Oikeustapauskokoelma

JULKISASIAMIEHEN RATKAISUEHDOTUS
MANUEL CAMPOS SÁNCHEZ-BORDONA
12 päivänä toukokuuta 2016 [1]

Asia C-582/14

Patrick Breyer
vastaan
Saksan liittotasavalta

(Ennakkoratkaisupyyntö – Bundesgerichtshof (liittovaltion ylin tuomioistuin, Saksa))

Henkilötietojen käsittely — Direktiivi 95/46/EY — 2 artiklan a alakohta ja 7 artiklan f alakohta — Henkilötietojen käsite — IP-osoitteet — Sähköisiä viestintäpalveluita tarjoavan toimijan harjoittama tietojen säilyttäminen — Kansallinen säännöstö, jonka perusteella ei voida ottaa huomioon rekisterinpitäjän tavoittelemaa oikeutettua intressiä

1. Internetprotokollaosoite, jäljempänä IP-osoite, on laitteelle (tietokoneelle, tabletille, älypuhelimelle) annettava binaarilukujen sarja, joka yksilöi kyseisen laitteen ja sallii laitteen pääsyn sähköiseen tieto- ja viestintäverkkoon. Laitteen on käytettävä tätä verkkoyhteyden tarjoajan antamaa numerosarjaa verkkoyhteyden luomiseksi. IP-osoite välitetään palvelimelle, jolla käynnin kohteena oleva verkkosivu sijaitsee.

2. Verkkoyhteyden tarjoaja (yleensä puhelinyhtiö) antaa asiakkaalleen tilapäisesti jokaista verkkoyhteyttä varten niin kutsutun dynaamisen IP-osoitteen, joka vaihtuu toiseksi, kun asiakas ottaa verkkoyhteyden seuraavan kerran. Kyseisillä yhtiöillä on rekisteri, josta selviää tietylle laitteelle kullakin hetkellä annettu IP-osoite. [2]

3. Myös verkkosivujen haltijat, joiden sivuilla käydään dynaamisten IP-osoitteiden kautta, ylläpitävät yleensä rekistereitä siitä, millä sivuilla on vierailtu, mihin aikaan ja mistä dynaamisesta IP-osoitteesta. Tällaisia rekistereitä voidaan säilyttää tekniseltä kannalta rajoittamattoman ajan sen jälkeen, kun käyttäjän verkkoyhteys on päättynyt.

4. Pelkkä dynaaminen IP-osoite ei riitä siihen, että palveluntarjoaja voisi tunnistaa verkkosivujensa käyttäjän. Sen sijaan se voisi tehdä näin, jos se yhdistäisi dynaamisen IP-osoitteen muihin lisätietoihin, joita verkkoyhteyden tarjoajalla on hallussaan.

1 — Alkuperäinen kieli: espanja.

2 — Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta 15.3.2006 annetun Euroopan parlamentin ja neuvoston direktiivin 2006/24/EY (EUVL 2006 L 105, s. 54) 5 artiklassa säädetään muiden velvollisuuksien ohella seuraavien tietoluokkien säilyttämisestä vakavaksi rikollisuudeksi määritellyn rikollisuuden tutkintaa, selvittämistä ja syyteharkintaa varten: ”Internet-yhteyspalvelun alkamisen ja päättymisen päivämäärät ja kellonajat – –, Internet-palvelun tarjoajan liittymälle osoittama dynaaminen tai staattinen Internet-protokollaosoite (IP-osoite) sekä tilaajan tai rekisteröidyn käyttäjän käyttäjätunnus”.

5. Riidan kohteena on se, ovatko dynaamiset IP-osoitteet direktiivin 95/46/EY [3] 2 artiklan a alakohdassa tarkoitettuja henkilötietoja. Asian ratkaisemiseksi on selvitettävä ensin, mikä merkitys tässä yhteydessä on sillä seikalla, että käyttäjän tunnistamiseksi tarvittavat lisätiedot eivät ole verkkosivuston haltijan vaan sivullisen (tässä tapauksessa verkkoyhteyden tarjoajan) hallussa.

6. Unionin tuomioistuin ei ole käsitellyt tätä kysymystä aiemmin, vaikka se on todennut tuomion Scarlet Extended [4] 51 kohdassa, että IP-osoitteet ”ovat suojattuja henkilötietoja, koska niiden avulla mainitut käyttäjät on mahdollista tunnistaa täsmällisesti”, mutta kyseisessä asiayhteydessä IP-osoitteet oli kerännyt ja tunnistanut verkkoyhteyden tarjoaja, [5] ei sisällöntarjoaja, kuten nyt käsiteltävässä tapauksessa.

7. Jos dynaamiset IP-osoitteet ovat verkkoyhteyden tarjoajan kannalta henkilötietoja, sen jälkeen on tutkittava, kuuluuko niiden käsittely direktiivin 95/46 soveltamisalaan.

8. On mahdollista, että vaikka kyseiset tiedot olisivat henkilötietoja, ne eivät saa direktiiviin 95/46 perustuvaa suojaa, esimerkiksi jos niiden käsittelyn tarkoitus olisi rikosoikeudellisen menettelyn käyttäminen mahdollisia verkkosivulle hyökänneitä vastaan. Tällöin direktiiviä 95/46 ei sovelleta sen 3 artiklan 2 kohdan ensimmäisen luetelmakohdan mukaisesti.

9. Lisäksi on selvitettävä, käyttääkö palveluntarjoaja (tässä tapauksessa Saksan liittotasavalta), joka tallentaa dynaamiset IP-osoitteet verkkosivuilleen suuntautuvan käynnin yhteydessä, viranomaisen ominaisuudessa vai toimiiko se tällöin yksityisenä toimijana.

10. Jos direktiiviä 95/46 sovelletaan, on vielä selvitettävä, miten pitkälti sen 7 artiklan f alakohdan kanssa on yhteensopiva sellainen kansallinen säännöstö, jossa rajoitetaan yhtä mainitussa alakohdassa säädetyistä edellytyksistä, joiden perusteella henkilötietoja voidaan käsitellä.

I Asiaa koskevat oikeussäännöt

A *Unionin oikeus*

11. Direktiivin 95/46 johdanto-osan 26 perustelukappaleen sanamuoto on seuraava:

”26) tietosuojaa koskevia periaatteita on sovellettava kaikkiin tunnistettua tai tunnistettavissa olevaa henkilöä koskeviin tietoihin; sen määrittämiseksi, onko henkilö tunnistettavissa, olisi otettava huomioon kaikki kohtuullisesti toteutettavissa olevat keinot, joita joko rekisterinpitäjä tai joku muu voi kyseisen henkilön tunnistamiseksi käyttää; tietosuojaa koskevia periaatteita ei sovelleta tietoihin, jotka on tehty anonyymeiksi siten, ettei rekisteröity enää ole tunnistettavissa; 27 artiklassa tarkoitettuja käytännesääntöjä voidaan käyttää ohjeena, kun pohditaan keinoja tietojen anonyymeiksi tekemistä varten ja niiden säilyttämiseksi muodossa, josta rekisteröidyn henkilöllisyys ei käy ilmi.”

12. Direktiivin 95/46 1 artiklassa säädetään seuraavaa:

”1. Tämän direktiivin mukaisesti jäsenvaltioiden on henkilötietojen käsittelyssä turvattava yksilöille heidän perusoikeutensa ja -vapautensa ja erityisesti heidän oikeutensa yksityisyyteen.

3 — Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annettu Euroopan parlamentin ja neuvoston direktiivi (EYVL 1995, L 281, s. 31).

4 — Tuomio 24.11.2011 (C-70/10, EU:C:2011:771, 51 kohta).

5 — Näin oli myös 19.4.2012 annetussa tuomiossa Bonnier Audio ym. (C-461/10, EU:C:2012:219, 51 ja 52 kohta).

2. Jäsenvaltiot eivät voi rajoittaa tai kieltää henkilötietojen vapaata liikkuvuutta jäsenvaltioiden välillä syistä, jotka liittyvät 1 kohdan mukaisesti turvattavaan suojaan.”

13. Direktiivin 95/46 2 artiklassa säädetään seuraavaa:

”Tässä direktiivissä tarkoitetaan

a) ’henkilötiedoilla’ kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä (’rekisteröity’) koskevia tietoja; tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa, erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella,

b) ’henkilötietojen käsittelyllä’ (’käsittely’) kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittaminen tai yhdistäminen sekä suojaaminen, poistaminen tai tuhoaminen,

– –

d) ’rekisterinpitäjällä’ luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot; jos käsittelyn tarkoitus ja keinot määritellään kansallisilla tai yhteisön laeilla tai asetuksilla, rekisterinpitäjä tai erityiset perusteet rekisterinpitäjän nimeämiseksi voidaan vahvistaa kansallisten tai yhteisön säännösten mukaisesti,

– –

f) ’sivullisella’ luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää,

– –”.

14. Direktiivin 95/46 3 artiklan otsikkona on ”Soveltamisala”, ja siinä säädetään seuraavaa:

”1. Tätä direktiiviä sovelletaan osittain tai kokonaan automatisoituun tietojenkäsittelyyn sekä sellaisten henkilötietojen manuaaliseen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

2. Tätä direktiiviä ei sovelleta henkilötietojen käsittelyyn,

— joka suoritetaan sellaisessa toiminnassa, joka ei kuulu yhteisön oikeuden soveltamisalaan, kuten toiminta, josta on määrätty Euroopan unionista tehdyn sopimuksen V ja VI osastossa, ja kaikissa tapauksissa käsittely, joka koskee yleistä turvallisuutta, puolustusta, valtion turvallisuutta (myös valtion taloudellista hyvinvointia, kun käsittelyoperaatio on sidoksissa valtion turvallisuutta koskeviin kysymyksiin) ja rikosoikeuden alalla tapahtuvaa valtion toimintaa,

– –”.

15. Direktiivin 95/46 II luvun otsikkona on ”Yleiset säännöt henkilötietojen käsittelyn laillisuudesta”, ja sen aloittavan 5 artiklan mukaan ”jäsenvaltioiden on määriteltävä henkilötietojen käsittelyn laillisuuden edellytykset tämän luvun säännösten rajoissa”.

