttelise nõusoleku või

b) töötlemine on vajalik sellise lepingu täitmiseks, mille osapool andmesubjekt on, või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele või

c) töötlemine on vajalik vastutava töötleja seadusjärgse kohustuse täitmiseks või

d) töötlemine on vajalik andmesubjekti eluliste huvide kaitsmiseks või

e) töötlemine on vajalik üldiste huvidega seotud ülesande täitmiseks või sellise avaliku võimu teostamiseks, mis on tehtud ülesandeks volitatud töötlejale või andmeid saavale kolmandale isikule, või

f) töötlemine on vajalik vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huvide elluviimiseks, kui selliseid huve ei kaalu üles artikli 1 lõike 1 kohaselt kaitstavate andmesubjekti põhiõiguste ja -vabadustega seotud huvid.“

18. Direktiivi 95/46 artikkel 13 sätestab:

„1. Liikmesriigid võivad artikli 6 lõikes 1, artiklis 10, artikli 11 lõikes 1 ja artiklites 12 ja 21 sätestatud kohustuste ja õiguste ulatuse piiramiseks võtta vastu õigusakte, kui sellised piirangud on vajalikud, et kindlustada:

a) riigi julgeolek;

b) riigikaitse;

c) avalik kord;

d) kuritegude või reguleeritud kutsealade ametieetika rikkumiste ennetamine, uurimine, avastamine ja nende eest vastutuselevõtmine;

e) liikmesriigi või Euroopa Liidu olulised majanduslikud või rahanduslikud huvid, sealhulgas raha-, eelarve- ja maksuküsimused;

f) jälgimine, kontrollimine ja regulatiivne funktsioon, mis on kas või ajutiselt seotud avaliku võimu teostamisega punktides c, d ja e osutatud juhtudel;

g) andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse.

[…]“

B. *Liikmesriigi õigus*

19. Elektrooniliste teabe- ja sideteenuste seaduse (Telemediengesetz, edaspidi „TMG“)****** § 12 näeb ette:

„1. Teenuseosutaja võib elektrooniliste teabe- ja sideteenuste kättesaadavaks tegemisel koguda ja kasutada isikuandmeid üksnes juhul, kui see on lubatud käesoleva seadusega või sõnaselgelt elektroonilisi teabe- ja sideteenuseid käsitleva muu õigusnormiga või kasutaja nõusolekul.

2. Teenuseosutaja võib elektrooniliste teabe- ja sideteenuste kättesaadavaks tegemiseks kogutud isikuandmeid kasutada muul eesmärgil üksnes juhul, kui see on lubatud käesoleva seadusega või sõnaselgelt elektroonilisi teabe- ja sideteenuseid käsitleva muu õigusnormiga või kasutaja nõusolekul.

3. Kui ei ole sätestatud teisiti, kohaldatakse vastavalt isikuandmete kaitse kohta kehtivaid sätteid ka juhul, kui andmed ei kuulu automaatselt töötlemisele.“

20. TMG § 15 näeb ette:

„1. Teenuseosutaja võib kasutaja isikuandmeid koguda ja kasutada üksnes juhul, kui see on vajalik elektrooniliste teabe- ja sideteenuste konkreetse kasutuselevõtu võimaldamiseks ja arve esitamiseks (kasutusandmed). Kasutusandmed on eelkõige:

1) tunnused kasutaja tuvastamiseks;

2) andmed side toimumise alguse ja lõpu ning kestuse kohta ja

3) andmed kasutatud elektrooniliste teabe- ja sideteenuste kohta.

2. Teenuseosutaja võib kasutaja andmeid eri elektrooniliste teabe- ja sideteenuste kasutuselevõtmise kohta üksteisega seostada juhul, kui see on kasutajale arve esitamiseks vajalik.

[…]

4. Teenuseosutaja võib kasutada kasutusandmeid ka pärast side toimumist, kui see on vajalik kasutajale arve esitamiseks (arveldusandmed). Teenuseosutaja võib seadusjärgsetest, põhikirjale tuginevatest ja lepingulistest säilitamistähtaegadest kinnipidamiseks andmetele juurdepääsu blokeerida. […]“

21. Föderaalse andmekaitseseaduse (Bundesdatenschutzgesetz, edaspidi „BDSG“)******* § 3 lõike 1 kohaselt on „[i]sikuandmed […] üksikud andmed tuvastatud või tuvastatava füüsilise isiku (andmesubjekt) isiklike või materiaalsete suhete kohta. […]“.

****** 26. veebruari 2007. aasta seadus (*BGBl* 2007 I, lk 179).

******* 20. detsembri 1990. aasta seadus (*BGBl* 1990 I, lk 2954).

II. **Faktilised asjaolud**

22. P. Breyer esitas Saksamaa Liitvabariigi vastu hagi nõudega lõpetada IP-aadresside registreerimine.

23. Paljud Saksa avalik-õiguslikud institutsioonid peavad üldsusele ligipääsetavaid internetiportaale, kus nad pakuvad ajakohastatud teavet. Rünnete ära hoidmiseks ja selleks et võimaldada ründajaid kriminaalvastutusele võtta, säilitatakse enamikus nendest Saksa portaalidest kõik külastused failides või protokolliregistrites. Nendes säilitatakse (s.h ka pärast side lõppu) allalaaditud faili või külastatud lehekülje nimi, otsinguväljale sisestatud sõnad, külastuse aeg, edastatud andmete hulk, teade, kas külastus oli edukas, ja selle arvuti IP-aadress, millelt külastus tehti.

24. P. Breyer, kes külastas mitmeid nimetatud veebilehti, nõudis oma hagis, et Saksamaa Liitvabariiki kohustataks lõpetama ise või kolmandate isikute kaudu selle süsteemi hosti IP-aadressi salvestamine, millelt külastused tehti, välja arvatud juhul, kui see on vajalik elektrooniliste teabe- ja sideteenuste kättesaadavuse taastamiseks rikke korral.

25. P. Breyeri nõue jäeti esimeses astmes rahuldamata. Tema apellatsioonkaebus, aga osaliselt rahuldati ning Saksamaa Liitvabariiki kohustati lõpetama aadressiandmete säilitamine pärast iga side lõppu. Lõpetamise korralduse tingimuseks seati, et apellant esitaks side ajal oma isikuandmed, kaasa arvatud elektronposti aadressi kujul, ja et andmete säilitamine ei ole tingimata vajalik sideteenuse kättesaadavuse taastamiseks.

III. **Esitatud küsimus**

26. Kui mõlemad pooled esitasid kassatsioonkaebuse, sõnastas Bundesgerichtshofi (Saksamaa kõrgeim üldkohus) VI kolleegium järgmised eelotsuse küsimused, mis esitati 17. detsembril 2014:

„1. Kas […] direktiivi 95/46/EÜ artikli 2 punkti a tuleb tõlgendada nii, et Interneti-protokolli aadress (IP-aadress), mida teenuseosutaja seoses juurdepääsuga oma veebileheküljele salvestab, kujutab endast teenuseosutaja jaoks isikuandmeid juba hetkest, kui kolmandal isikul (käesolevas kohtuasjas ühenduse pakkuja) on olemas andmesubjekti tuvastamiseks vajalik lisateave?

2. Kas andmekaitsedirektiivi artikli 7 punktiga f on vastuolus siseriiklik säte, mille kohaselt võib teenuseosutaja koguda ja kasutada kasutaja isikuandmeid ilma tema nõusolekuta üksnes juhul, kui see on vajalik kasutaja poolt elektrooniliste teabe- ja sideteenuste konkreetse kasutuselevõtu võimaldamiseks ja arve esitamiseks ja mille kohaselt ei saa elektrooniliste teabe- ja sideteenuste üldise toimimise tagamise eesmärk õigustada andmete kasutamist pärast vastava side toimumist?“

27. Nagu selgitab eelotsusetaotluse esitanud kohus, võib kassatsioonkaebuse esitaja Saksa õiguse kohaselt nõuda IP-aadresside salvestamise lõpetamist, kui nende säilitamine on andmekaitse õigusaktide kohaselt õigusvastane sekkumine tema üldistesse isikuõigustesse, konkreetsemalt tema „informatsioonilise enesemääramise“ õigusesse (Saksa tsiviilseadustiku (Bürgerliches Gesetzbuch) § 1004 lõige 1 ja § 823 lõige 1 koostoimes põhiseaduse (Grundgesetz) artiklitega 1 ja 2).