16. Direktiivin 95/46 6 artiklassa säädetään seuraavaa:

”1. Jäsenvaltioiden on säädettävä siitä, että

a) henkilötietoja käsitellään asianmukaisesti ja laillisesti,

b) henkilötiedot kerätään tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä myöhemmin saa käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Myöhempää käsittelyä historiantutkimusta taikka tilastollisia tai tieteellisiä tarkoituksia varten ei pidetä yhteensopimattomana, sillä edellytyksellä, että jäsenvaltiot toteuttavat tarpeelliset suojatoimet,

c) henkilötietojen on oltava asianmukaisia ja olennaisia eivätkä ne saa olla liian laajoja suhteessa tarkoituksiin, mihin ne on kerätty ja missä niitä myöhemmin käsitellään;

d) henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä; on tehtävä kaikki mahdollinen sen varmistamiseksi, että niihin tarkoituksiin nähden virheelliset tai puutteelliset tiedot, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään, poistetaan tai oikaistaan,

e) henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan sen ajan, kuin on tarpeen niiden tarkoitusten toteuttamista varten, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään. Jäsenvaltiot toteuttavat niiden henkilötietojen tarpeelliset suojatoimet, joita säilytetään edellä tarkoitettua aikaa kauemmin historiantutkimusta taikka tilastollisia tai tieteellisiä tarkoituksia varten.

2. Rekisterinpitäjän on huolehdittava 1 kohdan noudattamisesta.”

17. Direktiivin 95/46 7 artiklassa säädetään seuraavaa:

”Jäsenvaltioiden on säädettävä siitä, että henkilötietoja voidaan käsitellä ainoastaan,

a) jos rekisteröity on yksiselitteisesti antanut suostumuksensa, tai

b) jos käsittely on tarpeen sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena, tai sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä; tai

c) jos käsittely on tarpeen rekisterinpitäjän laillisen velvoitteen noudattamiseksi, tai

d) jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi, tai

e) jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan, tai

f) jos käsittely on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi, paitsi milloin tämän intressin syrjäyttävät rekisteröidyn 1 artiklan 1 kohdan perusteella suojaa tarvitsevat intressit ja perusoikeudet ja -vapaudet.”

18. Direktiivin 95/46 13 artiklan sanamuoto on seuraava:

”1. Jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla pyritään rajoittamaan 6 artiklan 1 kohdassa, 10 artiklassa, 11 artiklan 1 kohdassa sekä 12 ja 21 artiklassa säädettyjen oikeuksien ja velvoitteiden alaa, jos tällaiset rajoitukset ovat välttämättömiä, jotta varmistettaisiin

a) valtion turvallisuus,

b) puolustus,

c) yleinen turvallisuus,

d) rikosten tai, säännellyn ammattitoiminnan osalta, ammattietiikan rikkomusten torjunta, tutkinta, selvittäminen ja syyteharkinta,

e) jäsenvaltiolle tai Euroopan unionille tärkeä taloudellinen tai rahoituksellinen etu, myös rahaa, talousarviota ja verotusta koskevissa asioissa,

f) valvonta-, tarkastus- tai sääntelytehtävä, joka satunnaisestikin liittyy julkisen vallan käyttämiseen c, d ja e alakohdassa tarkoitetuissa tapauksissa,

g) rekisteröidyn suojelu tai muiden oikeudet ja vapaudet.

– –”

B *Kansallinen oikeus*

19. Sähköisistä tieto- ja viestintäpalveluista annetun lain (Telemediengesetz, jäljempänä TMG)[6] 12 §:ssä säädetään seuraavaa:

”1) Palveluntarjoaja saa kerätä ja hyödyntää henkilötietoja sähköisten tieto- ja viestintäpalvelujen tarjoamiseksi vain, kun se on sallittu tässä laissa tai muussa nimenomaisesti sähköisiä tieto- ja viestintäpalveluja koskevassa säännöksessä tai kun käyttäjä on antanut siihen suostumuksensa.

2) Palveluntarjoaja saa hyödyntää sähköisten tieto- ja viestintäpalvelujen tarjoamista varten kerättyjä tietoja muihin tarkoituksiin vain, kun se on sallittu tässä laissa tai muussa nimenomaisesti sähköisiä tieto- ja viestintäpalveluja koskevassa säännöksessä tai kun käyttäjä on antanut siihen suostumuksensa.

3) Jollei toisin ole säädetty, sovelletaan kulloinkin voimassa olevia henkilötietojen suojaa koskevia säännöksiä myös silloin, kun tietoja ei käsitellä automaattisesti.”

20. TMG:n 15 §:ssä säädetään seuraavaa:

”1) Palveluntarjoaja saa kerätä ja hyödyntää käyttäjän henkilötietoja vain, kun se on tarpeen sähköisten tieto- ja viestintäpalvelujen käyttämisen mahdollistamiseksi ja niiden käytöstä laskuttamiseksi (käyttötiedot). Käyttötietoina pidetään erityisesti seuraavia:

1. käyttäjän yksilöintitiedot

2. kunkin yksittäisen käytön alkamista, päättymistä ja laajuutta koskevat tiedot ja

6 — 26.2.2007 annettu laki (BGBl 2007 I, s. 179).

3. tiedot käytetyistä sähköisistä tieto- ja viestintäpalveluista.

2) Palveluntarjoaja saa yhdistää käyttäjän käyttämiä sähköisiä tieto- ja viestintäpalveluja koskevat käyttötiedot siltä osin kuin se on käyttäjän laskutuksen kannalta tarpeen.

– –

4) Palveluntarjoaja saa hyödyntää käyttötietoja yksittäisen käyttökerran päätyttyä siltä osin kuin tämä on tarpeen käyttäjän laskuttamiseksi (laskutustiedot). Palveluntarjoaja voi suojata tiedot voimassa olevien lakiin, sääntöihin tai sopimukseen perustuvien säilytysaikojen noudattamiseksi. – –”

21. Liittovaltion tietosuojalain (Bundesdatenschutzgesetz, jäljempänä BDSG)[7] 3 §:n 1 momentin mukaan ”henkilötiedot ovat tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä tai tiettyjä luonnollisia henkilöitä (rekisteröity) koskevia henkilökohtaisia tai asiallisia olosuhteita koskevia yksittäisiä tietoja. – –”.

II Tosiseikat

22. Patrick Breyer vaatii kieltomääräyksen antamista Saksan liittotasavallalle IP-osoitteiden tallentamisen vuoksi.

23. Saksassa useat julkiset laitokset pitävät yllä yleisön saatavilla olevia internetsivustoja, joilla ne tarjoavat ajankohtaisia tietoja. Hyökkäyksiltä suojautumista ja hyökkääjien rikosoikeudelliseen vastuuseen saattamista varten useimmilla näistä sivustoista tallennetaan kaikki käynnit protokollatietoihin. Tiedoissa säilytetään myös käynnin päätyttyä haettujen tiedostojen tai sivun nimi, hakukentissä käytetyt hakusanat, käynnin ajankohta, siirrettyjen tietojen määrä, ilmoitus sivustolle pääsyn onnistumisesta ja sen tietokoneen IP-osoite, jolta sivustolle on pyritty.

24. Breyer oli käynyt useilla tällaisilla sivustoilla, ja hän vaatii kanteessaan antamaan määräyksen, jossa liittovaltiota kielletään tallentamasta itse tai antamasta kolmannen tallennettavaksi sen isäntäjärjestelmän IP-osoitetta, jolta sivustolla on käyty, jollei tallentaminen ole tarpeen televiestintäpalveluiden käytettävyyden palauttamiseksi häiriön ilmetessä.

25. Breyerin kanne hylättiin ensimmäisessä oikeusasteessa. Valitus hyväksyttiin kuitenkin osittain, ja liittovaltio määrättiin lopettamaan tietojen säilyttäminen yksittäisen sivustolla käynnin päättymisen jälkeen. Kieltomääräyksen taustaolettamana oli se, että kantajan on annettava sivustolla käynnin yhteydessä henkilötietojaan myös sähköpostiosoitteen muodossa, ja sen ehtona oli, ettei tallennus ole välttämätöntä tieto- ja viestintäpalvelun käytettävyyden palauttamiseksi häiriötilanteessa.

III Ennakkoratkaisukysymykset

26. Molemmat asianosaiset tekivät Revision-valituksen, jonka perusteella Bundesgerichtshofin (liittovaltion ylin tuomioistuin, Saksa) neljäs jaosto esitti 17.12.2014 nyt tarkasteltavat ennakkoratkaisukysymykset:

”1) Onko [direktiivin 95/46] 2 artiklan a alakohtaa tulkittava siten, että internetprotokollaosoite (IP-osoite), jonka palveluntarjoaja tallentaa, kun sen internetsivulla käydään, on palveluntarjoajan kannalta henkilötieto jo silloin, kun kolmannella (tässä: yhteyksien tarjoaja) on käytettävissään rekisteröidyn tunnistamiseksi tarvittavat lisätiedot?

7 — 20.12.1990 annettu laki (BGBl 1990 I, s. 2954).

2) Onko [direktiivin 95/46] 7 artiklan f alakohta esteenä sellaiselle kansalliselle säännökselle, jonka mukaan palveluntarjoaja saa kerätä ja hyödyntää käyttäjän henkilötietoja ilman tämän suostumusta vain silloin, kun tämä on tarpeen, jotta mahdollistetaan kyseisen käyttäjän kyseisen sähköisen tieto- ja viestintäpalvelun tosiasiallinen käyttö ja tämän käytön laskutus, ja jonka mukaan sähköisen tieto- ja viestintäpalvelun yleisen toiminnan takaamisen tavoitteella ei voida oikeuttaa kulloisenkin yksittäisen käytön päättymisen jälkeistä hyödyntämistä?”

27. Kuten ennakkoratkaisua pyytänyt tuomioistuin selvittää, kantaja voisi vaatia Saksan oikeuden mukaisesti IP-osoitteiden tallentamisesta luopumista, jos IP-osoitteiden tallentaminen on tietosuojalainsäädännön vastaista laitonta puuttumista yleiseen persoonallisuusoikeuteen, tarkemmin sanottuna tietoja koskevaan itsemääräämisoikeuteen (Saksan siviililain (Bürgerliches Gesetzbuch) 1004 §:n 1 momentti ja 823 §:n 1 momentti, luettuina yhdessä perustuslain (Grundgesetz) 1 ja 2 §:n kanssa).

28. Lähtökohta olisi tämä, jos a) IP-osoitetta voidaan pitää – ainakin internetsivulla käymisen ajankohdan yhteydessä – direktiivin 95/46 2 artiklan a alakohdassa, luettuna yhdessä kyseisen direktiivin johdanto-osan 26 perustelukappaleen toisen lauseen kanssa, tai TMG:n 12 §:n 1 ja 3 momentissa, luettuina yhdessä BDSG:n 3 §:n 1 momentin kanssa, tarkoitettuna henkilötietona ja b) ellei kyseessä ole direktiivin 95/46 7 artiklan f alakohdassa tai TMG:n 12 §:n 1 ja 3 momentissa ja 15 §:n 1 ja 4 momentissa tarkoitettu oikeuttamisperuste.

29. Saman tuomioistuimen mukaan kansallisen lainsäädännön (TMG:n 12 §:n 1 momentin) tulkinta edellyttää sen selvittämistä, miten direktiivin 95/46 2 artiklan a alakohdassa tarkoitettujen henkilötietojen osalta tietojen ”henkilöön” liittyminen on ymmärrettävä.

30. Ennakkoratkaisua pyytänyt tuomioistuin toteaa lisäksi, että TMG:n 15 §:n 1 momentin mukaan palveluntarjoaja saa kerätä ja käyttää käyttäjän henkilötietoja vain, kun se on tarpeen sähköisten tieto- ja viestintäpalveluiden käyttämiseksi ja niiden käytöstä laskuttamiseksi (käyttötiedot),[8] joten kyseisen kansallisen oikeuden säännöksen tulkinta on yhteydessä direktiivin 95/46 7 artiklan f alakohdan tulkintaan.

IV Asian käsittely unionin tuomioistuimessa. Asianosaisten ja muiden osapuolten lausumat

31. Kirjallisia huomautuksia ovat esittäneet Saksan, Itävallan ja Portugalin hallitukset sekä komissio. Suulliseen käsittelyyn, joka pidettiin 25.2.2016, osallistuivat ainoastaan komissio ja Breyer; Saksan hallitus kieltäytyi osallistumasta.

A *Ensimmäiseen kysymykseen liittyvät asianosaisten ja muiden osapuolten lausumat*

32. Breyerin mukaan henkilötietoja ovat myös tiedot, joiden yhdistäminen on mahdollista vain teoreettisesti, eli lähtökohdaksi on otettava mahdollinen abstrakti vaara, jolloin on merkityksetöntä, toteutuuko tällainen yhdistäminen käytännössä. Breyerin mukaan se seikka, että jokin elin saattaa olla suhteellisen kykenemätön tunnistamaan henkilöä IP-osoitteen perusteella, ei merkitse sitä, ettei kyseiselle henkilölle aiheutuisi vaaraa. Lisäksi sillä seikalla, että Saksa tallentaa Breyerin IP-tiedot pystyäkseen tarvittaessa tunnistamaan mahdolliset hyökkäykset tai käynnistämään rikosoikeudelliset menettelyt TMG:n 113 §:n mukaisesti, on Breyerin mielestä merkitystä ja näin on käynyt lukuisia kertoja.

8 — Ennakkoratkaisua pyytäneen tuomioistuimen mukaan käyttötietoja ovat käyttäjän yksilöintitiedot; kunkin yksittäisen käytön alkamista, päättymistä ja laajuutta koskevat tiedot sekä käyttäjän käyttämiä tieto- ja viestintäpalveluja koskevat tiedot.

33. Saksan hallituksen mukaan ensimmäiseen ennakkoratkaisukysymykseen on vastattava kieltävästi. Sen mukaan dynaamiset IP-osoitteet eivät paljasta direktiivin 95/46 2 artiklan a alakohdassa tarkoitettua tunnistettua henkilöä. Sen selvittämiseksi, koskevatko tiedot samassa säännöksessä tarkoitettua *tunnistettavissa olevaa* henkilöä, on tunnistettavissa olemista tarkasteltava suhteellisen perusteen pohjalta. Tämä käy sen mukaan ilmi direktiivin 95/46 johdanto-osan 26 perustelukappaleesta, jonka mukaan huomioon on otettava ainoastaan kohtuullisesti toteutettavissa olevat keinot, joita rekisterinpitäjä tai sivullinen voi käyttää henkilön tunnistamiseen. Tämä täsmennys merkitsee sen mukaan, ettei unionin lainsäätäjä ole halunnut sisällyttää direktiivin 95/46 soveltamisalaan tilanteita, joissa kenen tahansa sivullisen on objektiiviselta kannalta mahdollista tunnistaa henkilöllisyys.

34. Saksan hallitus katsoo myös, että direktiivin 95/46 2 artiklan a alakohdassa tarkoitettua henkilötiedon käsitettä on tulkittava kyseisen direktiivin tarkoituksen eli perusoikeuksien kunnioittamisen takaamisen kannalta. Luonnollisten henkilöiden suojelun tarve voidaan nähdä toisin sen mukaan, kenen hallussa tiedot ovat ja onko kyseisellä toimijalla käytettävissään keinoja tietojen käyttämiseksi tunnistamiseen.

35. Saksan hallitus väittää, ettei Breyer ole tunnistettavissa yhdistämällä IP-osoitteet sisällöntarjoajan tallentamiin muihin tietoihin. Tunnistamista varten olisi käsiteltävä verkkoyhteyden tarjoajan hallussa olevia tietoja, mutta oikeusperustan puuttuessa nämä eivät voi antaa kyseisiä tietoja sisällöntarjoajalle.

36. Itävallan hallitus on päinvastoin sitä mieltä, että kysymykseen on vastattava myöntävästi. Direktiivin 95/46 johdanto-osan 26 perustelukappaleen perusteella henkilön tunnistettavissa oleminen ei edellytä, että kaikki henkilön tunnistamisessa käytettävät tiedot olisivat yhden ainoan toimijan hallussa. IP-osoite voi siis olla henkilötieto, jos sivullisella (esimerkiksi verkkoyhteyden tarjoajalla) on käytettävissään keinot kyseisen IP-osoitteen haltijan tunnistamiseksi ilman kohtuuttomia ponnistuksia.

37. Portugalin hallitus kallistuu niin ikään myöntävän vastauksen kannalle ja katsoo, että IP-osoite yhdessä sivulla käynnin päivämäärän kanssa on henkilötieto, sillä se voi johtaa siihen, että käyttäjän tunnistaa muu toimija kuin IP-osoitteen tallentanut toimija.

38. Komissio ehdottaa niin ikään myöntävää vastausta unionin tuomioistuimen tuomiossa Scarlet Extended[9] esitetyn ratkaisun perusteella. Komission mukaan on niin, että koska IP-osoitteita tallennetaan nimenomaan käyttäjien tunnistamiseksi verkkohyökkäysten yhteydessä, verkkoyhteyden tarjoajan tallentamien lisätietojen hyödyntäminen voi tarjota keinon, joka voi olla direktiivin 95/46 johdanto-osan 26 perustelukappaleessa tarkoitetulla tavalla kohtuullisesti toteutettavissa. Komission mielestä sekä kyseisellä direktiivillä tavoiteltu päämäärä että Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 7 ja 8 artikla puoltavat direktiivin 95/46 2 artiklan a alakohdan laajaa tulkintaa.

B *Toiseen kysymykseen liittyvät asianosaisten ja muiden osapuolten lausumat*

39. Breyerin mukaan direktiivin 95/46 7 artiklan f alakohta on yleinen säännös, jonka käytännön täytäntöönpano edellyttää konkretisointia. Unionin tuomioistuimen oikeuskäytännön mukaisesti nyt olisi siis arvioitava tapauksen erityiset olosuhteet ja selvitettävä, onko olemassa ryhmiä, joilla on kyseisessä säännöksessä tarkoitettu oikeutettu intressi, jolloin on paitsi mahdollista, myös välttämätöntä säätää tällaisia ryhmiä koskevista erityissäännöksistä kyseisen artiklan soveltamiseksi. Tällöin kansallinen säännös on Breyerin näkemyksen mukaan direktiivin 95/46 7 artiklan f alakohdan mukainen, jos julkisella portaalilla ei ole intressiä säilyttää henkilötietoja tai jos anonymiteetin suojaamista koskeva intressi on painoarvoltaan suurempi. Breyerin mukaan henkilötietojen

9 — Tuomio 24.11.2011 (C-70/10, EU:C:2011:771, 51 kohta).

järjestelmällinen säilyttäminen ei kuitenkaan ole demokraattisen yhteiskunnan mukaista eikä tarpeellista tai oikeasuhteista sähköisten tieto- ja viestintäpalveluiden toiminnan varmistamiseksi, sillä sähköisten tieto- ja viestintäpalveluiden toiminnan varmistaminen on täysin mahdollista ilman henkilötietojen tallentamista, kuten muutamien liittovaltion ministeriöiden verkkosivustot osoittavat.

40. Saksan hallituksen mukaan toista kysymystä ei ole tarpeen käsitellä, sillä se esitetään yksinomaan siinä tilanteessa, että ensimmäiseen kysymykseen vastataan myöntävästi, mikä ei sen mielestä tule tässä tapauksessa kyseeseen edellä esitetyistä syistä.

41. Itävallan hallitus ehdottaa, että kysymykseen vastataan, ettei direktiivi 95/46 ole yleisesti esteenä pääasiassa riidanalaisten tietojen kaltaisten tietojen säilyttämiselle, kun niiden säilyttäminen on välttämätöntä sähköisten tieto- ja viestintäpalveluiden moitteettoman toiminnan takaamiseksi. Sen mukaan IP-osoitteen rajallinen säilyttäminen verkkosivulla käynnin päättymisen jälkeen voi olla laillista, sillä henkilötietoja säilyttävällä rekisterinpitäjällä on velvollisuus soveltaa direktiivin 95/46 17 artiklan 1 kohdassa säädettyjä toimenpiteitä kyseisten tietojen suojaamiseksi. Verkkohyökkäysten torjumiseksi voi olla perusteltua analysoida aiempiin hyökkäyksiin liittyviä tietoja ja estää verkkosivuille pääsy tietyistä IP-osoitteista. Pääasiassa kyseessä olevan kaltaisten tietojen säilyttämisen oikeasuhteisuutta olisi arvioitava tapauskohtaisesti siltä kannalta, mikä on sähköisten tieto- ja viestintäpalveluiden moitteettoman toiminnan takaamisen tavoite, ottaen huomioon direktiivin 95/46 6 artiklan 1 kohdassa luetellut periaatteet.