28. Nii oleks see juhul, kui: a) IP-aadressi (igal juhul koos veebilehe külastamise ajaga) saaks kvalifitseerida „isikuandmeteks“ direktiivi 95/46 artikli 2 punkti a tähenduses koostoimes selle direktiivi põhjenduse 26 teise lausega või TMG § 12 lõigete 1 ja 3 tähenduses koostoimes BDSG § 3 lõikega 1; ja kui b) ei ole täidetud ükski lubamise tingimus direktiivi 95/46 artikli 7 punkti f tähenduses või TMG § 12 lõigete 1 ja 3 ning § 15 lõigete 1 ja 4 tähenduses.

29. Bundesgerichtshofi (kõrgeim üldkohus) hinnangul on liikmesriigi õiguse (TMG § 12 lõige 1) tõlgendamiseks vältimatult vajalik teada, kuidas tuleb mõista direktiivi 95/46 artikli 2 punktis a nimetatud isikuandmete tähendust.

30. Lisaks märgib eelotsusetaotluse esitanud kohus, et kuna TMG § 15 lõike 1 kohaselt võib teenuseosutaja isikuandmeid koguda ja kasutada ainult siis, kui see on tingimata vajalik selleks, et võimaldada sideteenuste kasutuselevõttu ja nende eest arveid esitada (kasutusandmed),******** on selle siseriikliku õigusnormi tõlgendamine seotud direktiivi 95/46 artikli 7 punkti f tõlgendamisega.

IV. **Menetlus Euroopa Kohtus. Poolte argumendid.**

31. Oma kirjalikud seisukohad esitasid Saksamaa, Austria ja Portugali valitsus ja lisaks komisjon. Ainult see institutsioon, nagu ka P. Breyer, osalesid avalikul kohtuistungil, mis peeti 25. veebruaril 2016, millel osalemast Saksamaa valitsus keeldus.

A. *Poolte argumendid esimese küsimuse kohta*

32. P. Breyer on seisukohal, et isikuandmed on ka need, mida saab omavahel kombineerida ainult teoreetiliselt, see tähendab lähtudes potentsiaalsest abstraktsest ohust, kusjuures ei ole oluline, kas neid praktikas tegelikult kombineeritakse. Tema arvates ei tähenda asjaolu, et asutusel võib olla suhteliselt võimatu isikut IP-aadressi abil tuvastada, et ei esineks ohtu selle isiku jaoks. Pealegi on tema arvates oluline asjaolu, et Saksamaa säilitab tema IP-aadresse selleks, et vajaduse korral tuvastada võimalikke ründeid või algatada kriminaalasju, nagu on lubatud telekommunikatsiooniseaduse (Telekommunikationsgesetz) §-ga 113 ja nagu on mitmel korral juhtunud.

33. Saksamaa valitsuse arvates tuleb esimesele küsimusele vastata eitavalt. Tema arvates ei näita dünaamilised IP-aadressid direktiivi 95/46/EÜ artikli 2 punkti a tähenduses „tuvastatud“ isikut. Selleks et otsustada, kas antakse teavet sama sätte tähenduses „tuvastatava“ isiku kohta, tuleb tuvastatavust kontrollida „suhtelise“ kriteeriumi põhjal. Nii nähtub tema arvates direktiivi 95/46 põhjendusest 26, mille kohaselt tuleb arvesse võtta ainult neid vahendeid, mida volitatud töötleja või keegi kolmas isik võib isiku tuvastamiseks „tõenäoliselt“ kasutada. Niisugune täpsustus näitab tema arvates, et liidu seadusandja ei ole soovinud lisada direktiivi 95/46 kohaldamisalasse olukordi, kus on objektiivselt võimalik tuvastamine mis tahes kolmanda isiku poolt.

34. Saksamaa valitsus leiab ühtlasi, et mõistet „isikuandmed“ direktiivi 95/46 artikli 2 punkti a tähenduses tuleb tõlgendada, pidades silmas direktiivi eesmärki, mis on tagada põhiõiguste kaitse. Vajadust kaitsta füüsilisi isikuid võiks vaadelda teisiti, olenevalt sellest, kelle valduses andmed on ja kas tal on või ei ole vahendeid, mida kasutada nende isikute tuvastamiseks.

35. Saksamaa valitsus väidab, et P. Breyer ei ole tuvastatav IP-aadresside abil koostoimes muude andmetega, mida sisupakkujad säilitavad. Selleks tuleks käsitleda teavet, mis on internetiühenduse pakkujate valduses, kes ei või seda ilma õigusliku aluseta anda sisupakkujatele.

36. Austria valitsuse arvates peab, vastupidi, vastus olema jaatav. Direktiivi 95/46 põhjenduse 26 kohaselt ei ole selleks, et isikut käsitada tuvastatavana, vajalik, et kõik tema identifitseerimisandmed oleksid ühe ainsa üksuse käes. Seepärast võiksid IP-aadressid olla isikuandmed juhul, kui kolmandal isikul (nagu näiteks internetiühenduse pakkuja) on olemas vahendid selle aadressi omaniku tuvastamiseks, ilma et selleks tuleks teha ülemääraseid pingutusi.

37. Portugali valitsus pooldab samuti jaatavat vastust, leides, et IP-aadress kombineeritult külastusseansi kuupäevaga on isikuandmed, kuna nende järgi saab kasutajat tuvastada muu isik peale selle isiku, kes on salvestanud IP-aadressi.

******** Bundesgerichtshofi (kõrgeim üldkohus) sõnul on kasutusandmed kasutaja tuvastamise, kasutuse alguse ja lõpu ja selle kestuse ning kasutaja kasutatud sideteenuse andmed.

38. Komisjon teeb samuti ettepaneku vastata jaatavalt, tuginedes Euroopa Kohtu lahendile kohtuasjas Scarlet Extended******** . Komisjon on seisukohal, et kuna IP-aadresse säilitatakse just nimelt selleks, et tuvastada kasutajaid küberrünnakute korral, oleksid lisaandmed, mida internetiühenduse pakkujad salvestavad, vahend, mida saab direktiivi 95/46 põhjenduse 26 tähenduses „tõenäoliselt“ kasutada. Lõppkokkuvõttes räägivad komisjoni hinnangul nii selle direktiivi eesmärk kui ka Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artiklid 7 ja 8 direktiivi 95/46 artikli 2 punkti a laialt tõlgendamise poolt.

B. *Poolte argumendid teise küsimuse kohta*

39. P. Breyer on seisukohal, et direktiivi 95/46 artikli 7 punkt f on üldsäte, mille rakendamine nõuab selle konkreetset määratlemist. Euroopa Kohtu praktika kohaselt tuleks seega hinnata konkreetse juhtumi asjaolusid ja määrata kindlaks, kas on rühmi, kellel on selle sätte tähenduses õiguspärane huvi, mistõttu ei ole mitte ainult lubatud, vaid on tingimata vajalik näha niisuguste rühmade jaoks ette erinormid selle artikli kohaldamiseks. Sel juhul ja P. Breyeri jaoks on tema arvates siseriiklik õigusnorm direktiivi 95/46 artikli 7 punktiga f kooskõlas, kuna avalikul portaalil ei ole huvi säilitada isikuandmeid, või seepärast, et huvi kaitsta anonüümsust on ülekaalukam. Tema arvates ei ole siiski süstemaatiline ja isiklikku laadi andmete säilitamine demokraatliku ühiskonnaga kooskõlas ega vajalik ega proportsionaalne elektroonilise meedia toimimise tagamiseks, mis on täiesti võimalik ka ilma neid isikuandmeid salvestamata, nagu on näha liitvabariigi mõne ministeeriumi veebisaidi näitel.