42. Portugalin hallituksen mukaan direktiivin 95/46 7 artiklan f alakohta ei ole esteenä pääasiaan liittyville kansallisille säännöksille, sillä Saksan lainsäätäjä on jo punninnut kyseisessä säännöksessä säädetyn mukaisesti yhtäältä henkilötietoja säilyttävän rekisterinpitäjän oikeutettuja intressejä ja toisaalta kyseisten rekisteröityjen oikeuksia ja vapauksia.

43. Komission mukaan kansallisessa säännöksessä, jolla saatetaan direktiivin 95/46 7 artiklan f alakohta kansallisen oikeuden osaksi, on määritettävä henkilötietojen käsittelyn tavoitteet siten, että ne ovat asianomaisen yksittäisen henkilön ennakoitavissa. Sen näkemyksen mukaan Saksan kansallisessa säännöksessä ei noudateta tätä vaatimusta, sillä TMG:n 15 §:n 1 momentissa säädetään, että IP-osoitteiden säilyttäminen on sallittua, ”kun se on tarpeen sähköisten tieto- ja viestintäpalveluiden käyttämiseksi”.

44. Komissio esittää siis, että toiseen kysymykseen vastataan siten, että kyseinen säännös on esteenä kansallisen säännöksen tulkitsemiselle niin, että palveluntarjoajana toimiva viranomainen voi kerätä ja hyödyntää käyttäjän henkilötietoja ilman tämän suostumusta, myös silloin, kun sen tavoitteena on sähköisen tieto- ja viestintäpalvelun yleisen moitteettoman toiminnan varmistaminen, ellei kyseisessä kansallisessa säännöksessä määritetä tätä tavoitetta riittävän selkeästi ja täsmällisesti.

V Arviointi

A *Ensimmäinen kysymys*

1. Ensimmäisen kysymyksen rajaaminen

45. Ensimmäisessä ennakkoratkaisukysymyksessä pyritään sen sanamuodon mukaan selvittämään, onko IP-osoite, jonka kautta käydään tietyllä verkkosivulla, kyseisen verkkosivun haltijana olevan julkisen elimen kannalta (direktiivin 95/46 2 artiklan a alakohdassa tarkoitettu) henkilötieto, mikäli verkkoyhteyden tarjoajan hallussa on lisätietoja, joiden avulla rekisteröity voidaan tunnistaa.

46. Näin muotoiltuna kysymys on niin täsmällinen, että heti alussa voidaan sulkea pois muut kysymykset, joita IP-osoitteiden oikeudellisesta luonteesta voisi teoriassa herätä henkilötietojen suojaamisen yhteydessä.

47. Ensinäkin ennakkoratkaisua pyytänyt tuomioistuin viittaa ainoastaan dynaamisiin IP-osoitteisiin eli osoitteisiin, jotka annetaan väliaikaisesti kutakin verkkoyhteyttä varten ja jotka vaihtuvat seuraavissa verkkoyhteyksissä. Sivuun jäävät siis kiinteät IP-osoitteet, jotka ovat muuttumattomia ja joiden perusteella verkkoyhteydessä oleva laite voidaan tunnistaa pysyvästi.

48. Toiseksi ennakkoratkaisua pyytänyt tuomioistuin olettaa, ettei verkkosivuston haltija pysty nyt käsiteltävässä asiassa tunnistamaan verkkosivujensa kävijöitä dynaamisten IP-osoitteiden perusteella eikä sillä itsellään ole lisätietoja, jotka yhdistettyinä kyseisiin IP-osoitteisiin auttaisivat tunnistamisessa. Mainittu tuomioistuin vaikuttaa asettuvan tässä yhteydessä sille kannalle, ettei dynaaminen IP-osoite ole direktiivin 95/46 2 artiklan a alakohdassa tarkoitettu henkilötieto *verkkosivuston tarjoajan kannalta*.

49. Ennakkoratkaisua pyytäneelle tuomioistuimelle on epäselvää, voidaanko dynaamista IP-osoitetta pitää verkkosivujen haltijan kannalta henkilötietona, *jos sivullisella on lisätietoja*, jotka yhdessä IP-osoitteiden kanssa mahdollistavat verkkosivujen kävijöiden tunnistamisen. On kuitenkin syytä panna merkille, ettei mainittu tuomioistuin kuitenkaan tarkoita mitä tahansa sivullista, jonka hallussa lisätiedot ovat, vaan verkkoyhteyden tarjoajaa (näin suljetaan pois muut mahdolliset tällaisten tietojen haltijat).

50. Tarkasteltaviksi eivät siis tule esimerkiksi seuraavat seikat: a) ovatko kiinteät IP-osoitteet direktiivin 95/46 mukaisia henkilötietoja;[10] b) ovatko dynaamiset IP-osoitteet aina ja kaikissa olosuhteissa kyseisessä direktiivissä tarkoitettuja henkilötietoja tai c) onko dynaamisten IP-osoitteiden pitäminen henkilötietoina väistämätöntä aina, kun on olemassa mikä tahansa sivullinen, joka pystyy käyttämään dynaamisia IP-osoitteita verkonkäyttäjien tunnistamiseen.

51. Ratkaistavaksi jääkin ainoastaan se, onko dynaaminen IP-osoite internetpalvelun tarjoajan kannalta henkilötieto, kun verkkoyhteyden tarjoajan hallussa on lisätietoja, jotka yhdistettyinä kyseiseen IP-osoitteeseen auttavat tunnistamaan, kuka on käynyt ensin mainitun palveluntarjoajan verkkosivuilla.

2. Asiakysymys

52. Ennakkoratkaisupyynnön taustalla olevasta tutkintaongelmasta on käyty Saksassa paljon keskustelua sekä oikeuskirjallisuudessa että oikeuskäytännössä, ja keskustelussa on erottunut kaksi toisistaan poikkeavaa näkemystä.[11] Toisen näkemyksen mukaan (jossa sovelletaan objektiivista tai ehdotonta perustetta) käyttäjä on tunnistettavissa, jolloin IP-osoite on suojattavaksi tuleva henkilötieto, kun käyttäjä voidaan tunnistaa vain yhdistämällä kyseinen dynaaminen IP-osoite sivullisen (esimerkiksi verkkoyhteyden tarjoajan) antamiin tietoihin internetpalvelun tarjoajan omista valmiuksista ja keinoista riippumatta.

10 — Unionin tuomioistuin on käsitellyt kyseistä ongelmaa tuomiossa 24.11.2011, Scarlet Extended (C-70/10, EU:C:2011:771, 51 kohta) ja tuomiossa 19.4.2012, Bonnier Audio ym. (C-461/10, EU:C:2012:219). Viimeksi mainitun tuomion 51 ja 52 kohdassa todetaan, että ”sellaisen – – internetin käyttäjän [nimen] ja [osoitteen], joka käyttää IP-osoitetta, jonka kautta suojattuja teoksia sisältäviä tiedostoja oletetaan vaihdetun laittomasti – –, luovuttaminen on direktiivin 2002/58 2 artiklan ensimmäisessä kohdassa, kun sitä luetaan yhdessä direktiivin 95/46 2 artiklan b alakohdan kanssa, tarkoitettua henkilötietojen käsittelyä”.

11 — Ks. molemmista oikeusopillisista kannoista esim. Schreibauer, M., teoksessa *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P. ja von Lewinski, K. (toim.), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4. painos, § 11 Telemediengesetz (4–10). Nink, J. ja Pohle, J., ”Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze”, julkaisussa *Multimedia und Recht*, 9/2015, s. 563–567. Heidrich, J. ja Wegener, C., ”Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging”, julkaisussa *Multimedia und Recht*, 8/2015, s. 487–492. Leisterer, H., ”Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr”, julkaisussa *Computer und Recht*, 10/2015, s. 665–670.

53. Toisen näkemyksen (jossa sovelletaan suhteellista perustetta) kannattajien mukaan mahdollisuus saada sivullisen apua käyttäjän tunnistamiseen ei riitä siihen, että dynaaminen IP-osoite katsottaisiin henkilötiedoksi. Olennaista on, kykeneekö toimija, jolla on pääsy kyseisiin tietoihin, käyttämään kyseisiä tietoja omin keinoin ja tunnistamaan näin henkilön.

54. Tämän sisäisessä oikeudessa ilmenevän ristiriidan taustalla olevista perusteista riippumatta unionin tuomioistuimen on tulkittava vastauksessaan ainoastaan niitä direktiivin 95/46 kahta säännöstä, joihin sekä ennakkoratkaisua pyytänyt tuomioistuin että asian osapuolet viittaavat, eli direktiivin 2 artiklan a alakohtaa [12] ja sen johdanto-osan 26 perustelukappaletta. [13]

55. Dynaamisista IP-osoitteista välittyvät päivämäärä ja aika, jona tietyltä tietokoneelta (tai muulta laitteelta) on käyty tietyllä internetsivulla, ja jo tämän perusteella niistä ilmenee tiettyjä piirteitä internetin käyttäjän käyttäytymisestä, ja näin ollen ne merkitsevät mahdollista puuttumista yksityiselämän suojaa koskevaan oikeuteen, [14] joka on taattu ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn eurooppalaisen yleissopimuksen 8 artiklassa sekä perusoikeuskirjan 7 artiklassa, jonka valossa – samoin kuin perusoikeuskirjan 8 artiklan valossa – direktiiviä 95/46 on tulkittava. [15] Todellisuudessa riita-asian osapuolet eivät kiistä tätä oletusta, eikä se ole myöskään varsinaisesti ennakkoratkaisukysymyksen kohteena.

56. Henkilö, jota kyseiset tiedot koskevat, ei ole tunnistettu luonnollinen henkilö. Käynnin päivämäärästä, kellonajasta ja numeerisesta alkuperästä ei käy välittömästi ja suoraan ilmi, kenelle luonnolliselle henkilölle laite, jolta internetsivulla on käyty, kuuluu, eikä niistä paljastu myöskään laitetta käyttävän henkilön henkilöllisyys (käyttäjänä voi olla kuka tahansa luonnollinen henkilö).

57. Dynaamisen IP-osoitteen avulla voidaan kuitenkin selvittää joko yksin tai yhdessä muiden tietojen kanssa, kuka omistaa laitteen, jolta internetsivulla on käyty, joten sitä voidaan pitää tunnistettavissa olevaa henkilöä koskevina tietoina. [16]

58. Ennakkoratkaisua pyytäneen tuomioistuimen näkemyksen mukaan dynaaminen IP-osoite ei riitä yksin tietyllä verkkosivulla kyseisen osoitteen kautta käyneen käyttäjän tunnistamiseen. Jos internetpalvelun tarjoaja voisi sitä vastoin tunnistaa käyttäjän dynaamisen IP-osoitteen perusteella, kyseessä olisi kiistatta direktiivissä 95/46 tarkoitettu henkilötieto. Ennakkoratkaisukysymyksessä ei kuitenkaan vaikuta olevan kysymys tästä, sillä siitä käy ilmi, että käsiteltävän riita-asian osapuolena olevat internetpalvelun tarjoajat eivät pysty tunnistamaan käyttäjää pelkän dynaamisen IP-osoitteen perusteella.

12 — Ks. edellä 13 kohta.

13 — Ks. edellä 11 kohta.

14 — Tästä muistutettiin julkisasiamies Cruz Villalónin ratkaisuehdotuksessa Scarlet Extended (C-70/10, EU:C:2011:255, 76 kohta), ja samoin asiaan on suhtautunut myös Euroopan tietosuojavaltuutettu 22.2.2010 antamassaan lausunnossa Euroopan unionin tällä hetkellä käymistä väärentämisenvastaista kauppasopimusta (ACTA) koskevista neuvotteluista (EUVL 2010, C 147, s. 1, 24 kohta) sekä 10.5.2010 antamassaan lausunnossa ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja puitepäätöksen 2004/68/YOS kumoamisesta (EUVL 2010, C 323, s. 6, 11 kohta).

15 — Ks. vastaavasti tuomio 20.5.2003, Österreichischer Rundfunk (C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, 68 kohta) sekä julkisasiamies Kokottin ratkaisuehdotus Promusicae (C-275/06, EU:C:2007:454, 51 kohta ja sitä seuraavat kohdat).

16 — On oletettava, ellei toisin osoiteta, että kyseinen henkilö on sama henkilö, joka on ollut internetissä ja käynyt kyseisellä internetsivulla. Vaikka viimeksi mainittua oletusta ei otettaisi huomioon, internetsivulla käynnin päivämäärää, kellonaikaa ja numeerista alkuperää koskevat tiedot antavat kuitenkin mahdollisuuden yhdistää kyseinen käynti laitteen omistajaan ja liittää hänet välillisesti niistä ilmi käyviin internetkäyttäytymisen piirteisiin. Kuviteltavissa olevan poikkeuksen muodostavat IP-osoitteet, jotka on annettu yleisessä käytössä oleville tietokoneille, kuten nettikahviloiden tietokoneille, joiden anonyymit käyttäjät eivät ole tunnistettavissa ja joiden omistajista kyseisessä tilassa tapahtunutta tietoliikennettä koskevat tiedot eivät anna mitään oleellisia henkilökohtaisia tietoja. Tämä on kuitenkin ainoa direktiivillä 95/46 perustetun tietosuojatyöryhmän (29 artiklan mukainen tietosuojatyöryhmä) hyväksymä poikkeus periaatteeseen, jonka mukaan IP-osoitteet ovat henkilötietoja. Asia käy ilmi tietosuojatyöryhmän 20.6.2007 antamasta lausunnosta 4/2007 henkilötietojen käsitteestä (WP 136), joka on saatavana osoitteessa http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

59. Muihin tietoihin yhdistettynä dynaaminen IP-osoite antaa mahdollisuuden käyttäjän tunnistamiseen välillisesti, mistä kaikki osapuolet ovat yhtä mieltä. Voidaanko pelkästään sillä perusteella, että tällaisia dynaamiseen IP-osoitteeseen yhdistettävissä olevia lisätietoja on mahdollisesti olemassa, dynaamista IP-osoitetta pitää direktiivissä tarkoitettuna henkilötietona? On siis selvitettävä, riittääkö tähän pelkkä abstrakti kyseisten tietojen tutustuttavaksi saamisen mahdollisuus, vai onko tietojen sitä vastoin oltava sen toimijan, jonka tiedossa on jo dynaaminen IP-osoite, tai sivullisen käytettävissä.

60. Osapuolet ovat keskittyneet huomautuksissaan tulkitsemaan direktiivin 95/46 johdanto-osan 26 perustelukappaletta, jossa käytetään ilmausta ”kaikki kohtuullisesti toteutettavissa olevat keinot, joita joko rekisterinpitäjä tai joku muu voi kyseisen henkilön tunnistamiseksi käyttää”. Ennakkoratkaisua pyytäneen tuomioistuimen kysymys ei koske lisätietoja, jotka ovat pääasiassa kyseessä olevien palveluntarjoajien hallussa. Siinä ei viitata myöskään mihin tahansa sivulliseen, jonka hallussa lisätiedot (joiden yhdistäminen dynaamiseen IP-osoitteeseen auttaa tunnistamaan käyttäjän) ovat, vaan siinä viitataan verkkoyhteyden tarjoajaan.

61. Unionin tuomioistuimen ei siis ole välttämätöntä tutkia tässä tapauksessa kaikkia kohtuullisesti toteutettavissa olevia keinoja, joita pääasian vastaaja voi käyttää, jotta vastaajan hallussa olevia dynaamisia IP-osoitteita voitaisiin pitää henkilötietoina. Ennakkoratkaisua pyytänyt tuomioistuin viittaa ainoastaan sivullisen hallussa oleviin lisätietoihin, mikä voi tarkoittaa joko sitä, että a) vastaajalla ei ole käyttäjän tunnistamiseen tarvittavia asianmukaisia lisätietoja, tai sitä, että b) nämä tiedot olisivat vastaajan saavutettavissa, mutta vastaaja ei pysty kohtuullisesti toteutettavissa olevin keinoin käyttämään niitä tähän tarkoitukseen rekisterinpitäjänä direktiivin 95/46 johdanto-osan 26 perustelukappaleen mukaisesti.

62. Molemmat hypoteesit edellyttävät tosiseikkojen toteamista, joka on yksin ennakkoratkaisua pyytäneen tuomioistuimen tehtävä. Unionin tuomioistuin voi esittää yleisiä perusteita ilmauksen ”kaikki kohtuullisesti toteutettavissa olevat keinot, joita – – rekisterinpitäjä – – voi – – käyttää” tulkintaa varten, jos ennakkoratkaisua pyytänyt tuomioistuin epäilee vastaajan kykyä käyttää tarvittavia lisätietoja kohtuullisesti toteutettavissa olevin keinoin. Muutoin unionin tuomioistuin ei voi nähdäkseni esittää tulkintaperusteita, jotka eivät ole ennakkoratkaisua pyytäneelle tuomioistuimelle välttämättömiä ja joita se ei ole pyytänyt.

63. Esitetyssä kysymyksessä on siis ratkaistava pohjimmiltaan, vaikuttaako se seikka, että tietyn hyvin erityisen sivullisen (verkkoyhteyden tarjoajan) hallussa on lisätietoja, jotka antavat dynaamisiin IP-osoitteisiin yhdistettyinä mahdollisuuden tunnistaa tietyllä verkkosivulla käyneen käyttäjän, siihen, pidetäänkö dynaamisia IP-osoitteita henkilötietoina.

64. Direktiivin 95/46 johdanto-osan 26 perustelukappale on syytä ottaa jälleen esille. Ilmaus ”kohtuullisesti toteutettavissa olevat keinot, joita – – *joku muu* voi – – käyttää”[17] voi johtaa tulkintaan, jonka mukaan dynaamisen IP-osoitteen pitäminen itsessään henkilötietona edellyttää ainoastaan, että sivullinen voi saada lisätietoja (jotka voidaan yhdistää dynaamiseen IP-osoitteeseen tietyn henkilön tunnistamiseksi).

65. Tällainen mahdollisimman laaja tulkinta johtaisi käytännössä siihen, että henkilötiedoksi luokiteltaisiin kaikenlaiset tiedot, vaikkeivät ne riittäisi yksin käyttäjän tunnistamiseen. Missään tilanteessa ei voida todeta ehdottoman varmasti, ettei ole olemassa sivullista, jonka hallussa on lisätietoja, jotka voidaan yhdistää kyseisiin tietoihin ja joiden avulla voidaan näin paljastaa tietyn henkilön henkilöllisyys.

17 — Kursivointi tässä.

66. Nähdäkseni se mahdollisuus, että tekniset välineet kehittyvät ennemmin tai myöhemmin siten, että tietojen keräämisessä ja käsittelyssä käytettäviä, yhä pidemmälle kehittyneitä välineitä on selvästi helpompi saada käyttöön, riittää perustelemaan ne varotoimet, joilla pyritään edistämään yksityisyyden suojaa. Tietosuojan alalla merkityksellisiä oikeudellisia tietoluokkia määriteltäessä on otettava huomioon riittävän laajat ja joustavat hypoteettiset mahdollisuudet, niin että kaikki mahdolliset kuviteltavissa olevat tilanteet saadaan katettua. [18]

67. Tämä näkemys, joka on tosin erittäin perusteltu, ei voi nähdäkseni kuitenkaan johtaa lainsäätäjän tahdon sivuuttamiseen, ja direktiivin 95/46 johdanto-osan 26 perustelukappaleen systemaattinen tulkinta sisältää uskoakseni *tiettyjen sivullisten* käyttämät ”kohtuullisesti toteutettavissa olevat keinot”.

68. Johdanto-osan 26 perustelukappaleessa ei viitata mihin tahansa rekisterinpitäjän (tässä: internetpalvelun tarjoajan) käytettävissä oleviin keinoihin vaan ainoastaan niihin, jotka ovat kohtuullisesti toteutettavissa, ja samoin on ymmärrettävä, että lainsäätäjä viittaa sivullisiin, joiden puoleen rekisterinpitäjä voi *niin ikään kohtuullisella tavalla* kääntyä saadakseen lisätietoja tunnistamista varten. Näin ei ole silloin, kun yhteydenotto kolmansiin veisi tosiasiallisesti paljon henkilöresursseja ja taloudellisia resursseja tai kun yhteydenotto ei ole käytännössä toteutettavissa tai se on kielletty laissa. Kuten edellä korostettiin, muutoin olisi käytännössä mahdotonta tehdä eroa eri keinojen välillä, sillä aina olisi otettava huomioon se hypoteettinen mahdollisuus, että sivullisella – vaikka se olisi internetpalvelun tarjoajan saavuttamattomissa – voisi olla nyt tai jatkossa merkityksellisiä lisätietoja, joiden avulla käyttäjä voitaisiin tunnistaa.