40. Saksamaa valitsus väidab, et teist küsimust ei ole vaja käsitleda, kuna see on esitatud ainult juhuks, kui esimesele küsimusele vastatakse jaatavalt, mis tema arvates aga nii ei ole eespool nimetatud põhjustel.

41. Austria valitsus teeb ettepaneku vastata, et niisuguste andmete säilitamine, nagu on vaidluse all põhikohtuasjas, ei ole üldiselt direktiiviga 95/46 vastuolus, kui see on tingimata vajalik selleks, et tagada elektroonilise meedia nõuetekohane toimimine. Selle valitsuse arvates võib IP-aadressi piiratud säilitamine veebilehe külastuse kestusest kauem olla õiguspärane, kuna vastutav isikuandmete töötleja on kohustatud rakendama nende andmete kaitse meetmeid, mis on direktiivi 95/46 artikli 17 lõikega 1 kohustuslikud. Küberrünnakute vastu võitlemiseks võib olla põhjendatud analüüsida andmeid varasemate rünnakute kohta ja keelata mõnele IP-aadressile juurdepääs internetilehele. Niisuguste – nagu põhikohtumenetluses arutatavate – andmete säilitamise proportsionaalsust elektroonilise meedia nõuetekohase toimimise tagamise eesmärgi seisukohast tuleks hinnata igal üksikjuhul eraldi, võttes arvesse direktiivi 95/46 artikli 6 lõikes 1 sätestatud põhimõtteid.

42. Portugali valitsus asub seisukohale, et põhikohtuasjas arutatavad siseriiklikud õigusnormid ei ole direktiivi 95/46 artikli 7 punktiga f vastuolus, sest tema hinnangul on Saksamaa seadusandja juba kaalunud ühelt poolt vastutava isikuandmete töötleja õiguspärast huvi ja teiselt poolt nende andmete omaniku õigusi ja vabadusi, nagu on nimetatud õigusnormis ette nähtud.

43. Komisjoni hinnangul peavad siseriiklikus õigusnormis, milles on direktiivi 95/46 artikli 7 punkt f üle võetud, olema määratletud isikuandmete töötlemise eesmärgid nii, et need oleksid asjaomasele isikule ootuspärased. Kuna TMG § 15 lõikes 1 on sätestatud, et IP-aadresse on lubatud säilitada, kui „see on vajalik […] sideteenuste konkreetse kasutuselevõtu võimaldamiseks […]“, ei vasta Saksa õigusnorm tema arvates sellele nõudele.

******** Kohtuotsus, 24.11.2011 (C-70/10, EU:C:2011:771, punkt 51).

44. Seepärast pakub komisjon teisele küsimusele vastuseks, et selle õigusnormiga on vastuolus siseriikliku õigusnormi tõlgendamine nii, et teenusepakkujana tegutsevad riigiasutused võivad koguda ja kasutada kasutaja isikuandmeid ilma tema loata, isegi juhul kui eesmärk, mida taotletakse, on tagada elektroonilise meedia üldine nõuetekohane toimimine, kui see eesmärk ei ole nimetatud siseriiklikus õigusnormis piisavalt selgelt ja täpselt sätestatud.

V. **Õiguslik hinnang**

A. *Esimene küsimus*

1. Esitatud küsimuse piiritlemine

45. Sõnastuse kohaselt, milles Bundesgerichtshof (kõrgeim üldkohus) oma esimese eelotsuse küsimuse esitas, tahetakse sellega välja selgitada, kas IP-aadress, millega veebilehte külastatakse, on selle lehe omanikust avalik-õigusliku isiku jaoks isikuandmed (direktiivi 95/46/EÜ artikli 2 punkti a tähenduses) juhul, kui võrguühenduse pakkujal on lisaandmeid, mille abil saab asjaomast isikut tuvastada.

46. Selliselt sõnastatult on küsimus piisavalt täpne selleks, et kohe välistada muud küsimused, mis võiksid in abstracto tekkida seoses IP-aadresside juriidilise olemusega isikuandmete kaitse kontekstis.

47. Kõigepealt peab Bundesgerichtshof (kõrgeim üldkohus) silmas ainult „dünaamilisi IP-aadresse“, see tähendab neid, mis eraldatakse iga võrguühenduse puhuks ajutiselt ja mida järgnevate ühenduste korral muudetakse. Seega on välja jäetud „püsivad ehk staatilised IP-aadressid“, millele on iseloomulik, et need on muutumatud ja nende abil saab võrku ühendatud seadet alaliselt tuvastada.

48. Teiseks lähtub eelotsusetaotluse esitanud kohus eeldusest, et põhikohtumenetluses ei ole veebilehe pakkujal võimalik tema veebilehe külastajaid dünaamilise IP-aadressi abil tuvastada ega temal endal ei ole lisaandmeid, mille abil selle IP-aadressiga kombineerituna saaks neid isikuid tuvastada. Näib, et Bundesgerichtshof (kõrgeim üldkohus) leiab, et selles kontekstis ei ole dünaamiline IP-aadress direktiivi 95/46 artikli 2 punkti a tähenduses isikuandmed veebilehe pakkuja jaoks.

49. Eelotsusetaotluse esitanud kohtu kahtlus on seotud võimalusega, et dünaamilist IP-aadressi võiks kvalifitseerida veebilehe pakkuja jaoks isikuandmetena, kui kolmandal isikul on lisaandmeid, mille abil koostoimes selle aadressiga saaks selle pakkuja lehe külastajaid tuvastada. Ent – ja see on just see kõige määravam – Bundesgerichtshof (kõrgeim üldkohus) ei nimeta ühtegi kolmandat isikut, kellel oleks lisaandmeid, vaid ainult võrguühenduse pakkujat (välistades seega teised võimalikud isikud, kellel oleks seda laadi andmeid).

50. Niisiis jäävad arutelust muu hulgas välja järgmised aspektid: a) kas staatilised IP-aadressid on direktiivi 95/46 kohaselt isikuandmed;********** b) kas dünaamilised IP-aadressid on alati ja mis tahes asjaoludel selle direktiivi tähenduses isikuandmed, ja lõpuks c) kas dünaamiliste IP-aadresside kvalifitseerimine isikuandmeteks on vältimatu, niipea kui on mis tahes kolmas isik, kes suudab neid kasutada võrgu kasutajate tuvastamiseks.

********** Selle probleemi lahendas Euroopa Kohus kohtuotsustes, 24.11.2011, Scarlet Extended (C-70/10, EU:C:2011:771, punkt 51) ja 19.4.2012, Bonnier Audio jt (C-461/10, EU:C:2012:219). Viimati nimetatud kohtuotsuse punktides 51 ja 52 järeldas Euroopa Kohus, et „sellise […] interneti kasutaja nimi ja aadress, kes kasutab IP-aadressi, mille kaudu kaitstud teoseid sisaldavaid faile võidi ebaseaduslikult vahetada, [avaldamine] kujutab endast isikuandmete töötlemist direktiivi 2002/58 artikli 2 esimese lõigu tähenduses koostoimes direktiivi 95/46 artikli 2 punktiga b“.

51. Tuleb seega ainult otsustada, kas dünaamilised IP-aadressid on internetiteenuse pakkuja jaoks isikuandmed, kui sideettevõtja, kes pakub võrguühendust (ühendusepakkuja), käitleb lisaandmeid, mis koostoimes selle aadressiga võimaldab esimese poolt hallatava veebilehe külastajat tuvastada.

2. Sisulised küsimused

52. Käesoleva eelotsusetaotluse küsimus on tõstatanud Saksa õiguskirjanduses ja kohtupraktikas ägedat poleemikat, milles pooled on jagunenud kahte arvamusleeri.********** Ühe arvates (kes otsustab „objektiivse“ või „absoluutse“ kriteeriumi kasuks) on kasutaja tuvastatav – ja seega IP-aadressid on isikuandmed, mida tuleks kaitsta –, kui internetiteenuse pakkuja võimalustele ja vahenditele vaatamata on kasutajat võimalik tuvastada ainult selle dünaamilise IP-aadressi kombineerimise teel kolmanda isiku (näiteks võrguühenduse pakkuja) antud andmetega.