69. Kuten olen todennut, ennakkoratkaisua pyytäneen tuomioistuimen tarkoittama sivullinen on verkkoyhteyden tarjoaja. Voidaan varmasti ajatella, että palveluntarjoajan yhteydenotto juuri tähän sivulliseen on erityisen kohtuullisesti toteutettavissa lisätietojen hankkimiseksi, jos palveluntarjoaja haluaa tunnistaa mahdollisimman tehokkaasti, käytännöllisesti ja suoraan verkkosivullaan käyneen käyttäjän dynaamisen IP-osoitteen perusteella. Kyseessä ei ole millään tavalla hypoteettinen, tuntematon ja tavoittamattomissa oleva sivullinen vaan yksi internetverkon kannalta merkittävä toimija, jonka hallussa tiedetään varmuudella olevan tietoja, joita palveluntarjoaja tarvitsee tunnistaakseen käyttäjän. Kuten ennakkoratkaisua pyytänyt tuomioistuin toteaa, pääasian vastaaja pyrkii tosiasiassa ottamaan yhteyttä juuri kyseiseen konkreettiseen sivulliseen hankkiakseen tarvitsemansa lisätiedot.

70. Internetyhteyden tarjoaja on tyypillisesti direktiivin 95/46 johdanto-osan 26 perustelukappaleessa tarkoitettu sivullinen, jonka puoleen käsiteltävässä asiassa kyseessä oleva palveluntarjoaja voi kohtuullisimmin kääntyä. On kuitenkin selvitettävä, voidaanko kyseisen sivullisen hallussa olevien lisätietojen saaminen katsoa kohtuullisesti tai käytännössä toteutettavissa olevaksi.

71. Saksan hallitus väittää, että koska internetyhteyden tarjoajan hallussa olevat tiedot ovat henkilötietoja, se ei voi antaa niitä muutoin kuin henkilötietojen käsittelystä annettuja oikeussääntöjä noudattaen. [19]

72. Asia on kiistatta näin, sillä kyseisten tietojen hyödyntämisessä on noudatettava henkilötietoihin sovellettavaa lainsäädäntöä. Tieto voidaan saada kohtuullisesti toteutettavissa olevin keinoin vain, jos tämäntyyppisten tietojen saamista tutustuttavaksi koskevat edellytykset täyttyvät, ja kyseisistä edellytyksistä ensimmäinen on lain mukainen mahdollisuus niiden säilyttämiseen ja muille

18 — Tällainen varovainen ja varautunut lähestymistapa on tietosuojatyöryhmän kannan taustalla. Kuten edellä todettiin, tietosuojatyöryhmän mukaan lähtökohtana on periaate, jonka mukaan IP-osoitteet ovat henkilötietoja, ja ainoan hyväksyttävän poikkeuksen tähän muodostaa hypoteettinen tilanne, jossa palveluntarjoaja pystyy osoittamaan ehdottoman varmasti, että kyseiset osoitteet kuuluvat tunnistamattomille henkilöille, kuten nettikahvilan käyttäjille. Ks. edellä alaviitteen 16 loppuosa.

19 — Ks. Saksan hallituksen esittämien kirjallisten huomautusten 40 ja 45 kohta.

välittämiseen. Internetyhteyden tarjoajalla on kiistatta valtuus kieltäytyä luovuttamasta kyseisiä tietoja, mutta sama pätee myös toisin päin. Tietojen siirtämisen mahdollisuus on täysin kohtuullisesti toteutettavissa, mikä jo itsessään tekee dynaamisesta IP-osoitteesta direktiivin 95/46 johdanto-osan 26 perustelukappaleen perusteella henkilötiedon internetpalvelun tarjoajan kannalta.

73. Kyseessä on *lainsäädännön puitteissa* toteutettavissa oleva mahdollisuus, eli se on kohtuullinen. Direktiivissä 95/46 tarkoitettujen kohtuullisesti toteutettavissa olevien keinojen on oltava ehdottomasti laillisia.[20] Ennakkoratkaisua pyytänyt tuomioistuin lähtee luonnollisesti liikkeelle tästä olettamasta, kuten Saksan hallitus muistuttaa.[21] Näin karsitaan huomattavasti oikeudelliselta kannalta merkityksellisiä tiedonsaannin keinoja, sillä keinojen on oltava ehdottomasti laillisia. Tällaisia keinoja on kuitenkin olemassa, ja vaikka niiden käytännön soveltaminen voi vaikuttaa hyvin rajalliselta, ne ovat kohtuullisesti toteutettavissa direktiivissä 95/46 tarkoitetulla tavalla.

74. Katson näin ollen, että ensimmäiseen ennakkoratkaisukysymykseen on vastattava myöntävästi. Dynaaminen IP-osoite on luokiteltava internetpalvelun tarjoajan kannalta henkilötiedoksi, kun otetaan huomioon, että olemassa on sivullinen (verkkoyhteyden tarjoaja), johon internetpalvelun tarjoaja voi ottaa kohtuullisesti toteutettavissa olevin keinoin yhteyttä hankkiakseen lisätietoja, jotka dynaamiseen IP-osoitteeseen yhdistettynä auttavat tunnistamaan käyttäjän.

75. Ehdottamaani päinvastainen ratkaisu johtaisi lopputulokseen, joka mielestäni vain vahvistaa ehdottamaani ratkaisua. Jos dynaamisia IP-osoitteita ei pidettäisi henkilötietoina internetpalvelun tarjoajan kannalta, internetpalvelun tarjoaja voisi säilyttää niitä loputtomiin ja se voisi pyytää milloin tahansa verkkoyhteyden tarjoajalta lisätietoja yhdistääkseen ne dynaamiseen IP-osoitteeseen käyttäjän tunnistamiseksi. Näissä olosuhteissa, kuten Saksan hallitus myöntää,[22] dynaamisista IP-osoitteista tulee henkilötietoja, jos käyttäjän tunnistamiseen tarvittavat lisätiedot saadaan, ja tällöin tilanteeseen sovelletaan tietosuojalainsäädäntöä.

76. Kyseessä olisi siis tieto, jonka säilyttäminen on ollut mahdollista ainoastaan siksi, ettei sitä ole tätä aiemmin pidetty henkilötietona palveluntarjoajan kannalta. Dynaamisen IP-osoitteen oikeudellinen luokittelu henkilötiedoksi jää siis viimeksi mainitun valinnan varaan, mikä edellyttää sellaista mahdollisuutta, että viimeksi mainittu päättää joskus myöhemmin käyttää dynaamista IP-osoitetta käyttäjän tunnistamiseen yhdistämällä osoitteen lisätietoihin, jotka sen on hankittava sivulliselta. Nähdäkseni direktiivin 95/46 sisällön perusteella määräävänä tekijänä on kuitenkin se, että on kohtuulliselta kannalta mahdollista, että olemassa on sivullinen, johon voidaan ottaa yhteyttä ja jolla on tarvittavat keinot auttaa henkilön tunnistamisessa – ei se, että mahdollisuus ottaa yhteyttä tällaiseen sivulliseen toteutuisi käytännössä.

77. Saksan hallituksen tavoin voitaisiin tunnustaa, että dynaamisesta IP-osoitteesta tulee henkilötieto vasta, kun verkkoyhteyden tarjoaja vastaanottaa sen. Tällöin olisi siis hyväksyttävä, että kyseinen luokittelu tapahtuu taannehtivasti IP-osoitteen säilyttämisen määräaikaan nähden, ja näin ollen olisi katsottava, ettei luokittelua ollut olemassa, jos alun perin henkilötiedoksi luokiteltavan tiedon säilyttämiselle asetettu määräaika olisi ylittynyt. Tällöin päädyttäisiin lopputulokseen, joka olisi vastoin henkilötietojen suojasta annetun lainsäädännön henkeä. Syy, jolla perustellaan kyseisten tietojen yksinomaan väliaikaista säilyttämistä, menettäisi merkityksensä, jos kyseisten tietojen alusta lähtien sisältämä olennainen ominaisuus, implisiittinen keino auttaa tunnistamaan luonnollinen henkilö joko yksin tai muihin tietoihin yhdistettyinä, muuttuisi merkitykselliseksi vastaa viipeellä. Myös tästä täysin käytännöllisestä syystä on järkevämpää antaa tiedoille kyseinen ominaisuus heti alusta lähtien.

20 — Tässä yhteydessä on merkityksetöntä, että henkilötiedon saaminen on tosiasiassa mahdollista tietosuojalainsäädäntöä rikkomalla.

21 — Saksan hallituksen esittämien kirjallisten huomautusten 47 ja 48 kohta.

22 — Saksan hallituksen esittämien kirjallisten huomautusten 36 kohta.

78. Näin ollen esitän ensimmäisenä ratkaisuehdotuksena, että direktiivin 95/46 2 artiklan a alakohtaa on tulkittava siten, että IP-osoite, jonka palveluntarjoaja tallentaa sen verkkosivuilla käynnin yhteydessä, on palveluntarjoajan kannalta henkilötieto, jos verkkoyhteyden (internetyhteyden) tarjoajalla on hallussaan rekisteröidyn tunnistamiseksi tarvittavat lisätiedot.

B *Toinen kysymys*

79. Ennakkoratkaisua pyytänyt tuomioistuin pyrkii selvittämään toisella kysymyksellään, onko direktiivin 95/46 7 artiklan f alakohta esteenä sellaiselle kansalliselle säännökselle, jonka mukaan käyttäjän henkilötietoja saa kerätä ja hyödyntää ilman käyttäjän suostumusta vain silloin, kun tämä on tarpeen, jotta kyseisen sähköisen tieto- ja viestintäpalvelun tarjoaminen ja tämän käytön laskutus on tosiasiassa mahdollista, ilman että palvelun toiminnan takaamisen tavoitteella voitaisiin perustella kyseisten tietojen hyödyntämistä kulloisenkin yksittäisen käytön jälkeen.

80. Ennen vastaamista on täsmennettävä ennakkoratkaisua pyytäneen tuomioistuimen antamia tietoja, joiden mukaan riidanalaisia tietoja säilytetään pääasiassa kyseessä olevien internetsivustojen moitteettoman toiminnan varmistamiseksi, jotta niihin mahdollisesti kohdistuvista verkkohyökkäyksistä pystytään tarvittaessa käynnistämään rikosoikeudelliset menettelyt.