53. Teise leeri pooldajate (kes pooldavad „suhtelist“ kriteeriumit) arvates ei piisa võimalusest arvestada kasutaja lõplikul tuvastamisel kolmanda isiku abiga selleks, et pidada dünaamilist IP-aadresse isikuandmeteks. Oluline on see, et andmetele juurdepääsu omav isik suudab neid kasutada oma vahenditega ja nii isikut tuvastada.

54. Millised selle poleemika seisukohad liikmesriigi õiguses ka ei oleks, peab Euroopa Kohus oma vastuses tõlgendama ainult direktiivi 95/46 neid sätteid, mida nimetasid nii eelotsusetaotluse esitanud kohus kui ka kohtumenetluse pooled, s.o selle artikli 2 punkti a********** ja selle põhjendust 26.**********

55. Ainult sellega, et dünaamilised IP-aadressid annavad teavet arvutist (või muust seadmest) veebilehe külastamise kuupäeva ja kellaaja kohta, avaldavad need internetikasutajate teatavaid käitumisjooni ja seega tähendavad potentsiaalset sekkumist õigusesse eraelu puutumatusele,********** mis on tagatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 ja harta artikliga 7, millest, nagu ka selle harta artiklist 8 tuleb direktiivi 95/46 tõlgendamisel lähtuda.********** Tegelikult ei sea kohtuvaidluse pooled seda eeldust kahtluse alla, mis ei ole iseenesest ka eelotsuse küsimuse ese.

56. Isik, kelle andmed need üksikasjalikud andmed on, ei ole „tuvastatud füüsiline isik“. Side kuupäev ja kellaaeg, nagu ka selle lähtekoha number, ei näita otseselt ega vahetult, kes on füüsiline isik, kellele kuulub seade, millelt veebilehte külastatakse, ega ka seadet käsitseva kasutaja isikut (võib olla mis tahes füüsiline isik).

********** Nende kahe seisukoha kohta õiguskirjanduses võib vaadata näiteks Schreibauer, M., *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P. ja von Lewinski, K. (kirj), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4. trükk, § 11 Telemediengesetz (4-10). Nink, J. ja Pohle, J.: „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze“, *Multimedia und Recht*, 9/2015, lk 563–567. Heidrich, J., ja Wegener, C.: „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging“, *Multimedia und Recht*, 8/2015, lk 487–492. Leisterer, H.: „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr“, *Computer und Recht*, 10/2015, lk 665–670.

********** Ära toodud punktis 13.

********** Ära toodud punktis 11.

********** Nii tuletas seda meelde kohtujurist Cruz Villalón ettepanekus kohtuasjas Scarlet Extended (C-70/10, EU:C:2011:255, punkt 76) ja nii mõistab seda Euroopa andmekaitseinspektor oma 22. veebruari 2010. aasta arvamuses Euroopa Liidu praeguste läbirääkimiste kohta võltsimisvastast võitlust käsitleva kaubanduslepingu üle (ELT 2010, C 147, lk 1, punkt 24) ja 10. mai 2010. aasta arvamuses järgmise õigusakti ettepaneku kohta: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust ja millega tunnistatakse kehtetuks raamotsus 2004/68/JSK (ELT 2010, C 323, lk 6, punkt 11).

********** Vt selle kohta kohtuotsus, 20.5.2003, Österreichischer Rundfunk (C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, punkt 68) ja kohtujuristi ettepanek, Kokott, kohtuasi Promusicae (C-275/06, EU:C:2007:454, punkt 51 jj).

57. Kuivõrd aga dünaamilise IP-aadressi abil – kas üksi või siis koos teiste andmetega – saab kindlaks määrata, kellele veebilehe külastamiseks kasutatud seade kuulub, võib seda aadressi kvalifitseerida teabeks „tuvastatava isiku“ kohta.**********

58. Bundesgerichtshofi (kõrgeim üldkohus) käsitusviisi kohaselt ainuüksi IP-aadressist ei piisa selleks, et tuvastada kasutajat, kes on sellelt aadressilt veebilehte külastanud. Kui internetiteenuse pakkuja saaks seevastu dünaamilise IP-aadressi kaudu kasutajat tuvastada, siis oleks kahtlemata tegu direktiivi 95/46 tähenduses isikuandmetega. See ei näi siiski olevat eelotsuse küsimuse mõte, sest küsimuse aluseks on, et põhikohtuasjasse kaasatud internetiteenuse pakkujad ei saa kasutajat ainult dünaamilise IP-aadressi järgi tuvastada.

59. Teiste andmetega kombineeritult hõlbustab dünaamiline IP-aadress kasutaja „kaudset“ tuvastamist, milles on kõik üksmeelel. Kas võimalus, et on olemas niisugused dünaamilise IP-aadressiga seostatavad lisaandmed, lubab seda aadressi automaatselt liigitada direktiivi tähenduses isikuandmeteks? Tuleks lahendada küsimus, kas selleks piisab pelgalt abstraktsest võimalusest, et need andmed on teada, või kas on vastupidi vaja, et need oleksid kättesaadavad isikule, kellel on dünaamiline IP-aadress juba teada, või kolmandale isikule.

60. Pooled keskendusid oma seisukohtades sellele, kuidas tõlgendada direktiivi 95/46 põhjendust 26, mille sisust nad rõhutasid väljendit „vahendeid, mida volitatud töötleja või keegi muu võib andmesubjekti tuvastamiseks tõenäoliselt kasutada“. Eelotsusetaotluse esitanud kohtu küsimus ei puuduta lisaandmeid, mis on põhikohtuasjasse kaasatud teenusepakkujate valduses. Selles ei ole silmas peetud ka kedagi kolmandat isikut, kellel oleks neid lisaandmeid (mille ühendamine dünaamilise IP-aadressiga võimaldaks kasutajat tuvastada), vaid võrguühenduse pakkujat.

61. Seepärast ei ole käesoleval juhul Euroopa Kohtul vaja analüüsida kõiki vahendeid, mida põhikohtumenetluse vastustaja võiks „tõenäoliselt“ kasutada selleks, et tema käsutuses olevaid dünaamilisi IP-aadresse võiks kvalifitseerida isikuandmeteks. Kuna Bundesgerichtshof (kõrgeim üldkohus) viitab ainult kolmanda isiku käsutuses olevatele lisaandmetele, võib sellest järeldada: a) et vastustajal ei ole asjakohaseid lisaandmed, millega saaks kasutajat tuvastada, b) või siis, et kui need andmed on talle kättesaadavad, ei saa ta neid tõenäoliselt sel otstarbel kasutada kui vastutav andmete töötleja direktiivi 95/46 põhjenduse 26 kohaselt.

62. Mõlemad juhud sõltuvad faktiliste asjaolude tuvastamisest, mis on ainult eelotsusetaotluse esitatud kohtu pädevuses. Euroopa Kohus võiks anda talle üldkriteeriumid väljendi „vahendeid, mida volitatud töötleja võib tõenäoliselt kasutada“ tõlgendamiseks juhul, kui Bundesgerichtshofil (kõrgeim üldkohus) on kahtlusi selles suhtes, kas vastustaja võib tõenäoliselt kasutada oma lisaandmeid. Kui see nii ei ole, ei ole minu arvates kohane, et Euroopa Kohus märgiks siin tõlgendamiskriteeriumid, mis ei ole eelotsusetaotluse esitanud kohtu jaoks tingimata vajalikud ja mida ta ei ole ka taotlenud.

63. Esitatud küsimuse tuum on aga, kas dünaamiliste IP-aadresside isikuandmeteks kvalifitseerimiseks on oluline asjaolu, et konkreetsel kolmandal isikul (internetiühenduse pakkujal) on lisaandmeid, mis nende aadressidega kombineeritult võimaldavad teatud kindlat veebilehte külastanud kasutajat tuvastada.

********** Kui ei ole tõendatud teisiti, tuleb eeldada, et nimetatud isik ongi see, kes on internetti lehitsenud ja vastavat veebilehte külastanud. Ent isegi kui viimati nimetatud eeldus kõrvale jätta, võimalaks teave veebilehe külastuse kuupäeva, kellaaja ja numbrilise lähtekoha kohta siduda seda külastust seadme omanikuga ja seostada seda kaudselt tema võrgukäitumisega. Mõeldavaks erandiks oleksid niisuguste lokaalide arvutitele eraldatud IP-aadressid nagu internetikohvikud, mille anonüümseid kasutajaid ei saa lõppkokkuvõttes tuvastada ja mille omanike kohta isiklikult ei anna kasutuskohas toimunud liiklus mingisugust olulist teavet. See on pealegi ainus erand põhimõttest, et IP-aadressid on isikuandmed, mida on direktiiviga 95/46 loodud töörühm üksikisikute kaitseks seoses isikuandmete töötlemisega (niinimetatud artikli 29 töörühm) lubanud teha. Võib lugeda tema 20. juuni 2007. aasta põhjendatud arvamust 4/2007 isikuandmete mõiste kohta, WP 136, kättesaadav aadressil http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

64. Taas on oluline märkida direktiivi 95/46 põhjendust 26. Väljend „vahendeid, mida […] keegi muu võib tõenäoliselt kasutada“ ********** võiks anda alust tõlgendada seda nii, et selleks, et mõelda, et dünaamilised IP-aadressid on iseenesest isikuandmed, piisab sellest, kui kellelgi kolmandal isikul on võimalik saada lisaandmeid (mida saab kombineerida dünaamilise IP-aadressiga selleks, et isikut tuvastada).

65. Selle maksimalistliku tõlgenduse põhjal võiks praktikas liigitada isikuandmeteks igat tüüpi teavet, kui tahes ebapiisav see iseenesest ka ei oleks selleks, et võimaldada kasutaja tuvastamist. Kunagi ei saaks täie kindlusega välistada võimalust, et võib leiduda keegi, kellel on lisaandmeid, mida saab selle teabega kombineerida ja mille abil saab järelikult isiku samasust kindlaks teha.

66. Minu arvates on võimaluse tõttu, et tehnika areng muudab üha keerukamate teabe saamise ja töötlemise vahendite kasutusviisid lähemas või kaugemas tulevikus tunduvalt hõlpsamaks, põhjendatud ettevaatusabinõud, millega püütakse ette näha eraelu puutumatuse kaitse. Andmekaitse kohaldamisalasse kuuluvate juriidiliste kategooriate määratlemisel on püütud hõlmata piisavalt ulatuslikke ja paindlikke tegevusjuhtusid, et need hõlmaksid kõiki mõeldavaid juhtusid. **********

67. Arvan siiski, et sellest – pealegi igati põhjendatud – hoolest kantuna ei tohi eirata õigusnormides seadusandja väljendatud tahet ja et direktiivi 95/46 põhjenduse 26 süstemaatiline tõlgendamine taandub „vahenditele, mida võivad tõenäoliselt kasutada“ teatavad kolmandad isikud.

68. Nii nagu põhjenduses 26 ei ole viidatud vahenditele, mida võib vastutav töötleja (siinsel juhul internetiteenuse pakkuja) kasutada, vaid ainult neile, mida ta võib „tõenäoliselt“ kasutada, tuleb ka mõista, et seadusandja peab silmas „kolmandaid isikuid“, kelle poole võib samuti tõenäoliselt pöörduda vastutav töötleja, kes soovib saada tuvastamiseks lisaandmeid. See ei ole nii, kui nende kolmandate isikute poole pöördumine on tegelikkuses inimressursside poolest ja majanduslikult väga kulukas või praktiliselt teostamatu või seadusega keelatud. Vastasel juhul oleks – nagu ma eespool märkisin – ühtedel ja teistel vahenditel praktiliselt võimatu vahet teha, sest alati oleks mõeldav, et on kolmandaid isikuid, kellel on – kui tahes kättesaamatud need ka internetiteenuse pakkujale ei oleks – nüüd või tulevikus asjaomaseid lisaandmeid, mille abil saaks kasutajat tuvastada.

69. Nagu ma märkisin, on Bundesgerichtshofi (kõrgeim üldkohus) nimetatud kolmas isik võrguühenduse pakkuja. Tema on kindlasti see kõige tõenäolisem mõeldav isik, kelle poole teenusepakkuja pöördub selleks, et saada vajalikke lisaandmeid, kui ta tahab kõige tõhusamalt, praktiliselt ja otseselt tuvastada tema veebilehte külastanud kasutajat dünaamilise IP-aadressi abil. See ei ole mingil juhul tundmatu ja kättesaamatu hüpoteetiline kolmas isik, vaid põhiline internetivõrgustiku peategelane, kelle kohta on täpselt teada, et tal on andmed, mida on teenusepakkujal vaja kasutaja tuvastamiseks. Tegelikult, nagu selgitab eelotsusetaotluse esitanud kohus, just selle konkreetse kolmanda isiku poole kavatsebki põhikohtuasja vastustaja pöörduda, et saada talle tingimata vajalikke lisaandmeid.

70. Internetiühenduse pakkuja ongi tüüpiliselt see direktiivi 95/46 põhjenduses 26 mõeldud kolmas isik, kelle poole võib põhikohtuasja teenusepakkuja kõige „tõenäolisemalt“ pöörduda. Jääb siiski veel välja selgitada, kas selle kolmanda isiku valduses olevate lisaandmete hankimist võib kvalifitseerida „tõenäoliselt“ praktikas teostatavaks.

********** Originaalis kursiivita.

********** Sellest ettevaatusest ja ennetamisest on juhindunud oma hoiakus artikli 29 töörühm, kelle seisukoht on, nagu ma märkisin, et tuleb lähtuda põhimõttest, et IP-aadressid on isikuandmed, millest ainsaks lubatud erandiks on juhud, kus teenusepakkuja saab täie kindlusega kindlaks määrata, et need on tuvastatavate isikute aadressid, nagu võivad olla internetikohviku kasutajad. Vt märkus 16, *in fine*.

71. Saksamaa valitsus väidab, et kuna internetiühenduse pakkuja valduses olevad andmed on isikuandmed, ei saa see neid anda automaatselt, vaid ainult vastavuses isikuandmete töötlemist reguleerivate õigusnormidega.**********

72. Kahtlemata see nii on, sest selle teabe saamiseks tuleb järgida isikuandmete suhtes kehtivaid õigusakte. Teavet võib „tõenäoliselt“ saada ainult siis, kui on täidetud seda laadi andmetega tutvumiseks kehtestatud tingimused, millest esimene on nende säilitamise ja teistele edastamise seaduslik võimalus. On kindel, et internetiühenduse pakkujal on õigus asjaomaste andmete avaldamisest keelduda, kuid võimalik on ka vastupidine. Ainuüksi andmete edastamise võimalus, mis on täiesti „tõenäoline“, muudab dünaamilised IP-aadressid direktiivi 95/46 põhjenduse 26 kohaselt internetiteenuse pakkuja jaoks isikuandmeteks.

73. See on seaduse raames teostatav ja seepärast „tõenäoline“ võimalus. Direktiivis 95/46 nimetatud tõenäolised andmetega tutvumise vahendid peavad olema põhimõtteliselt õiguspärased vahendid.********** Saksamaa valitsus tuletab meelde, et eelotsusetaotluse esitanud kohus lähtub sellisest eeldusest, nagu ongi loomulik.********** Sel viisil vähendatakse õiguslikult asjassepuutuvaid andmetega tutvumise viise märgatavalt, sest need peavad olema eranditult õiguspärased. Kui need aga olemas on, siis on need direktiivi 95/46 tähenduses „tõenäoline vahend“, vaatamata sellele, kui piiravad need ka praktikas ei oleks.