81. Ensimmäiseksi on siis selvitettävä, sisältyykö ennakkoratkaisupyynnössä tarkoitettujen IP-osoitteiden käsittely direktiivin 95/46 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa säädetyn poikkeuksen soveltamisalaan.[23]

1. Direktiivin 95/46 sovellettavuus riidanalaisten tietojen käsittelyyn

82. Saksan liittotasavalta vaikuttaa toimivan pääasiassa pelkkänä internetpalvelun tarjoajana, toisin sanoen yksityisenä toimijana (julkista valtaa käyttämättä). Tästä seikasta voidaan päätellä, että riita-asian kohteena oleva tietojenkäsittely kuuluu lähtökohtaisesti direktiivin 95/46 soveltamisalaan.

83. Tuomiossa Lindqvist[24] on jo todettu, että direktiivin 95/46 3 artiklan 2 kohdassa mainitut toiminnat ”ovat kaikki valtiolle tai valtion viranomaisille tyypillisiä toimintoja, jotka eivät liity yksityisten henkilöiden toiminta-aloihin”.[25] Koska tarkasteltavassa tietojenkäsittelyssä rekisterinpitäjä on toiminut todellisuudessa yksityisen oikeussubjektin tavoin, vaikka onkin viranomainen, direktiiviä 95/46 voidaan soveltaa.

84. Ennakkoratkaisua pyytänyt tuomioistuin tuo esille päätarkoituksen, jonka vuoksi Saksan hallintoviranomainen säilyttää dynaamisia IP-osoitteita, ja korostaa sen tekevän näin ”sähköisten tieto- ja viestintäpalvelujen turvallisuuden ja toimivuuden takaamiseksi ja ylläpitämiseksi”, erityisesti ”toistuvien denial-of-service-hyökkäysten tunnistamista ja ehkäisemistä varten. Näissä hyökkäyksissä teleinfrastruktuuri lamautetaan siten, että tukitaan yksittäiset verkkoserverit kohdennetuilla ja koordinoiduilla hyökkäyksillä, joissa käytetään suurta määrää tiedusteluja”.[26] Dynaamisten IP-osoitteiden säilyttäminen tätä tarkoitusta varten on kaikkien merkittävien verkkosivustojen haltijoiden yleinen tapa, eikä siihen liity suoraan eikä välillisesti julkisen vallan käyttöä, joten sen sisällyttäminen direktiivin 95/46 soveltamisalaan ei tuota suuria vaikeuksia.

23 — Direktiivin 95/46 soveltamisalaan ei kuulu ”käsittely, joka koskee yleistä turvallisuutta, puolustusta, valtion turvallisuutta – – ja *rikosoikeuden alalla tapahtuvaa valtion toimintaa*” (kursivointi tässä).

24 — Tuomio 6.11.2003 (C-101/01, EU:C:2003:596, 43 kohta).

25 — Ks. vastaavasti tuomio 16.12.2008, Satakunnan Markkinapörssi ja Satamedia (C-73/07, EU:C:2008:727, 41 kohta).

26 — Ennakkoratkaisupyyntöpäätöksen 36 kohta.

85. Ennakkoratkaisua pyytänyt tuomioistuin vakuuttaa kuitenkin, että pääasiassa osapuolina olevien palveluntarjoajien harjoittaman dynaamisten IP-osoitteiden säilyttämisen tarkoituksena on myös rikosoikeudellisten menettelyiden käynnistäminen tarvittaessa verkkohyökkäysten tekijöitä vastaan. Riittääkö tämä tarkoitus siihen, että kyseisten tietojen käsittely jää direktiivin 95/46 soveltamisalan ulkopuolelle?

86. Jos rikosoikeudellisilla menettelyillä tarkoitetaan sitä, että pääasiassa vastaajana olevat palveluntarjoajat käyttävät valtion rankaisuvaltaa, on tilanteessa nähdäkseni kyse ”rikosoikeuden alalla tapahtuvasta valtion toiminnasta” ja näin ollen yhdestä direktiivin 95/46 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa säädetystä poikkeuksesta.

87. Näissä olosuhteissa tuomiossa Huber [27] vahvistetun kannan perusteella palveluntarjoajan sähköisen tieto- ja viestintäpalvelun turvallisuuden ja teknisen toimivuuden nimissä suorittama henkilötietojen käsittely sisältyisi direktiivin 95/46 soveltamisalaan, kun taas rikosoikeuden alalla tapahtuvaan valtion toimintaan liittyvä tietojenkäsittely jäisi sen ulkopuolelle.

88. Vastaavasti myös silloin, kun varsinaiset rikosoikeudelliset menettelyt eivät kuuluisi Saksan liittovaltiolle pelkkänä palveluntarjoajana, joka ei käytä julkista valtaa vaan toimii minkä tahansa yksityisen toimijan tavoin siirtäen vain riidanalaiset IP-osoitteet valtion elimelle rangaistustoimenpiteiden toteuttamista varten, dynaamisten IP-osoitteiden käsittelyn tarkoituksena olisi niin ikään direktiivin 95/46 soveltamisalan ulkopuolelle jäävä toiminta.

89. Tämä ilmenee tuomiosta parlamentti v. neuvosto ja komissio, [28] jossa vahvistettiin, ettei se seikka, että yksityiset toimijat keräävät tiettyjä henkilötietoja ”kaupalliseen tarkoitukseen ja että ne järjestävät kyseisten tietojen siirron kolmanteen valtioon”, aiheuta sitä, ettei kyseinen siirto kuuluisi direktiivin 95/46 3 artiklan 2 kohdan ensimmäisen luetelmakohdan soveltamisalaan silloin, kun siirron tarkoituksena on rikosoikeuden alalla tapahtuva valtion toiminta, koska tällöin se ”tapahtuu julkishallinnon asettamissa puitteissa, jotka liittyvät yleiseen turvallisuuteen”. [29]

90. Sitä vastoin silloin, jos rikosoikeudellisilla menettelyillä tarkoitetaan, kuten katson ja kuten ennakkoratkaisupyynnöstä ilmenee, sellaisen yksityisen toteuttamia toimia, jolla on laillinen oikeus vaatia valtion rankaisuvaltaa käytettäväksi kyseisten toimien kautta, ei voida väittää, että dynaamisten IP-osoitteiden käsittelyn tarkoituksena olisi rikosoikeuden alalla tapahtuva valtion toiminta, joka ei kuulu direktiivin 95/46 soveltamisalaan.

91. Kyseisten tietojen säilyttäminen ja tallentaminen olisivat nimittäin yksi todistelukeino, jonka avulla verkkosivuston haltija voisi pyytää valtiota toteuttamaan rangaistustoimenpiteitä laitonta menettelyä vastaan osapuolen aloitteesta. Tällöin kyseessä olisi oikeusjärjestyksessä yksityiselle toimijalle (tässä tapauksessa julkiselle elimelle, joka toimet kuuluvat yksityisoikeuden alaan) vahvistettujen oikeuksien rikosoikeudellinen puolustuskeino. Tältä kannalta tämä ei eroa mitenkään minkä tahansa muun internetpalvelun tarjoajan aloitteesta, joka vaatii valtiolta suojaa oikeusjärjestyksessä vahvistettujen rikosoikeudellisiin toimiin liittyvien menettelyiden mukaisesti.

92. Näin ollen siltä osin kuin Saksan hallintoviranomainen on menetellyt internetpalvelun tarjoajana, joka ei käytä julkista valtaa, minkä arvioiminen on ennakkoratkaisua pyytäneen tuomioistuimen tehtävä, dynaamisten IP-osoitteiden käsittely kuuluu henkilötietojen käsittelynä direktiivin 95/46 soveltamisalaan.

27 — Tuomio 16.12.2008 (C-524/06, EU:C:2008:724, 45 kohta).

28 — Tuomio 30.5.2006 (C-317/04 ja C-318/04, EU:C:2006:346, 54–59 kohta).

29 — Ibid., tuomion 59 kohta. Kyseessä olivat henkilötiedot, joiden käsittely ei ollut välttämätöntä kyseisen palveluntarjonnan eli asianomaisten yksityisten toimijoiden (lentoyhtiöiden) liiketoiminnan kannalta, vaan yksityisten toimijoiden oli pakko siirtää henkilötiedot Yhdysvaltain viranomaisille terrorismin ehkäisemiseksi ja torjumiseksi.

2. Asiakysymys

93. TMG:n 15 §:n 1 momentin mukaan käyttäjän henkilötietoja saa kerätä ja hyödyntää vain silloin, kun se on tarpeen sähköisten tieto- ja viestintäpalveluiden tosiasiallisen tarjoamisen ja käytöstä laskuttamisen kannalta. Tarkemmin sanottuna palveluntarjoaja saa kerätä ja hyödyntää ainoastaan niin sanottuja käyttötietoja eli käyttäjän henkilötietoja, jotka ovat välttämättömiä kyseisen sähköisen tieto- ja viestintäpalvelun käytön mahdollistamiseksi ja käytöstä laskuttamiseksi. Kyseiset tiedot on poistettava käytön päättyessä (eli kun sähköisen tieto- ja viestintäpalvelun varsinainen käyttö päättyy), ellei niitä tule säilyttää laskuttamista varten, kuten TMG:n 15 §:n 4 momentissa säädetään.

94. TMG:n 15 §:ssä ei mitä ilmeisimmin jätetä mahdollisuutta säilyttää käyttötietoja yhteyden päättymisen jälkeen muilla perusteilla, eikä niitä voida säilyttää myöskään sähköisen tieto- ja viestintäpalvelun käytön yleiseksi takaamiseksi. Kyseisessä TMG:n säännöksessä tietojen säilyttämisen perusteeksi mainitaan ainoastaan laskutus, joten säännöksen voitaisiin katsoa vahvistavan (joskin säännöksen lopullinen tulkinta on ennakkoratkaisua pyytäneen tuomioistuimen tehtävä), että käyttötietoja voidaan käyttää ainoastaan konkreettisen yhteyden aikaan saamiseksi ja ne on poistettava tämän päättyessä.