74. Järelikult arvan ma, et Bundesgerichtshofi (kõrgeim üldkohus) esimesele küsimusele tema esitatud sõnastuses tuleb vastata jaatavalt. Dünaamilised IP-aadressid tuleb liigitada internetiteenuse pakkuja jaoks isikuandmeteks, arvestades et on kolmas isik (võrguühenduse pakkuja), kelle poole võib tõenäoliselt pöörduda, et saada muid lisaandmeid, mille abil saab koostoimes selle aadressiga kasutajat tuvastada.

75. Ma leian, et tulemus, mille annaks minu pakutule vastupidine lahendus, kinnitab seda lahendust. Kui dünaamilised IP-aadressid ei oleks internetis teenusepakkuja jaoks isikuandmed, võiks see neid säilitada määramata ajaks ja võiks taotleda igal ajal internetiühenduse pakkujalt lisaandmeid, et kombineerida neid selle aadressiga ja kasutajat tuvastada. Nendel asjaoludel, nagu möönab Saksamaa valitsus,********** muutuvad dünaamilised IP-aadressid isikuandmeteks, kui tal juba oleks lisaandmeid, millega saab kasutajat tuvastada, ning selle suhtes kehtivad andmekaitse õigusaktid.

76. Tegu on tema sõnul aga andmetega, mida oleks võimalik säilitada ainult sel juhul, kui neid ei oleks seni peetud teenusepakkuja jaoks isikuandmeteks. Sel viisil jääks viimase otsustada dünaamiliste IP-aadresside õiguslik kvalifitseerimine isikuandmeteks, mis sõltub võimalusest, et ta otsustab tulevikus neid kasutada kasutaja tuvastamiseks nende aadresside kombineerimise teel lisaandmetega, mida tuleb hankida kolmandalt isikult. Minu arvates on aga direktiivi 95/46 kohaselt määrav – tõenäoline – võimalus, et on kolmas isik, „kelle poole saab pöörduda“ ja kellel on vajalikud vahendid, millega saab isikut tuvastada, mitte see, et see kolmanda isiku poole pöördumise võimalus tegelikult realiseerub.

77. Võiks koguni möönda koos Saksamaa valitsusega, et dünaamilised IP-aadressid muutuvad isikuandmeteks alles siis, kui internetiühenduse pakkuja need kätte saab. Sel juhul tuleks aga tunnistada, et selline kvalifitseerimine tuleb teha tagasiulatuvalt, arvestades IP-aadressi säilitamise tähtaega, ja järelikult seda, et seda aadressi ei tohi enam alles olla, kui lõpeb aeg, mille vältel seda oleks lubatud säilitada, kui see oleks kvalifitseeritud isikuandmeteks algusest peale. See annaks tulemuse, mis on vastuolus isikuandmete kaitse õigusaktide mõttega. Nende andmete üksnes ajutise

********** Tema kirjalike seisukohtade punktid 40 ja 45.

********** Selles kontekstis ei oma tähtsust, et isikuandmeid on *de facto* võimalik kätte saada andmekaitseseadusi rikkudes.

********** Tema kirjalike seisukohtade punktid 47 ja 48.

********** Tema kirjalike seisukohtade punkt 36.

säilitamise põhjusest hiilitaks kõrvale, kui võidaks viivitada nendele andmetele algusest peale omase omaduse kindlakstegemisega, st et neid saab kasutada – kas üksi või koos teiste andmetega – füüsilise isiku tuvastamise vahendina. Ka seepärast on puhtalt ökonoomsuse huvides mõistlikum omistada neile see omadus algusest peale.

78. Seepärast leian esimese järeldusena, et direktiivi 95/46 artikli 2 punkti a tuleb tõlgendada nii, et IP-aadress, mida teenusepakkuja säilitab seoses veebilehe külastamisega, on tema jaoks isikuandmed, kuivõrd võrguühenduse (internet) pakkujal on lisaandmeid, mille abil saab andmesubjekti tuvastada.

B. *Teine küsimus*

79. Oma teise eelotsuse küsimusega soovib Bundesgerichtshof (kõrgeim üldkohus) teada, kas direktiivi 95/46 artikli 7 punktiga f on vastuolus liikmesriigi õigusnorm, millega on lubatud koguda ja kasutada kasutaja isikuandmeid ilma tema nõusolekuta ainult siis, kui see on vajalik konkreetse sideteenuse pakkumiseks ja selle kasutajale selle eest arve esitamiseks, ilma et eesmärk tagada teenuse toimimine võiks õigustada nende andmete kasutamist pärast iga side lõppu.

80. Enne vastamist tuleb märkida, et Bundesgerichtshof (kõrgeim üldkohus) täpsustas, et vaidlusaluseid andmeid säilitatakse selleks, et tagada põhikohtuasjas arutamisel olevate internetisaitide nõuetekohane toimimine, võimaldades vajaduse korral kriminaalvastutusele võtmist nende saitide vastu toime pandud küberrünnakute eest.

81. Seega tuleb kõigepealt välja selgitada, kas eelotsusetaotluses nimetatud IP-aadresside töötlemine kuulub direktiivi 95/46 artikli 3 lõike 2 esimeses taandes ette nähtud erandi alla.**********

1. Direktiivi 95/46 kohaldatavus vaidlusaluste andmete töötlemisele

82. Saksamaa Liitvabariik tegutseb põhikohtuasjas, nagu näib, üksnes internetiteenuse pakkujana, see tähendab eraõigusliku isikuna (ja seega sine imperio). Sellest järeldub, et põhimõtteliselt ei ole selle kohtuvaidluse esemeks olevate andmete töötlemine direktiivi 95/46 kohaldamisalast välja jäetud.

83. Euroopa Kohus märkis kohtuotsuses Lindqvist,********** et direktiivi 95/46 artikli 3 lõikes 2 ette nähtud tegevused kujutavad „endast igal juhul toiminguid, mis on iseloomulikud riigile või riigi ametiasutustele, ega ole omased eraõiguslike isikute tegevusvaldkondadele“ ********** . Kuivõrd vaidlusaluste andmete vastutav töötleja on isik, kes vaatamata oma riigivõimu staatusele, tegutseb tegelikult eraisikuna, on direktiiv 95/46 kohaldatav.

84. Märkides, mis on Saksamaa administratsiooni põhieesmärk dünaamiliste IP-aadresside salvestamisel, rõhutab eelotsusetaotluse esitanud kohus, et see „on vajalik elektrooniliste teabe- ja sideteenuste turvalisuse ja töökindluse säilitamiseks ja tagamiseks“; eelkõige „sagedasti esinevate Denial-of-Service (teenuse tõkestamise rünne, edaspidi „DDoS“) rünnete äratundmise ja tõrjumise [edendamiseks], mille puhul blokeeritakse massiliste päringutega elektroonilise side infrastruktuur, suunates need päringud sihilikult ja koordineeritult üksikuile veebiservereile“.********** Dünaamiliste IP-aadresside säilitamine sel otstarbel on ühine kõikidele teatud tähtsusega veebisaitide omanikele ja see ei eelda otseselt ega kaudselt avaliku võimu teostamist, mistõttu ei tekita ülemääraseid raskusi arvata see direktiivi 95/46 kohaldamisalasse.

********** Direktiivi 95/46 kohaldamisalasse ei kuulu „töötlemi[n]e […], mis on seotud avaliku korra, riigikaitse, riigi julgeoleku […] ja *riigi toimingutega kriminaalõiguse valdkonnas*“ (originaalis kursiivita).

********** Kohtuotsus, 6.11.2003 (C-101/01, EU:C:2003:596, punkt 43).

********** Samas väljenduses kohtuotsus, 16.12.2008, Satakunnan Markkinapörssi ja Satamedia (C-73/07, EU:C:2008:727, punkt 41).

********** Eelotsusetaotluse esitamise kohtumääruse punkt 36.

85. Bundesgerichtshof (kõrgeim üldkohus) kinnitab siiski, et põhikohtuasja kaasatud teenusepakkujad säilitavad dünaamilisi IP-aadresse ka selleks, et vajaduse korral algatada kriminaalasi võimalike küberrünnakute toimepanijate vastu. Kas see tegevuse eesmärk on piisav selleks, et nende andmete töötlemine direktiivi 95/46 kohaldamisalast välja jätta?

86. Minu arvates, kui „kriminaalasja“ all mõistetakse riigi ius puniendi teostamist põhikohtuasjas vastustajateks olevate teenusepakkujate poolt, siis oleks tegu „riigi toimingutega kriminaalõiguse valdkonnas“ ja seega ühega direktiivi 95/46 artikli 3 lõike 2 esimeses taandes ette nähtud eranditest.

87. Nendel asjaoludel on Euroopa Kohus kohtuasjas Huber********** välja kujundanud doktriini, mille kohaselt kuulub isikuandmete töötlemine teenusepakkujate poolt nende sideteenuste turvalisuse ja tehnilise toimivuse eesmärkidel direktiivi 95/46 kohaldamisalasse, samas kui andmete töötlemine riigi tegevuses kuritegevuse vastu võitlemise eesmärgil jääb sellest välja.

88. Kuigi otseses mõttes kriminaalmenetluse algatamine ei ole Saksamaa Liitvabariigi kui pelgalt valitsusvõimuta teenusepakkuja pädevuses, kes, nagu iga eraõiguslik isik, üksnes edastab vaidlusalused IP-aadressid riigiorganile sunnimeetmete rakendamiseks, on sarnaselt ka dünaamiliste IP-aadresside töötlemise eesmärgiks tegevus, mis jääb direktiivi 95/46 kohaldamisalast välja.

89. Nii tuleneb kohtupraktikast, mis sedastati kohtuasjas parlament vs. nõukogu ja komisjon,********** milles Euroopa Kohus kinnitas, et asjaolu, et teatavaid isikuandmeid koguvad „eraõiguslikud ettevõtjad […] kommertseesmärgil ning just nemad korraldavad nende edastamist kolmandasse riiki“, ei tähenda, et see edastamine „ei kuulu“ direktiivi 95/46 artikli 3 lõike 2 esimese taande „kohaldamisalasse“, kui edastamise eesmärgiks on riigi toimingud kriminaalõiguse valdkonnas, tingimusel et sel juhul see „toimub sellises ametivõimude poolt loodud raamistikus, mille eesmärk on tagada riigi julgeolek“.**********

90. Kui seevastu, nagu ma arvan, tuleb „kriminaalmenetluse“ all mõista, nagu nähtub eelotsusetaotlusest, seda, mis on omane eraõiguslikule isikule kui vastava menetluse abil riigi ius puniendi algatamist nõudma õigustatud subjektile, siis ei saa väita, et dünaamiliste IP-aadresside töötlemise eesmärk on riigi toimingud kriminaalõiguse valdkonnas, mis on direktiivi 95/46 kohaldamisalast välja jäetud.

91. Nimelt kasutataks nende andmete säilitamist ja salvestamist veel ühe tõendusvahendina, millega veebilehe omanik saab riigilt taotleda poole algatusel õigusvastase tegevuse karistamist. See oleks lõppkokkuvõttes vahend, mille abil kaitsta õiguskorras eraõiguslikule õigussubjektile (sel juhul avalik-õiguslikule isikule, kes tegutseb eraõiguse korras) antud õigusi kriminaalmenetluse teel. Sellest aspektist ei erine see mis tahes muu internetiteenuse pakkuja algatusest, kes taotleb riigi kaitset õiguskorras kriminaalasja algatamiseks kehtestatud menetluse alusel.

92. Järelikult, kuna Saksamaa administratsioon toimib internetiteenuse pakkujana, kellel ei ole riigivõimu – mida tuleb hinnata eelotsusetaotluse esitanud kohtul –, kuulub dünaamiliste IP-aadresside kui isikuandmete tema poolt töötlemine direktiivi 95/46 kohaldamisalasse.

********** Kohtuotsus, 16.12.2008 (C-524/06, EU:C:2008:724, punkt 45).

********** Kohtuotsus, 30.5.2006 (C-317/04 ja C-318/04, EU:C:2006:346, punktid 54–59.

********** *Ibidem*, punkt 59. See puudutas isikuandmeid, mille töötlemine ei olnud vajalik nende teenuste osutamiseks, milles seisnes asjaomaste eraõiguslike ettevõtjate (lennukompaniid) äritegevus, kuid mida nad olid kohustatud edastama Ameerika Ühendriikide ametivõimudele terrorismi ennetamiseks ja selle vastu võitlemiseks.

2. Sisulised küsimused

93. TMG § 15 lõikes 1 on lubatud kasutaja isikuandmeid koguda ja kasutada ainult juhul, kui see on tingimata vajalik konkreetse sideteenuse kasutuse võimaldamiseks ja arve esitamiseks. Täpsemalt võib teenusepakkuja koguda ja kasutada ainult niinimetatud „kasutusandmeid“, see tähendab kasutaja isikuandmeid, mis on tingimata vajalikud „elektrooniliste teabe- ja sideteenuste konkreetse kasutuselevõtu võimaldamiseks“. Need andmed tuleb pärast side lõppu kustutada (see tähendab, kui sideteenuse konkreetne kasutus lõpeb), välja arvatud juhul, kui neid tuleb säilitada „arve esitamiseks“, nagu on sätestatud TMG sama § 15 lõikes 4.

94. Näib, et TMG §-ga 15 on välistatud pärast side lõppu kasutusandmete säilitamine muul otstarbel; ka mitte selleks, et tagada „sideteenuste kasutuselevõtt“ üldiselt. Kuna selles õigusnormis on nimetatud andmete säilitamise põhjenduseks ainult arvete esitamist, võiks seda TMG sätet mõista (kuigi selle lõplik tõlgendamine on eelotsusetaotluse esitanud kohtu ülesanne), nagu nõuaks see, et kasutusandmeid kasutatakse ainult selleks, et võimaldada konkreetset sidet, ja et need andmed tuleb pärast selle side lõppu kustutada.

95. Direktiivi 95/46 artikli 7 punktiga f********** on lubatud isikuandmete töötlemine tingimustel, mida ma nimetaksin (vastutava töötleja jaoks) heldemateks kui TMG § 15 sõna-sõnalises sisus ette nähtud tingimused. Saksa õigusnormi võib selles aspektis pidada piiravamaks kui liidu oma, sest selles ei ole põhimõtteliselt ette nähtud muu õiguspärane huvi kui teenuse eest arvete esitamisega seonduv huvi, nii et Saksamaa Liitvabariigil võiks internetiteenuste pakkujana olla ka õiguspärane huvi tagada oma veebilehtede nõuetekohane toimimine, mis läheb kaugemale igast kasutussuhtest.**********

96. Euroopa Kohtu doktriinis on antud juhised teisele eelotsuse küsimusele vastamiseks kohtuotsuses ASNEF ja FECEMD********** . Selles kinnitas Euroopa Kohus, et direktiivi 95/46 eesmärgist „tuleneb […], et direktiivi 95/46 artikkel 7 näeb ette ammendava ja piirava loetelu juhtudest, millal isikuandmete töötlemist võib pidada seaduslikuks“.********** Sellest tuleneb, et „liikmesriigid ei saa lisada direktiivi 95/46 artiklile 7 uusi isikuandmete töötlemise seaduslikkust puudutavaid kriteeriume ega kehtestada täiendavaid nõudeid, mis muudavad selles artiklis sätestatud kuuest kriteeriumist mõne kriteeriumi ulatust“.**********

97. TMG § 15 ei lisa võrreldes direktiivi 95/46 artiklis 7 nimetatuga andmete töötlemise seaduslikkuse kohta täiendavat nõuet – nagu see oli kohtuasjas ASNEF ja FECEMD,********** kuid selle kitsas tähenduses tõlgendamisel, millele viitab eelotsusetaotluse esitanud kohus, piirab see nimetatud sätte punktis f vaadeldud tingimuse sisu: seal, kus liidu seadusandja viitab üldiselt vajaduse korrale „[…] vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huvide elluviimiseks“, täidab TMG § 15 ainult vajadust „elektrooniliste teabe- ja sideteenuste [konkreetse] kasutuselevõtu võimaldamiseks ja arve esitamiseks“.