95. Direktiivin 95/46 7 artiklan f alakohdassa [30] oikeutetaan henkilötietojen käsittely edellytyksin, joita pidän hieman löyhempinä (rekisterinpitäjän kannalta) kuin niitä, jotka ilmenevät TMG:n 15 §:n sanamuodosta. Saksan oikeuteen kuuluvaa säännöstä voidaan pitää tässä kohti unionin säännöstä rajoittavampana, koska siinä ei lähtökohtaisesti sallita muun kuin palvelusta laskuttamiseen liittyvän oikeutetun intressin toteuttamista, vaikka Saksan liittotasavallalla voisi internetpalvelun tarjoajana olla myös oikeutettu intressi varmistaa verkkosivustojensa moitteeton toiminta jokaisen käyttöyhteyden lisäksi. [31]

96. Unionin tuomioistuimen tuomiossa ASNEF ja FECEMD [32] esittämä näkemys tarjoaa mallin toiseen ennakkoratkaisukysymykseen vastaamiseksi. Unionin tuomioistuin totesi tuolloin, että direktiivillä 95/46 tavoitellusta tavoitteesta ”johtuu – –, että direktiivin 95/46 7 artiklaan on otettu tyhjentävä luettelo, johon on rajattu tilanteet, joissa henkilötietojen käsittelyn voidaan katsoa olevan laillista”. [33] Tästä seuraa, että ”jäsenvaltiot eivät voi lisätä direktiivin 95/46 7 artiklaan uusia henkilötietojen käsittelyn laillistamista koskevia periaatteita eivätkä säätää lisävaatimuksista, joilla muutettaisiin jonkin niiden kuuden periaatteen ulottuvuutta, joista tässä artiklassa on säädetty”. [34]

97. TMG:n 15 §:ssä ei lisätä tietojenkäsittelyn laillisuutta koskevaa ylimääräistä vaatimusta direktiivin 95/46 7 artiklassa säädettyjen vaatimusten lisäksi, kuten oli tuomiossa ASNEF ja FECEMD, [35] vaan jos kyseistä pykälää tulkitaan suppeasti, mikä on asian ratkaisevan tuomioistuimen tehtävä, sillä kavennetaan mainitun pykälän f alakohdassa säädetyn edellytyksen sisältöä: kun unionin lainsäätäjä viittaa yleisluonteisesti ”rekisterinpitäjän tai tiedon saavan sivullisen oikeutetun intressin” toteuttamiseen, TMG:n 15 §:ssä otetaan huomioon ainoastaan tarve mahdollistaa kyseisten sähköisten tieto- ja viestintäpalveluiden konkreettinen käyttö ja käytöstä laskuttaminen.

30 — Ks. edellä 17 kohta.

31 — Ks. edellä 84 kohta. Verkkosivujen haltijoilla on varmasti oikeutettu intressi ehkäistä ja torjua palvelunestohyökkäyksiä (denial of service), jotka ennakkoratkaisua pyytänyt tuomioistuin mainitsee ja joilla tarkoitetaan laajamittaisia hyökkäyksiä, joita suunnataan koordinoidulla tavalla toisinaan jotain tiettyä verkkosivustoa vastaan sivuston tukkimiseksi ja sen käytön estämiseksi.

32 — Tuomio 24.11.2011 (C-468/10 ja C-469/10, EU:C:2011:777).

33 — Ibid., tuomion 30 kohta.

34 — Ibid., tuomion 32 kohta.

35 — Kansallisessa lainsäädännössä lisättiin direktiivin 95/46 7 artiklan f alakohdan vaatimuksiin vaatimus, jonka mukaan käsiteltävien tietojen on oltava yleisön saatavana olevissa lähteissä.

98. Samoin kuin tuomiossa ASNEF ja FECEMD,[36] myös käsiteltävässä tapauksessa kansallinen toimenpide – jälleen tulkittuna edellä esitetyllä tavalla suppeasti – muuttaa direktiivin 95/46 7 artiklaan sisältyvän periaatteen ulottuvuutta eikä pelkästään täsmennä sitä, vaikka täsmentäminen on direktiivin 95/46 5 artiklan mukaisesti ainoa keino, jolla jäsenvaltioiden viranomaiset voivat käyttää hieman harkintavaltaa.

99. Viimeksi mainitun säännöksen mukaan ”jäsenvaltioiden on määriteltävä henkilötietojen käsittelyn laillisuuden edellytykset tämän luvun[37] säännösten rajoissa”. Kuten tuomiossa ASNEF ja FECEMD[38] kuitenkin todetaan, ”jäsenvaltiot eivät voi myöskään [kyseisen säännöksen] perusteella ottaa käyttöön muita henkilötietojen käsittelyn laillistamista koskevia periaatteita kuin ne, jotka mainitaan direktiivin 7 artiklassa, eivätkä lisävaatimuksilla muuttaa mainitussa artiklassa säädettyjen kuuden periaatteen ulottuvuutta”.

100. TMG:n 15 §:llä kavennetaan merkittävästi direktiivin 95/46 7 artiklan f alakohdan osalta tietojenkäsittelyn perustelemisen kannalta merkityksellisen oikeutetun intressin ulottuvuutta, eikä kyseisellä pykälällä ole pelkästään täsmennetty tai rajattu sitä saman direktiivin 5 artiklassa sallituissa rajoissa. Kaventaminen tapahtuu lisäksi hyvin kattavalla ja ehdottomalla tavalla tunnustamatta, että sähköisen tieto- ja viestintäpalvelun yleisen käytön suojaamista ja takaamista voitaisiin punnita suhteessa direktiivin 95/46 1 artiklan 1 kohdan perusteella suojaamista edellyttäviin rekisteröidyn intresseihin ja perusoikeuksiin ja -vapauksiin, kuten mainitun direktiivin 7 artiklan f alakohdassa säädetään.

101. Kuten tuomion ASNEF ja FECEMD[39] taustalla olleessa asiassa, Saksan liittotasavallan lainsäätäjä oli vahvistanut lopullisesti sen, ”mikä vastakkaisten oikeuksien ja intressien punnitsemisen tulos on, sallimatta muunlaista tulosta tiettyjen konkreettisessa tapauksessa vallitsevien erityisten olosuhteiden perusteella”, jolloin ”kyseessä ei – – ole enää [direktiivin 95/46] 5 artiklassa tarkoitettu täsmennys”.

102. Näin ollen katson, että ennakkoratkaisua pyytäneellä tuomioistuimella on velvollisuus tulkita kansallista lainsäädäntöä direktiivin 95/46 mukaisesti, mikä merkitsee sitä, että a) niin sanottujen käyttötietojen käsittelyn perusteeksi soveltuviin syihin voidaan sisällyttää sähköisen tieto- ja viestintäpalvelun tarjoajan oikeutettu intressi suojata kyseisten palveluiden yleistä käyttöä, ja sitä, että b) palveluntarjoajan kyseistä intressiä voidaan punnita tapauskohtaisesti suhteessa käyttäjän intresseihin ja perusoikeuksiin ja -vapauksiin sen selvittämiseksi, mitä intressiä direktiivin 95/46 1 artiklan 1 kohdan perusteella on suojattava.[40]

103. Mielestäni ei ole aiheellista lisätä mitään niistä perusteista, joiden pohjalta tällainen punnitseminen on tehtävä ennakkoratkaisupyynnön taustalla olevassa tapauksessa. Ennakkoratkaisua pyytänyt tuomioistuin ei esitä mitään kysymystä tästä seikasta, vaan se pyrkii ratkaisemaan tällaista punnitsemista edeltävän kysymyksen eli sen, voidaanko tällainen punnitseminen toteuttaa.

36 — Tuomio 24.11.2011 (C-468/10 ja C-469/10, EU:C:2011:777).

37 — Direktiivin 95/46 II luku, jonka otsikkona on ”Yleiset säännöt henkilötietojen käsittelyn laillisuudesta” ja johon sisältyvät 5–21 artikla.

38 — Tuomio 24.11.2011 (C-468/10 y C-469/10, EU:C:2011:777, 36 kohta).

39 — Ibid., tuomion 47 kohta.

40 — Breyerin puolustus kiisti suullisessa käsittelyssä, että dynaamisten IP-osoitteiden tallentaminen olisi välttämätöntä internetpalvelun moitteettoman toiminnan suojaamiseksi mahdollisten hyökkäysten varalta. Ongelmaan ei nähdäkseni voida antaa ehdotonta yleispätevää ratkaisua, vaan ennen ongelman ratkaisemista on jokaisessa yksittäisessä tapauksessa sen sijaan punnittava ensin vastakkain verkkosivuston haltijan intressiä sekä käyttäjien oikeuksia ja intressejä.

104. Lienee merkityksetöntä tuoda esille, että asian ratkaiseva tuomioistuin voi ottaa huomioon ne mahdolliset oikeussäännöt, joita jäsenvaltio on antanut käyttäessään direktiivin 95/46 13 artiklan 1 kohdan d alakohdassa annettua valtaa kaventaa saman direktiivin 6 artiklassa säädettyjen velvollisuuksien ja oikeuksien ulottuvuutta silloin, kun tämä on välttämätöntä muiden seikkojen ohella rikosten torjumisen, tutkimisen, selvittämisen ja syyteharkinnan kannalta. Ennakkoratkaisua pyytänyt tuomioistuin ei myöskään viittaa tähän seikkaan, vaikka se on eittämättä tietoinen molempien artiklojen olemassaolosta.

105. Näin ollen ehdotan, että toiseen ennakkoratkaisukysymykseen vastataan siten, että direktiivin 95/46 7 artiklan f alakohta on esteenä sellaiselle kansalliselle säännökselle, jonka tulkinta estää palveluntarjoajaa keräämästä ja käsittelemästä käyttäjän henkilötietoja ilman käyttäjän suostumusta kulloisenkin yksittäisen käytön jälkeen, kun tavoitteena on taata sähköisen tieto- ja viestintäpalvelun toiminta.

VI Ratkaisuehdotus

106. Ehdotan edellä esitetyn perusteella, että unionin tuomioistuin vastaa esitettyihin kysymyksiin seuraavasti:

1) Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY 2 artiklan a alakohdan mukaisesti dynaaminen IP-osoite, jonka avulla käyttäjä on käynyt sähköisen tieto- ja viestintäpalvelun tarjoajan verkkosivuilla, on viimeksi mainitun kannalta henkilötieto edellyttäen, että verkkoyhteyden tarjoajalla on hallussaan lisätietoja, jotka dynaamiseen IP-osoitteeseen yhdistettyinä auttavat tunnistamaan käyttäjän.

2) Direktiivin 95/46 7 artiklan f alakohtaa on tulkittava siten, että sähköisen tieto- ja viestintäpalvelun toiminnan takaamisen tavoitetta voidaan lähtökohtaisesti pitää oikeutettuna intressinä, jonka toteuttamisella voidaan perustella kyseisen henkilötiedon käsittely, jos kyseisen intressin arvioidaan olevan tärkeämpi kuin kyseessä olevan henkilön intressit tai perusoikeudet. Kansallinen säännös, jonka perusteella kyseistä oikeutettua intressiä ei voida ottaa huomioon, on mainitun artiklan vastainen.