********** Ära toodud punktis 17.

********** Vt punkt 84. Mõistagi on veebilehtede omanikel õiguspärane huvi ennetada eelotsusetaotluse esitanud kohtu nimetatud teenuse tõkestamise juhtusid („denials of service“), see tähendab massilisi rünnakuid, mida mõnikord korraldatakse kokkumängus mõne veebisaidi vastu, et neid üle koormata ja need rivist välja viia, ning niisuguste rünnakute vastu võidelda.

********** Kohtuotsus, 24.11.2011 (C-468/10 ja C-469/10, EU:C:2011:777).

********** *Ibidem*, punkt 30.

********** *Ibidem*, punkt 32.

********** Juhtum, kus siseriikliku õigusaktiga lisati direktiivi 95/46 artikli 7 punkti f nõuetele nõue, et töödeldavad andmed oleksid esitatud üldsusele kättesaadavates allikates.

98. Nii nagu kohtuasjas ASNEF ja FECEMD,********** siis ka selles kohtuasjas käsitletud siseriiklik meede – jällegi, kui seda tõlgendada eespool selgitatud kitsas tähenduses – pigem muudab direktiivi 95/46 artikli 7 ühe põhimõtte ulatust, mitte ei piirdu selle täpsustamisega, kuigi see on ainus, milleks on iga liikmesriigi ametivõimudel vastavalt direktiivi 95/46 artiklile 5 teatav hindamisruum.

99. Viimati nimetatud sätte kohaselt nimelt „[k]uivõrd see on lubatud käesoleva peatüki sätetega,[**********] määravad liikmesriigid täpsemalt kindlaks tingimused, mille puhul isikuandmete töötlemine on seaduslik“. Nagu aga kinnitati kohtuasjas ASNEF ja FECEMD,********** „liikmesriigid ei saa [nimetatud sätte] alusel kehtestada ka muid isikuandmete töötlemise seaduslikkust puudutavaid kriteeriume kui neid, mis on sätestatud selle direktiivi artiklis 7, ega muuta täiendavate nõuetega nimetatud artiklis 7 sätestatud kuue kriteeriumi ulatust“.

100. Näib, et TMG § 15 piirab direktiivi 95/46 artikli 7 punktiga f võrreldes oluliselt andmete töötlemise põhjendamiseks olulise õiguspärase huvi ulatust, mitte ei piirdu ainult selle täpsustamise või selgitamisega sama direktiivi artikliga 5 lubatud piires. Lisaks teeb see paragrahv seda selgelt ja absoluutselt, lubamata, et sideteenuse üldise kasutuselevõtu kaitset ja tagamist võiks kaaluda direktiivi 95/46 „artikli 1 lõike 1 kohaselt kaitstavate andmesubjekti põhiõiguste ja -vabadustega seotud huvid[ega]“, nagu on ette kirjutatud selle direktiivi artikli 7 punktis f.

101. Lõppkokkuvõttes on nii nagu kohtuasjas ASNEF ja FECEMD********** Saksa riiklik seadusandja näinud „[teatavate isikuandmekategooriate suhtes] lõplikult ette vastanduvate õiguste ja huvide kaalumise tulemuse, ilma et lubatud oleks konkreetse juhtumi erilistest asjaoludest lähtuv teistsugune tulemus“, nii et „[enam ei ole tegemist direktiivi 95/46] artikli 5 tähenduses täpsustamisega“.

102. Nendel asjaoludel olen arvamusel, et Bundesgerichtshof (kõrgeim üldkohus) on kohustatud tõlgendama siseriiklikku õigusakti kooskõlas direktiiviga 95/46, mis eeldab: a) et niinimetatud „kasutusandmete“ töötlemist põhjendavate aluste hulka võib arvata sideteenusepakkuja õiguspärase huvi kaitsta nende teenuste üldist kasutuselevõttu ja b) et seda teenusepakkuja huvi võib kaaluda ad casum, kõrvutades seda kasutaja huvi või põhiõiguste ja -vabadustega, et välja selgitada, mis peab väärima direktiivi 95/46 artikli 1 lõike 1 kohaselt kaitset.**********

103. Minu arvates ei tule midagi rohkem lisada selle kohta, millistel tingimustel tuleb seda kaalumist teha asjas, milles on esitatud eelotsusetaotlus. Selle konkreetse aspekti kohta ei küsi Bundesgerichtshof (kõrgeim üldkohus) midagi, vaid ta muretseb sellele kaalumisotsusele eelneva küsimuse lahenduse pärast; nimelt, kas nimetatud otsust võib teha.

104. Lõpuks näib ülearune märkida, et eelotsusetaotluse esitanud kohus võib võtta arvesse võimalikke õigusnorme, mille on liikmesriik vastu võtnud seoses direktiivi 95/46 artikli 13 lõike 1 punktis d sisalduva loaga vähendada sama direktiivi artiklis 6 ette nähtud kohustuste ja õiguste ulatust, kui see on vajalik selleks et tagada muude hüvede hulgas „kuritegude […] ennetamine, uurimine, avastamine ja nende eest vastutuselevõtmine“. Ka seda aspekti eelotsusetaotluse esitanud kohus ei puuduta, olles nende mõlema artikli olemasolust kahtlemata teadlik.

********** Kohtuotsus, 24.11.2011 (C-468/10 ja C-469/10, EU:C:2011:777).

********** II peatükk pealkirjaga „Üldised eeskirjad isikuandmete töötlemise seaduslikkuse kohta“, mis hõlmab direktiivi 95/46 artikleid 5–21.

********** Kohtuotsus, 24.11.2011 (C-468/10 ja C-469/10, EU:C:2011:777, punkt 36).

********** *Ibidem*, punkt 47.

********** Kohtuistungil lükkas P. Breyeri kaitsja tagasi väite, et dünaamiliste IP-aadresside salvestamine oleks vajalik internetiteenuste nõuetekohase toimimise kaitsmiseks võimalike rünnakute korral. Ma ei usu, et võiks anda absoluutset vastust sellisele probleemile, mille lahendusele peab, vastupidi, eelnema igal üksikjuhul veebisaidi omaniku huvi ja kasutajate õiguste ja huvide kõrvutamine.

105. Järelikult pakun teisele eelotsuse küsimusele vastuseks, et direktiivi 95/46 artikli 7 punktiga f on vastuolus siseriiklik õigusnorm, mille tõlgendamine takistab teenusepakkujal koguda ja töödelda sideteenuse toimimise tagamise eesmärgil pärast iga side lõppu kasutaja isikuandmeid ilma tema nõusolekuta.

VI. **Ettepanek**

106. Eespool märgitu alusel teen Euroopa Kohtule ettepaneku vastata esitatud küsimustele järgmiselt:

1. Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta artikli 2 punkti a kohaselt on dünaamilised IP-aadressid, mille abil kasutaja külastab sideteenusepakkuja veebilehte, viimase jaoks „isikuandmed“, kuivõrd võrguühenduse pakkujal on muid lisaandmeid, mis dünaamilise IP-aadressiga koostoimes võimaldavad kasutajat tuvastada.

2. Direktiivi 95/46 artikli 7 punkti f tuleb tõlgendada nii, et eesmärki tagada sideteenuse toimimine võib põhimõtteliselt pidada nende isikuandmete töötlemist põhjendavaks õiguspäraseks huviks, mille puhul tuleb hinnata, kas see kaalub üles kasutaja huvi või põhiõigused. Siseriiklik õigusnorm, millega ei ole lubatud seda õiguspärast huvi arvesse võtta, oleks viidatud artikliga vastuolus.